ETSI TR 119 460 V1.1.1 (2021-02)

Electronic Signatures and Infrastructures (ESI);
Survey of technologies and regulatory requirements for identity proofing for trust service subjects

Reference
DTR/ESI-0019460

Keywords
electronic signatures, identity proofing, security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The actions proposed in this proposal respond to the policy area "Electronic identification and trust services including e-signatures" of the "Key enablers and security" cluster of the ICT RP. Action 2 of this policy area calls for European standardization organizations to update existing standards and to develop additional ones to address the requirements of the eIDAS regulation [i.1]. ETSI Technical Committee ESI (TC ESI) has concluded that the actions proposed by the present document are needed within the scope of additional standards.

The scope of the proposed actions is identity proofing for trust services as defined by eIDAS [i.1], in particular for issuers of qualified and non-qualified certificates supporting electronic signatures, electronic seals or website certificates. The results of the STF's work may however be applicable also in other areas such as issuing of electronic IDentity (eID) and Know-Your-Customer (KYC) processes in various industries.

Identity proofing is crucial for trust in all digital services that require identification of a natural or legal person. The current European standards published by ETSI on trust services specify identity proofing only by generic requirements like "physical presence" or "means which provide equivalent assurance as physical presence". Physical presence as a reference is not well-defined as no requirements are posed neither for the quality of (physical) identity documents nor for the competence or procedures to be carried out by the person performing the check. What constitutes equivalent assurance as physical presence is up to subjective judgement. Consequently, practices for identity proofing for trust services vary a lot across the EU Member States, hampering provision of trust services in the internal market. In particular, guidelines for remote identity proofing are needed to avoid cumbersome and expensive physical presence procedures when possible.

An ETSI specification for identity proofing for trust services will provide the following advantages:

- a rationalized mapping of policies and standards used in the trust services market for identity proofing;
- foundation upon which national specifications can be made, leading to harmonisation of such specifications;
- reference specification that can be used where national specifications do not exist.

Harmonisation with identity assurance for other purposes, such as eID issuing (including eIDAS eID means) and KYC processes.

NOTE: eID means, on the other hand, can also be a tool for performing an identity proofing process.

It is foreseen that a trust service provider may subcontract identity proofing to a specialized provider, and that such an identity proofing provider may serve several trust service providers. Thus, identity proofing is defined as **a trust service component**. Policy and security requirements for identity proofing will be specified, valid both for trust service providers and for specialized providers of identity proofing service components.

The present document provides the results of a survey on the technologies, legislations, specifications, guidelines and standards related to or used for identity proofing. The present document provides a "point in time" picture of the identity proofing landscape at the time of edition, i.e. September 2020. It aims to be rather broad and serves as a basis for, ETSI DTS/ESI-0019461 "*Policy and security requirements for trust service components providing identity proofing of trust service subjects*" that addresses identity-proofing for trust service providers.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document provides the results of a survey on the technologies, legislations, specifications, guidelines and standards related to or used for identity proofing.

Information has been collected as comprehensively as possible, and is analysed in the present document. The aim is to identify trends and select relevant elements for ETSI DTS/ESI-0019461 [i.50] to address both security policy and security requirements for enrolment of Trust Services subjects.

The methodology to achieve this goal is presented in clause 4 and is followed by the analysis.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.3] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.4] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.5] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.7] FIPS 140-2: "Security Requirements for Cryptographic Modules".

[i.8] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.9] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.10] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.11] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.12] NIST Special Publication 800-171 (Revision 2): "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations".

[i.13] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.14] NIST Special Publication 800-73: "Interfaces for Personal Identity Verification".

[i.15] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.16] ISO/IEC 29003: "Information technology -- Security techniques -- Identity proofing".

[i.17] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.18] ISO/IEC 24760-1: "IT Security and Privacy -- A framework for identity management -- Part 1: Terminology and concepts".

[i.19] ETSI TS 119 431-1 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev".

[i.20] Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (Text with EEA relevance).

[i.21] Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (Text with EEA relevance).

[i.22] Guidance for the application of the levels of assurance which support the eIDAS Regulation Published but undated.

[i.23] ISO/IEC 19989-3: "Information security -- Criteria and methodology for security evaluation of biometric systems -- Part 3: Presentation attack detection".

[i.24] ISO/IEC 27001 (2013): "Information technology -- Security techniques -- Information security management systems -- Requirements.

[i.25] ISO/IEC 15408 (multipart-series): "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.26] ISO/IEC 18045: "Information technology -- Security techniques -- Methodology for IT security evaluation".

[i.27] ISO 19011 (2011): "Guidelines for auditing management systems".

[i.28] ISO/IEC 30107-4: "Information technology - Biometric presentation attack detection -Part 4: Profile for testing of mobile devices.

[i.29] ISO/IEC 27007: "Information security, cybersecurity and privacy protection -- Guidelines for information security management systems auditing".

[i.30] ISO/IEC 29115 (2013): "Information technology -- Security techniques -- Entity authentication assurance framework".

[i.31] ISO/IEC 30107-2: "Information technology - Biometric presentation attack detection - Part 2: Data Formats".

[i.32] ISO/IEC 30107-1:2016: "Information technology - Biometric presentation attack detection - Part 1: Framework".

[i.33] ETSI TS 101 862: "Qualified Certificate profile".

[i.34] Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences (Recast) (Text with EEA relevance).

[i.35] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security controls".

[i.36] NIST Special Publication 800-63-3: "Digital Identity Guidelines".

[i.37] ISO/IEC 19794-5: "Information technology -- Biometric data interchange formats -- Part 5: Face image data".

[i.38] ISO 9001 (2015): "Quality management systems -- Requirements".

[i.39] OpenID Connect for Identity Assurance 1.0.

[i.40] EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements" (produced by CEN).

[i.41] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement.

[i.42] Common Criteria (V3.1/R5) (04/2017): "Common Methodology for Information Technology Security Evaluation".

[i.43] NIST Special Publication 800-63A: "Digital Identity Guidelines, Enrollment and Identity Proofing".

[i.44] NIST Special Publication 800-63B: "Digital Identity Guidelines, Authentication and Lifecycle Management".

[i.45] NIST Special Publication 800-63C: "Digital Identity Guidelines, Federation and Assertions".

[i.46] Commission Implementing Regulation (EU) No 1247/2012 of 19 December 2012 laying down implementing technical standards with regard to the format and frequency of trade reports to trade repositories according to Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories.

[i.47] Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights.

[i.48] Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004.

[i.49] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[i.50] ETSI DTS/ESI-0019461: "ESI Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[i.51] CEN TR 419010 (2017): "Framework for standardization of signatures. Extended structure including electronic identification and authentication".

[i.52] EU Commission: Single MarketStudy on eID and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the EU.

[i.53] ENISA Report - eIDAS COMPLIANT eID SOLUTIONS: "Security Considerations and the Role of ENISA". (March 2020).

[i.54] UNCITRAL Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services. A/CN.9/WG.IV/WP.168. Working Group IV (Electronic Commerce). Sixtieth session. New York, 6-9 April 20.

[i.55] UNCITRAL Draft Provisions on the Use and Cross border Recognition of Identity Management and Trust Services. Submission by the World Bank. A/CN.9/WG.IV/WP.163. Working Group IV (Electronic Commerce). Sixtieth session. New York, 6-9 April 20 CA/Browser forum requirements (V1.7.1).

[i.56] CA/Browser: "Guidelines For The Issuance And Management Of Extended Validation Certificates" (V1.7.4).

[i.57] UK guidance on Identity proofing and authentication.

[i.58] UK Good Practice Guide 45: "Natural person ID proofing".

[i.59] UK Good Practice Guide 46: "Organizations or individuals acting on behalf of those organizations ID proofing".

[i.60] UK Good Practice Guide 44: "Using authenticators to protect an online service".

[i.61] UK Good Practice Guide 43: "Requirements for Secure Delivery of Online Public Services".

[i.62] UK Good Practice Guide 53: "Transaction monitoring for HMG online service providers".

[i.63] Draft BSI 8626: "Design and operation of online user identification systems - Code of practice". Available online as of July 2020.

[i.64] Technical Guideline TR-03147 (V1.0.4): "Assurance Level Assessment of Procedures for Identity Verification of Natural Persons".

[i.65] Communication for Qualified Trust Service Providers in Romania.

[i.66] ANSSI: Moyens d'identification electronique - Référentiel d'exigences de sécurité. Draft dated August 29 2018 - version 1.0.d.

[i.67] BundesNetzAgentur/Gazette 126/2017 :"Konsolidierte Fassung der geänderten Verfügung der Bundesnetzagentur gemäß §111Absatz1Satz4 Telekommunikationsgesetz" (Stand: 22.11.2017).

[i.68] BNtAg 208/2018: "Verfügung gemäß", § 11 Absatz 1 VDG.

[i.69] G20 Digital Identity Onboarding.

[i.70] BITS: Norway. "Requirements for secure digital verification of identity". (November 2019).

[i.71] Directive (EU) 2018/843 of the European Parliament and of the Council amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('AMLD5').

[i.72] Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions - December 2019. European Commission. Directorate-General for Financial Stability, Financial Services and Capital Markets Union.

[i.73] Banking Assessing portable KYC/CDD solutions in the banking sector: The case for an attribute-based & LoA-rated KYC framework for the digital age - December 2019 European Commission. Directorate-General for Financial Stability, Financial Services and Capital Markets Union.

[i.74] FATF digital identity guidance MARCH 2020.

[i.75] National Bank of Belgium Object of the identification and identity verification: Comments and recommendations.

[i.76] SEPBLAC: Autorización de procedimientos de vídeo-identificación (2016).

[i.77] SEPBLAC: Autorización de procedimientos de identificación no presencial mediante videoconferencia (2017).

[i.78] PROVVEDIMENTO 30 luglio 2019. Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo. (19A05172) (GU Serie Generale n.189 del 13-08-2019).

[i.79] Regolamento IVASS n. 44 del 12 febbraio 2019. Regolamento IVASS recante disposizioni attuative volte a prevenire l'utilizzo delle imprese di assicurazione e degli intermediari assicurativi a fini di riciclaggio e di finanziamento del terrorismo in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela, ai sensi dell'articolo 7, comma 1, lettera a) del Decreto legislativo 21 novembre 2007, n. 231.

[i.80] BAFin Circular 3/2017 (GW) - Video Identification Procedures.

[i.81] SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market.

[i.82] NISTIR 8202. Blockchain Technology Overview.

[i.83] ILNAS White Paper. Blockchain And Distributed Ledgers Technology, Economic Impact And Technical Standardization. Version 1.0 - June 2018.

[i.84] Decentralized Identifiers (DIDs) v1.0. Core Data Model and Syntaxes. W3C Working Draft 09. December 2019.

[i.85] OpenID connect identity assurance working group (eKYC Project), Work in Progress - On-going TIR Draft Ongoing Face RecognitionVendor Test (FRVT) .

[i.86] European Council PRADO - Public Register of Authentic travel and identity Documents Online.

[i.87] Machine Readable Document (MRTD). ICAO 9303 (multipart).

[i.88] FIDO Alliance White Paper: Using FIDO with eIDAS Services Deploying FIDO2 for eIDAS QTSPs and eID schemes. May 2020.

[i.89] ISO/IEC 7501 (2005): "Identification cards -- Machine readable travel documents".

[i.90] ISO/IEC 7816 (2019): "Identification cards -- Integrated circuit cards".

[i.91] ISO/IEC 14443-1 (2018): "Cards and security devices for personal identification -- Contactless proximity objects".

[i.92] ISO/IEC 18092 (2013): "Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1) ISO/IEC 21491".

[i.93] ISO/IEC 15693-2 (2000): "Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards ISO/IEC 18013".

[i.94] ISO/IEC TR 19446 (2015): "Differences between the driving licences based on the ISO/IEC 18013 series and the European Union specifications".

[i.95] ISO/IEC 27701 (2019): "Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines ISO/IEC 29100".

[i.96] ISO/IEC 29101 (2018): "Information technology -- Security techniques -- Privacy architecture framework".

[i.97] ISO/IEC 29134 (2017): "Information technology -- Security techniques -- Guidelines for privacy impact assessment ISO/IEC 29151".

[i.98] ISO/IEC 29184 (2020): "Information technology -- Online privacy notices and consent ISO/IEC 29190".

[i.99] ISO/IEC 19792 (2009): "Information technology -- Security techniques -- Security evaluation of biometrics".

[i.100] ISO/IEC 24745 (2011): "Information technology -- Security techniques -- Biometric information protection".

[i.101] ISO/IEC 24761 (2019): "Information technology -- Security techniques -- Authentication context for biometrics".

[i.102] ISO/IEC 24779 (2016): "Information technology -- Cross-jurisdictional and societal aspects of implementation of biometric technologies -- Pictograms, icons and symbols for use with biometric systems".

[i.103] ISO/IEC 19784 (2018): "Information technology -- Biometric application programming interface".

[i.104] ISO/IEC 19785 (2020): "Information technology -- Common Biometric Exchange Formats Framework".

[i.105] ISO/IEC 19794 (multipart series): " Information technology -- Biometric data interchange formats".

[i.106] ISO/IEC 39794 (2019): "Information technology -- Extensible biometric data interchange formats".

[i.107] ISO/IEC 30108 (2015): "Information technology -- Biometric Identity Assurance Services -- Part 1: BIAS services".

[i.108] ISO/IEC TR 29196 (2018): "Guidance for biometric enrolment".

[i.109] ISO/IEC TR 29194 (2015): "Guide on designing accessible and inclusive biometric systems".

[i.110] ISO/IEC TR 29156 (2015): "Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics".

[i.111] ISO/IEC TR 30125 (2015): "Biometrics used with mobile devices".

[i.112] ISO/IEC TR 29144 (2014): "The use of biometric technology in commercial identity management applications and processes".

[i.113] CEN TS 17489: "Identification cards. Chip cards. Biometrics".

[i.114] ETSI EN 301 549 (V2.1.2) (2018-08) "Accessibility requirements for ICT products and services".

[i.115] IETF RFC 4226: "TOTP: Time-Based One-Time Password Algorithm".

[i.116] ISO/IEC 17025: "General requirements for the competence of testing and calibration laboratories".

[i.117] ISO/IEC 19795-1 (2006): "Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework".

[i.118] ISO/IEC 30107-3: "Information technology -- Biometric presentation attack detection -- Part 3: Testing and reporting".

[i.119] ISO 22301: "Security and resilience -- Business continuity management systems -- Requirements".

[i.120] CA/Browser forum EV Guidelines" Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (V1.7.1).

[i.121] IETF RFC 6238: "Time-Based One-Time Password Algorithm".

[i.122] ISO/IEC 24760 (multi-part series): "IT Security and Privacy -- A framework for identity management".

[i.123] ISO/IEC 27000: "Information technology - Security techniques -- Information security management systems -- Overview and vocabulary".

[i.124] The FATF Recommendations.

NOTE: Available at Documents - Financial Action Task Force (FATF) (fatf-gafi.org).

[i.125] NISTIR Draft Ongoing Face RecognitionVendor Test (FRVT) Part 1: Verification.

NOTE: Available at https://www.nist.gov/system/files/documents/2019/11/20/frvt_report_2019_11_19_0.pdf.

[i.126] NISTIR Draft Ongoing Face RecognitionVendor Test (FRVT) Part 2: Identification".

NOTE: Available at Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification (nist.gov).

[i.127] ISO/IEC 27005: "Information technology -- Security techniques -- Information security risk management".

[i.128] Apple® MFI Program.

[i.129] ISO/IEC 10536: "Identification cards -- Contactless integrated circuit(s) cards -- Close-coupled cards".

[i.130] ISO/IEC 30106: "Information technology -- Object oriented BioAPI".

[i.131] World Economic Forum (2016): "A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity".

[i.132] ISO/TR 23244: "Blockchain and distributed ledger technologies - Privacy and personally identifiable information protection considerations".

[i.133] ISO/NP TR 23246 "Overview of identity management using Blockchain and DLT".

[i.134] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

[i.135] CEN/TS 15480 (multipart): "Identification card systems - European Citizen Card".

[i.136] ISO/IEC 29100: "Information technology -- Security techniques -- Privacy framework".

[i.137] ISO/IEC 29151: "Information technology -- Security techniques -- Code of practice for personally identifiable information protection".

[i.138] ISO/IEC 29190: "Information technology -- Security techniques -- Privacy capability assessment model".

[i.139] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.140] ISO/IEC 18013: "Personal identification -- ISO-compliant driving licence".

[i.141] EU 2015/1505: "Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

applicant: person (legal or natural) whose identity is to be proofed to become subject or subscriber (of a trust service)

application: process whereby information to be used for identity proofing of a subject or subscriber is provided

NOTE: See ISO/IEC 29003 [i.16].

assertion: statement that contains information about an entity, e.g. a legal or natural person

NOTE: Assertions may contain verified attributes.

authoritative evidence: evidence that holds identifying attribute(s) that are managed by an authoritative party/source

NOTE 1: This is one type of evidence of identity.

NOTE 2: Source ISO/IEC 29003 [i.16].

authoritative source: any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity

NOTE: Source eIDAS [i.1].

attribute: quality or characteristic ascribed to someone or something

NOTE: See NIST SP 800-63-3 [i.36].

attribute evidence: information linking an attribute, or a series of attributes, to an entity e.g. a legal or natural person (see also **identity evidence** below)

NOTE: Attribute evidence may be either physical (documentary) or purely digital, or a digital representation of physical attribute evidence (e.g. a digital representation of a paper or plastic driver's license) (see FATF Digital Identity Guidance March 2020 [i.74]).

binding: step of identity proofing process that involves confirming that the validated identity relates to the applicant being identity-proofed

NOTE 1: Source FATF Digital Identity Guidance March 2020 [i.74].

NOTE 2: Some documents refer to "mapping".

credential: set of data presented as evidence of a claimed or asserted identity and/or entitlements

NOTE 1: Physical object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by the owner of the identity (see NIST SP 800-63-3 [i.36]).

NOTE 2: See ISO/IEC 29003 [i.16].

Credential Service Provider (CSP): entity that issues and/or registers authenticators and corresponding electronic credentials (binding the authenticators to the verified identity) to subscribers

NOTE 1: The CSP is responsible for maintaining the subscriber's identity credential and all associated enrolment data throughout the credential's lifecycle and for providing information on the credential's status to verifiers.

NOTE 2: Source FATF Digital Identity Guidance March 2020 [i.74].

digital identity: unique representation of a subject engaged in an online transaction

NOTE 1: A digital identity is always unique in the context of a trust service but does not necessarily need to uniquely identify the subject in all contexts (see NIST SP 800-63-3 [i.36]).

NOTE 2: See source NIST SP 800-63-3 [i.36].

electronic identification: process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person

NOTE: Source eIDAS [i.1].

electronic identification means: material and/or immaterial unit containing person identification data, and which is used for authentication for an online service

NOTE: Source eIDAS [i.1].

enrolment (registration): process through which an applicant applies to become a subject or a subscriber of a trust service

NOTE 1: Source NIST SP 800-63-3 [i.36].

NOTE 2: This process usually requires validating the applicant's identity.

NOTE 3: If the service is the provisioning of a credential, this process authoritatively binds the subject or subscriber's unique verified identity (i.e. the subject or subscriber's attributes/identifiers) to one or more authenticators possessed and controlled by the subscriber, using an appropriate binding protocol. The process of binding the subject or subscriber's identity to authenticator(s) is also referred to as ***'credentialing'*** (see FATF Digital Identity Guidance March 2020 [i.74]).

NOTE 4: A **registration authority** in the framework of issuance of certificates if the entity that is responsible for identification and authentication of subjects of certificates.

federation: process that allows the conveyance of identity and authentication information across a set of systems

NOTE: Source NIST SP 800-63-3 [i.36].

identifying attribute: attribute that contributes to uniquely identifying an entity (subject or subscriber) within a context

NOTE: Source ISO/IEC 29003 [i.16].

identity: attribute or set of attributes that uniquely describe an entity within a given context

NOTE: Source NIST SP 800-63-3 [i.36].

Identity Assurance Level (IAL): degree of confidence that the applicant's claimed identity is their real identity

NOTE: Source NIST SP 800-63-3 [i.36].

identity evidence: information or documentation provided by the ***applicant*** to support the claimed identity

NOTE 1: Identity evidence may be physical (e.g. a driver license) or digital (e.g. an assertion generated and issued by a CSP based on the applicant successfully authenticating to the CSP).

NOTE 2: Source NIST SP 800-63-3 [i.36].

identity proofing: process by which a (trust) service provider collects and validates information about an applicant and verifies that so collected and validated information actually belongs to the applicant

NOTE: This process may also imply resolving information about a person to a unique individual within a given population or context.

identity provider: entity that makes available identity information

NOTE 1: Source ETSI TR 119 001 [i.17].

NOTE 2: See ISO/IEC 24760-1 [i.18].

identity Service Provider (IDSP): generic umbrella term that refers to all of the various types of entities involved in providing and operating the processes and components of a digital ID system or solution

NOTE 1: IDSPs provide digital ID solutions to users and relying parties. A single entity can undertake the functional roles of one or more IDSPs.

NOTE 2: Source FATF Digital Identity Guidance March 2020 [i.74].

person identification data: set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established

NOTE: Source eIDAS [i.1].

relying party: natural or legal person that relies upon an electronic identification or a trust service

NOTE 1: Source NIST SP 800-63-3 [i.36].

NOTE 2: In the first case (electronic identification), it can be an entity that relies upon another entity authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to identify the later and/or to process a transaction or grant access to information or a system.

subject: person (or organization, device, hardware, network, software, or service) that is enrolled to a trust service

NOTE: Source NIST SP 800-63-3 [i.36].

EXAMPLE: Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations

NOTE: Source ETSI TR 119 001 [i.17].

(attributes) validation: part of identity proofing process that involves determining that an evidence is genuine (not counterfeit or misappropriated) and the information the evidence contains is accurate

NOTE 1: This can be done by checking the identity information/evidence against an acceptable (authoritative/reliable) source to establish that the information matches reliable, independent source data/records.

NOTE 2: Source FATF Digital Identity Guidance March 2020 [i.74].

pseudonym: name other than a "legal" name

NOTE: Source NIST SP 800-63-3 [i.36].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAL	Authenticator Assurance Level
AATL	Adobe® Approved Trust List
AI	Artificial Inteligence
AML	Anti-money laundering
AMLD	Anti-Money Laundering Directive
ANSSI	French National Agency for the Security of Information Systems
APCER	Attack Presentation Classification Error Rate
API	Application Programming Interface
BAFIN	Federal Financial Supervisory Authority (German: Bundesanstalt für finanzdienstleistungsaufsicht)
BDB	Biometric Data Block
BIAS	Biometric Identity Assurance Services
BIR	Biometric Information Record
BPCER	Bonafide Presentation Classification Error Rate
BR	Baseline Requirements
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CA/B	Certification Authority and Browser forum
CBEFF	Common Biometric Exchange Formats Framework
CDD	Customer Due Diligence
CDS	Certified Document Services
CIR	Commission Implementing Decision
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CS	Code Signing
CSCA	Country Signing Certification Authority
CSP	Credential Service Provider
DBA	Doing Business As
DID	Decentralized IDentifiers
DLT	Distributed Ledger Technology
DNI	National Identity Card (Spain)
DNS	Directory Name Server
DPI	Dots Per Inch
DRP	Disaster Recovy Plan
DV	Document Verifier
DVCP	Domain Validation Certificate Policy
EBA	European Banking Authority
EBSI	European Blockchain Services Infrastructure
ECOFIN	Economic and Financial Affairs Council
EEA	European Economic Area
EMEA	Europe, Middle East and Africa
EN	European Norm
ENISA	European Union Agency for Cybersecurity
ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
ESA	European Supervisory Authorities
ESSIF	European Self Sovereign Identity Framework

EV	Extended Validation
EVCP	Extended Validation Certificate Policy
EVG	Extended Validation Guidelines
FAL	Federation Assurance Leve
FAR	False Acceptance Rate
FATF	Financial Action Task Force
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FRVT	Face RecognitionVendor Test
GAFA	Google®, Apple®, Facebook®, Amazon®
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications
GwG	GeldwäscheGesetz (German Money Laundering Act)
HMG	Her/His Majesty's Government (British Government)
IAL	Identity Assurance Level
ICAO	International Civil Aviation Organization
IDV	IDentity Verification
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IGTF	Interoperable Global Trust Federation
ILNAS	Luxembourg Institute of Standardisation
INCITS	USA InterNational Committee for Information Technology Standards
IP	Internet Protocol/Identity Proofing
IR	InfraRed
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technologies
IVCP	Individual Validation Certificate Policy
JMLSG	Joint Money Laundering Steering Group (UK)
KYC	Know Your Client/Customer
LCP	Lightweight Certificate Policy
LoA	Level of Assurance
LP	Legal Person
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NA	Not Applicable
NCP	Normalized Certificate Policy
NFC	Near Field Communication
NISTIR	NIST InteRagency or Internal Reports
NP	Natural Person
OCR	Optical Character Recognition
OP	OpenID Connect Provider
OUIS	Online User Identification System
OV	Organizational Validation
OVCP	Organizational Validation Certificate Policy
PAD	Personal Attack Detection
PASS	Proof of Age Standards Scheme (UK)
PC	Personal Computer
PIN	Personal Identification Number
PIV	Personal Identity Verification
PK	Public Key
PKD	Public Key Directory
PKI	Public Key Infrastructure
PTC	Publicly-Trusted Certificate
QCP	Qualified Certificate Policy
QERDS	Qualified Electronic Registered Delivery Service
QERDSP	Qualified Electronic Registered Delivery Service Provider
QES	Qualified Electronic Signature
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
QR	Quick Response (code)
QSCD	Qualified electronic Signature/Seal Creation Device

QTSP	Qualified Trust Service Provider
RA	Registration Authority
RFC	Request for Comments
RFID	Radio Frequency IDentification
SAML	Security Assertion Markup Language
SBH	Standard Biometric Header
SCD	Signature Creation Device
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module/Subscriber Identification Module
SMS	Short Message Service
SPID	Service Profile IDentifier
SSI	Self Sovereign Identity
SSO	Single Sign-On
TAN	Tax deduction Account Number
TE	Type of Evidence
TKG	German Telecommunications Act
TLS	Transport Layer Security
TP	Type of Presentation
TSP	Trust Service Provider
TÜV	TÜV Informationstechnik GmbH
UN	United Nations
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UV	UltraViolet
VAT	Value Addes Tax
VDG	Confident Services Act (Germany)
VPN	Virtual Private Network
WCAG	W3C Web Content Accessibility Guidelines
WG	Working Group

4 Study methodology

4.1 Introduction

ID-proofing can be defined as **a three-step process** (see clause 4.2.3) following FATF Digital Identity Guidance March 2020 [i.74], or NIST guidance on Identity proofing). These steps will be the window through which the present document will analyze the received information as explained in the next clauses. This is done considering that identity proofing is a highly context-driven process which is dependent on a number of factors, including:

a) Purpose (expected output and related obligations):

   i) whether the use case of the ID-proofing process is implemented for the purpose of creating a digital identity, government issued electronic ID, offering a digital trust service or for commercial or recreational purpose;

   ii) whether the party relying on the ID-proofing needs/requires a given level of assurance as a result of the ID-proofing process; or

   iii) whether the ID-proofing process refers to a natural person or a legal entity or a natural person acting on behalf of a legal entity.

b) Technical and procedural criteria and constraints for proving identity (i.e. to collect evidence and attributes, validate these attributes and map it with the applicant):

   - whether the process takes place on-premises or remotely;

   - whether ID, travel documents or other credentials (e.g. social data) are used for the ID- proofing process;

   - whether third party databases (including government databases) are used for the ID-proofing process;

- the technologies available for ID-proofing processes;
- the technical standards or specifications available for ID-proofing processes; or
- the operating procedures of the entity(ies) implementing the ID-proofing process.

The technical and procedural criteria and constraints may be imposed by the purpose, legal context in particular, and beyond, are dependent of the identity proofing provider organization.

4.2 Method for analysing received info

4.2.1 Overview

The analysis consists of the following stages:

- the analysis against any source of information in reading sheets using the general methodology included in clause 4.2.3. This analysis is further completed considering the feedback from the questionnaires to vendors and TSPs, the eIDAS Regulation [i.1] revision consultation, and ID proofing harmonization coming from the general European finance strategy (see clause 5);
- the analysis across the sources of information, for each component of the methodology against reading sheets. This aims to derive market trends or identity gaps in the technical landscape. (see clause 6);
- the conclusion that identifies the relevant information for following developments (see clause 7).

4.2.2 Collection of information

The present document surveys the technologies, legislations, specifications, guidelines and standards related to or used for identity proofing.

Information comes from sources such as national agencies developing requirements, product and service vendors, research and academic environments, and **relevant** existing specifications and eIDAS Regulation revision [i.1]. Diverse stakeholders have been identified and categorized as sources of information.

Such sources were mostly contacted by eMails and some stakeholders (vendors of identity management solution and TSPs) were provided with a questionnaire (see Annexes B and C).

4.2.3 General methodology

The received information analysed in the present document aims to identify common trends and select relevant ones for the TS, addressing security policy and requirements for enrolment of Trust Services subjects.

As the the present document is to offer an overview of the diversity of existing ID-proofing processes, the outcome of the analysis describes a number of key topics in relation to each of the three "identity proofing process" steps detailed below, as this will facilitate the preparation of ETSI DTS/ESI-0019461 [i.50].

Step 1) Attribute and evidence collection. This will consider:

a) Identity attributes collected:
   - for individuals;
   - for legal entities;
   - for individuals acting on behalf of legal entities.

b) Type of evidence to be/that can be presented:
   - type of document or evidence (e.g. a passport);
   - trusted/authoritative sources for the ID attributes (Presentation of eligible issuers or trusted data sources of ID attributes);

NOTE: "*Determination that the evidence is genuine - issued by recognised independent/authoritative sources*" is addressed in the attribute validation clause that presents the way to verify that the evidence indeed comes from the expected source. The present clause indicates which sources are to be trusted.

c) Type of presentation of the attributes:

- collected as digital representation of an identity document (e.g. scan or photo of identity card or passport):
  - captured remotely;
  - captured on site (e.g. a photocopy) during a "on-premise" - physical presentation;
- digitally extracted from an electronic ID document;
- transmitted in purely digital form as an eID or e-signature/e-seal.

d) Communication:

- In the event of remote collection, e.g.:
  - protocol and APIs used for the transfer of ID attributes (e.g. SAML or OpenID Connect);
  - security measures deployed to protect the integrity of the attribute transmission (e.g. end-to-end encryption);
  - identity attributes remotely presented by the applicant or obtained from a third party independent of the applicant.
- In case of "on-premise" physical presentation, constraints to be observed e.g. by the personnel.

Step 2) Attribute and evidence validation. This will consider:

e) determination that the evidence is genuine (issued by recognized independent/authoritative sources);

f) determination that the ID attributes are valid (not expired, not revoked).

The following aspects are analysed:

- customary security checks implemented, and security features verified in relation to attributes collected as digital representation of an ID document;
- customary security checks implemented in relation to 'purely digital' attributes (digitally extracted from ID documents or obtained via an eID or SSI);
- description of other checks implemented if any (e.g. matching with other data, verification of expiry date, etc.);
- description of external (governmental) sources queries if any;
- applicable technical standards if any.

Step 3) Binding ID attributes with applicant. Mapping ID attributes with applicant or the attribute binding process can be defined as the steps taken to confirm, with a given degree of confidence, that the claimed identity credentials (for example those shown in a passport or ID card) which have been obtained and confirmed as valid are indeed those of the applicant and not of someone else.

This will consider that the applicant's verified identity (i.e. the applicant's attributes) is bound to one or more authenticators possessed and controlled by the applicant (binding protocol). This varies significantly with the assurance level achieved by the ID-proofing. Its presentation will consider:

- The technologies used for the binding protocol (lower, standard and higher assurance levels services).
- When no face to face identification is performed, whether remote liveliness detection and biometric factors are used, as well as:
  - Applicable regulatory constraints (e.g. privacy).

- Description of customary anti-fraud processes.
- Applicable technical standards.

It is also necessary to consider the identity proofing process as a whole and to analyse the **requirements of the process**, i.e. a description of the ID proofing process (what needs to be done and why) and how this process is done as well as elements common to all steps such as:

- What needs to be done and why.
- How the process is done.
- Possible security levels associated to one step or the whole process.
- Compliance measures implemented (traceable documentation, access policy, personnel training and authorization, premises security, etc.).
- Description of customary technical standards applied if any.
- Description of customary auditing processes if any.

To achieve the objective each document will be analysed through a "**reading sheet**" mapped with the above elements, to allow classification of information and further comparison.

Each reading sheet is further introduced by a short description presenting:

- purpose & context;
- identity type to be validated;
- expected outputs;
- sector;
- legal background if any.

5 Information collected on existing ID-proofing processes and models

5.1 Introduction

The present clause introduces each document analysed by the STF; a total of 47 documents, or series of documents, have been analysed through the perspective of the reading sheet. They are classified according to their origin.

The reading sheets are not a detailed description/comprehensive analysis of the referenced documents but try to summarize the main points. Readers are encouraged to consult the references provided at the end of the reading sheets if interested in more info. Some of the main requirements from the referenced document are restated for information in the present document.

It also summarizes the feedback received from stakeholders; vendors and TSPs as well as information related to the evolution of the identity proofing landscape in the framework of the eIDAS [i.1] revision.

5.2 International and national legal frameworks, standards and good practices

5.2.0 General

A basic principle and key assumption of public international law is that States are competent authorities when it comes to defining who their nationals are. Although the principle is not absolute and implies cooperation for its smooth implementation - for example when it comes to recognizing foreign travel documents with the ICAO rule 9303 - there is little doubt that States have a vested interest in identity-related matters. It is often the view that this falls within their core competencies, therefore limiting the scope of applicable treaties or international regulations. This situation is also, although to a lesser extent, reflected in more integrated zones such as the European Union, including in relation to digital identity regulations. For example, the eIDAS regulation [i.1] currently dictates that only member States can notify electronic identification schemes and CIR 2015/1502 [i.3] dealing with levels of assurance for notified electronic identification schemes gives only broad guidelines in relation to identity proofing, leaving significant room for variations in implementation (it is noted however that this CIR can be applied under the light of the LoA guidance, representing the consensus of the member states w.r.t. the technological state of the art and providing more technical guidance, see clause 5.2.1.7). The same trend can be seen in know-your-client (KYC) rules applicable pursuant to anti-money-laundering/terrorism financing regulations, and in the EU, the anti-money laundering directive now refers to eIDAS as well as 'nationally approved or authorised' eID schemes but contains no further guidelines as to how they should be implemented for KYC purposes.

5.2.1 EU

5.2.1.1 ETSI EN 319 411

5.2.1.1.1 Short description

Purpose and context: Issuance of certificates. Clause 6.2 provides security and policy requirements for registration of subject applying for a digital certificate (any type, including qualified).

ID type:

- natural person;
- natural person identified in association with a legal person;
- legal person;
- system or device operated by a natural person, or by/or on behalf of a legal person, or other organizational entity identified in association with a legal person.

Expected outputs: issuance of a certificate.

Sector: all sectors, including eIDAS seal, signature and web certificates.

Legal background: not applicable, but the document aims to covers eIDAS needs.

5.2.1.1.2 Attribute collection

Attributes to be collected: identity and any applicable attributes of the subject:

- natural person: full name (surname and given names) date and place of birth;
- natural person identified in association with a legal person: as above, full name and legal status of the associated legal person, any relevant existing registration information, affiliation of the natural person to the legal person, association with any attribute that would appear in O field of the certificate;
- legal person: full name of the organizational entity, association with any attribute that would appear in O field of the certificate;

- system or device operated by or on behalf of a legal person: identifier of the device, full name of the organizational entity, any relevant existing registration information, affiliation of the natural person to the legal person, association with any attribute that would appear in O field of the certificate, a nationally recognized identity number distinguish the organizational entity;

- system or device operated by a natural person: identifier of the device, a nationally recognized identity number to distinguish the natural person.

Type of evidence to be/that can be presented: direct evidence or an attestation, either paper or electronic documentation, from an appropriate and authorized source.

Type of presentation of the attributes: see type of evidence above.

5.2.1.1.3 Attribute validation

Determination that the ID attributes are valid (not expired, not revoked): no specification beyond the RA is required to validate their authenticity.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): no specification beyond the fact that documentation comes from an appropriate and authorized source.

5.2.1.1.4 Attribute binding

Face to face interactions or digital interactions are permitted as follows:

- For LCP: no specific requirement.

- For NCP: either directly by physical presence of the person (the subject is required to be witnessed in person unless a duly mandated subscriber represents the subject), or is required to checked indirectly using means which provides equivalent assurance to physical presence (e.g. registration documents electronically signed by a person trusted.

NOTE: For a legal person or a device or system, the check is done against a duly mandated subscriber.

- For QCP: as above but *"indirectly using means which provides equivalent assurance to physical presence"* needs to be *"using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence"*.

- For CA/B forum related CP: see reading sheet CA/B forum.

5.2.1.1.5 Requirements on the process

What needs to be done:

The TSP is required to verify the identity of the subscriber and subject, and is required to check that certificate request are accurate, authorized and complete according to the collected evidence or attestation of identity.

Why this needs to be done:

A TSP issuing certificate commits to certify verified information, in particular, the identity of the subject.

How this needs to be done:

The TSP is required to collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Verification of the subject's identity should be at time of registration by appropriate means.

The TSP should only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

Independence requirement: the subscriber and TSP organization entity should be separate entities.

Elements common to the whole process:

Possible security levels associated to one step or the whole process:

- With regard to ID proofing, the EN provides two basic sets of requirements, lightweight certificate policy (LCP) and normalized certificate policy (NCP) which requires additional controls to LCP. The CA/B forum PTC also adds details

Compliance measures implemented: the RA is a component of the TSP and the TSP ir required to fulfil general security requirements from ETSI EN 319 401 [i.9] (covering HR, network, ISMS, organization, etc., requirements), so that the RA inherits the ETSI EN 319 401 [i.9] requirements from the TSP.

Technical standards applied if any; ETSI EN 319 401 [i.9].

Security requirements: Yes

5.2.1.1.6 Reference material

Title	URL
ETSI EN 319 411-1 [i.10]: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".	https://www.etsi.org/standards-search%23search=EN319411-1#page=1&search=ETSI%20EN%20319%20411-1&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2021-02-15&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1
ETSI EN 319 411-2 [i.11]: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".	https://www.etsi.org/standards-search#search=EN319411-2

5.2.1.1.7 Reviewer note and conclusion

The ENs detail well what needs to be validated but do not provide specifications on how to do it (beyond physical presence or equivalent for NCP).

5.2.1.2 ETSI EN 319 521

5.2.1.2.1 Short description

Purpose and context: ETSI EN 319 521 [i.15] specifies generally applicable policy and security requirements for Electronic Registered Delivery Services Providers (ERDSP), including the services they provide (ERDSP and EU qualified ERDSP).

ID type: legal person and natural person.

Expected outputs: Electronic Registered Delivery (this covers sender and recipient identification).

Legal background: Norm is fit for eIDAS.

5.2.1.2.2 Attribute collection

Attributes to be collected: ERDS describes how sender and recipient are identified (including the attributes).

Type of evidence to be/that can be presented: left to the ERDSP (e.g. applicant's identity card or passport).

Type of presentation (of the attributes): left to the ERDSP.

5.2.1.2.3 Attribute validation:

Determination that the ID attributes are valid (not expired, not revoked): left to the ERDSP.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): left to the ERDSP.

5.2.1.2.4 Attribute binding

Face to face interactions or digital interactions, either directly or by relying on a third party:

a) by the physical presence of the natural person or of an authorized representative of the legal person; or

b) remotely, using electronic identification means, for which a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in Article 8 of the Regulation (EU) N° 910/2014 [i.1] with regard to the assurance levels 'substantial' or 'high'; or

c) by means of a certificate issued to the natural person or to an authorized representative of the legal person under NCP policy as defined in ETSI EN 319 411-1 [i.10], of a digital signature; or

d) by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalence of the assurance level should be confirmed by a conformity assessment body.

If the identification of the recipient is based on a digital signature, the signature validation precedes the handover of the user content.

5.2.1.2.5 Requirements on the process

What needs to be done:

The QERDSP verifies the identity of the sender and the recipient either directly or by relying on a third party.

How this needs to be done:

As indicated above in "Attribute binding".

Elements common to all steps:

Possible security levels associated to one step or the whole process: ERDSP and EU qualified ERDSP.

Compliance measures implemented and Technical standards applied if any:

- The TSP should fulfil general security requirements from ETSI EN 319 401 [i.9] (covering HR, network, ISMS, DRP, termination, organization, etc.).
- If the identification of the recipient is based on a QERDS internal process, the QERDSP should conduct the whole process in a secured and controlled environment. and all evidence of identification and consignment or handover process should be gathered and protected.

Other: The QERDSP appoints an identity verification officer in charge of ensuring that the actual processes conducted for verifying the identity of the sender and recipient are compliant with the initial identity verification process specified.

Security requirements: Yes (indirectly, by reference to ETSI EN 319 401 [i.9] or ETSI EN 319 411-2 [i.11]).

5.2.1.2.6 Reference material

Title	URL
ETSI EN 319 521 [i.15]: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Delivery Service Providers".	https://www.etsi.org/standards-search#search=EN319521

5.2.1.3 EN 419 241-1/ETSI TS 119 431-1

5.2.1.3.1 Short description

Purpose and context: the two standards specify requirements for TSP operating a (Q)SCD on behalf of signatories (or creator of seal), in the context of eIDAS. For such service, user enrolment (initial identification and beyond, authentication for day to day signature) is a crucial step to ensure the (sole) control on the signing key by the signatory. In particular, the mapping between an enrolled user and its signing certificate is key since the identification of the user through its signature, is made by the certificate.

ID type: natural and legal person.

Expected outputs: the two standards specify requirements for TSP operating a (Q)SCD on behalf of signatories (or creator of seal), in the context of eIDAS. For such service, user enrolment (initial identification and beyond, authentication for day to day signature) is a crucial step to ensure the (sole) control on the signing key by the signatory. In particular, the mapping between an enrolled user and its signing certificate is key since the identification of the user through its signature, is made by the certificate.

Sector: all sectors, private and public.

Legal background: eIDAS, signature creation service.

5.2.1.3.2 Attribute collection

Attributes to be collected: Not specified.

Type of evidence to be/that can be presented: eIDAS, signature creation service.

Type of presentation of the attributes: ETSI EN 319 411-1 [i.10] is recommended for guidance.

5.2.1.3.3 Attribute validation

Determination that the ID attributes are valid (not expired, not revoked): N/A.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): N/A.

Other checks implemented if any: there is a need to map the identity of enrolled subject with the subject certificate information (i.e. the certificate that will support the signature) and to ensure the enrolled subject has control on this certificate.

5.2.1.3.4 Attribute binding

Face to face interactions or digital interactions: no specification. ETSI EN 319 411-1 [i.10] is referred for guidance. A mapping between the applicant and its certificate is required (see above).

5.2.1.3.5 Requirements of the process

What needs to be done: secure user's enrolment, mapping between the identity of enrolled subject and the subject certificate information.

Why this needs to be done : to ensure the (sole) control on the signing key by the right subject and ensure the correct identification through the right certificate.

How this needs to be done: a series of security requirements are specified. For the user's identification reference is made to CIR 1502 [i.3] (see related reading sheet for more information).

Elements common to the whole process:

- Possible security levels associated to one step or the whole process: the TSP can host a SCD or a QSCD, specific requirements are provided for the later case.
- Compliance measures implemented: No.

- Technical standards applied if any; ETSI EN 319 411-1 [i.10] and CIR 1502 [i.3].

Security requirements: Yes.

5.2.1.3.6 Reference material

Title	URL
ETSI TS 119 431-1 [i.19] (V1.1.1) (2018-12), "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev". EN 419 241-1 [i.40]: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements".	https://www.etsi.org/standards-search#page=1&search=EN%20319%20431-1&title=1&etsiNumber=1&content=1&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2021-02-15&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1

5.2.1.3.7 Reviewer note and conclusion

The identity proofing is not the central scope of the norms but is a crucial component of the service.

Important notions are covered such as eID means linking, certificate linking and eID means provision.

The two first topic are very relevant for the TR but are not sufficiently developed in the norms; references are made to ETSI EN 319 411-1 [i.10], itself not complete enough in matter of identity proofing.

5.2.1.4 Regulation 2019/1157 on strengthening the security of identity cards

5.2.1.4.1 Short description

Purpose and context: this regulation introduces reinforced security standards that should provide sufficient guarantees to public authorities and private entities to enable them to rely on the authenticity of identity cards when used by Union citizens for identification purposes. This Regulation does not affect the use of identity cards and residence documents with an eID function by Member States for other purposes, nor does it affect the rules laid down in eIDAS. Security features are necessary to verify if a document is authentic and to establish the identity of a person (i.e. the inclusion of such biometric identifiers).

Secure travel and identity documents are crucial whenever it is necessary to establish without doubt a person's identity. Issuing authentic and secure identity cards requires a reliable identity registration process and secure 'breeder' documents (ndrl: i.e. source documents like birth certificates) to support the application process. There is a need to make breeder documents less vulnerable to fraud.

ICAO Documents 9303 [i.87] which ensures global interoperability, including in relation to machine readability and use of visual inspection should be considered. The formats used for the secure storage medium should be interoperable, including in respect of automated border crossing points.

Each Member State designates one body having responsibility for printing identity cards, and one body having responsibility for printing residence cards.

- ID type: natural persons;
- Expected outputs:
  - identity cards issued by Member States to their own nationals;
  - registration certificates;
  - residence cards.
- Sector: official identity document listed above can be used by public authorities and private entities

NOTE: Access to biometrics is limited by issuing states to entities they allow to do so.

- Legal background: Directive 2004/38/EC [i.20] (free movement)

5.2.1.4.2 Attribute collection

Attributes to be collected: The data elements included on identity cards should comply with the specifications set out in ICAO 9303 [i.87]:

- the name of the state or organization responsible for issuing the travel document;
- type or designation of the document;
- full name of the holder, as identified by the issuing State or organization (See ICAO 9303 [i.87]);
- predominant component(s) of the name of the holder;
- secondary component(s) of the name of the holder;
- sex of the holder;
- nationality;
- date of birth;
- document number;
- date of expiry;
- signature or usual mark of the holder;
- a portrait of the holder.

Identity cards should include a highly secure storage medium containing a facial image of the holder of the card and two fingerprints:

- Type of evidence to be/that can be presented: secure 'breeder' documents (ndrl: i.e. source documents) to support the application process. There is a need to make breeder documents less vulnerable to fraud. However, Member States retain full responsibility for the breeder documents and actually producing and issuing travel documents (that is why discrepancies will continue to exist with regard to the level of security of the different states eID).
- Type of presentation (of the attributes): the biometric identifiers are collected solely by qualified and duly authorized staff designated by the authorities responsible for issuing identity cards or residence cards for the purpose of being integrated into the highly secure storage medium.

With a view to ensuring the consistency of biometric identifiers with the identity of the applicant, the applicant should **appear in person** at least once during the issuance process for each application.

5.2.1.4.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): see discussion on breeder documents above.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): the Regulation only asks secure "breeder" documents. This is left to the issuing states (see discussion above).

5.2.1.4.4 Attribute binding

Face to face interactions: with a view to ensuring the consistency of biometric identifiers with the identity of the applicant, the applicant appears in person at least once during the issuance process for each application.

Digital interactions: not specified.

5.2.1.4.5 Requirement on the process

What needs to be done, why and how:

The Regulation only provides security requirements for the identity cards and left the process (and its securisation) to the Member States.

Elements common to all steps:

Possible security levels associated to one step or the whole process: not applicable.

Compliance measures implemented: Biometric data stored for the purpose of the personalization of identity cards or residence documents should be kept in a highly secure manner and only until the date of collection of the document and kept maximum 90 days. There are also the usual GDPR prescriptions (right to access personal data, ask modification, need to know basis, information etc.), as well as prescriptions for access to disabled persons.

Technical standards applied if any; the Commission is entitled to establish, by means of implementing acts, additional technical specifications (still to come).

Security requirements: No (only for the identity cards themselves, not on the process left to the Member State custody).

5.2.1.4.6 Reference material

Title	URL
Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement [i.41]	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32019R1157

5.2.1.4.7 Reviewer note and conclusion

The Regulation defines the attributes that can be found in eID cards and assigns the responsibility of the security to the issuing States. An identity proofing process can use and rely on these attributes:

- anybody can read the identity information printing on eID cards and visually assess the genuineness of the document;
- any entity equipped with an OCR reader can read the MRZ zone;
- any entity equipped with a contactless reader can read the identity information stored in the chip and validate the issuing state signature on this information; and
- any entitled authority can read the biometric to compare with the owner of the eID cards (this is generally limited to foreign member states that are allowed to do so by the issuing member state, as well as entitled organization within the issuing states, such as police, border controls, etc.).

In addition, some prescriptions are of interest here, such as the minimal set of data to be considered, the physical presence for collecting fingerprints, etc.

5.2.1.5 CIR EU 2015/1501

5.2.1.5.1 Short description

Purpose and context: Commission Implementing Regulation on the interoperability framework pursuant to Article 12(8) of eIDAS (i.e. Cooperation and interoperability with notified national electronic identification schemes).

ID type: natural and legal person.

Expected outputs: establishing secure and interoperable networks of nodes to support the transmission of person identification data and setting the collaboration between member states to do so, including the definition of minimum set of person identification data uniquely representing a natural or a legal person.

Sector: public administrations.

Legal background: eIDAS (see above).

5.2.1.5.2 Attribute collection

Attributes to be collected:

The minimum data set for a natural person contains all of the following mandatory attributes:

a) current family name(s);

b) current first name(s);

c) date of birth;

d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

The minimum data set for a natural person may contain one or more of the following additional attributes:

a) first name(s) and family name(s) at birth;

b) place of birth;

c) current address;

d) gender.

The minimum data set for a legal person contains all of the following mandatory attributes:

a) current legal name;

b) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

The minimum data set for a legal person may contain one or more of the following additional attributes:

a) current address;

b) VAT registration number;

c) tax reference number;

d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council [i.21] (1);

e) Legal Entity Identifier referred to in Commission Implementing Regulation (EU) No 1247/2012 [i.46] (2);

f) Economic Operator Registration and Identification referred to in Commission Implementing Regulation (EU) No 1352/2013 [i.47] (3);

g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012 [i.48] (4).

Type of evidence to be/that can be presented: N/A.

Type of presentation of the attributes: N/A.

5.2.1.5.3 Attribute validation

Determination that the ID attributes are valid (not expired, not revoked): N/A

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): N/A

5.2.1.5.4 Attribute binding

Not covered by the Commission Implementing Regulation.

5.2.1.5.5 Requirements of the process

Requirements on the process

What needs to be done: although the CIR is not about identity proofing it provides ***conditions*** for member states to exchange person identification data i.e. the member states establishes a secure network to exchange person identification data ensuring data privacy and confidentiality, integrity and authenticity, etc. (e.g. follow ISO/IEC 27001 [i.24]). The interoperability is ensured by harmonisation of metadata, minimal set of person identification data, etc. Elements for collaboration and dispute resolution are also specified.

Technical standards applied if any; ISO/IEC 27001 [i.24].

Security requirements: Yes

5.2.1.5.6 Reference material

Title	URL
Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) [i.2]	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0001

5.2.1.6 CIR (EU) 2015/1502

5.2.1.6.1 Short description

Purpose and context: Commission Implementing Regulation setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

This is the leading eIDAS implementation document for identity-proofing processes applied to electronic identification means (but not eIDAS trust services), providing a detailed description of the various steps required to ensure a given level of assurance for electronic identification means. Note that an official line-by-line guidance document [i.22] has been released by the eIDAS Cooperation Network in relation to CIR 2015/1502 [i.3], also presented in the present document.

ID type: natural person; legal person; and natural person acting on behalf of a legal person.

Expected outputs: CIR 2015/1502 [i.3] is the reference document for the assessment of pre-notified electronic identification schemes under eIDAS. In short, all notified electronic identification means have been benchmarked and assessed against the applicable assurance level specifications of CIR 2015/1502 [i.3] as part of the so-called 'peer review'.

Legal background: CIR 2015/1502 [i.3] is an EU regulation implementing article 8 of Regulation 910/2014 (eIDAS) [i.1].

5.2.1.6.2 Attribute collection

Attributes to be collected:

Not applicable - CIR 2015/1502 [i.3] does not discuss which attributes are needed or required as this is a matter primarily dealt with by CIR 2015/1501 [i.2], also presented in the present document. Note however that, for legal persons, CIR 2015/1502 [i.3] mentions the legal person's name, legal form, and (if applicable) its registration number.

Type of evidence to be/that can be presented: CIR 2015/1502 [i.3] generally refers to 'data, information and/or evidence that can be used to prove identity' provided by an 'authoritative source which can take many forms, such as registries, documents, bodies inter alia'. No further details are given.

Type of presentation of the attributes: CIR 2015/1502 [i.3] does not directly discuss the type of presentation or communication channel used for the attribute evidence.

5.2.1.6.3 Attribute validation

Determination that the ID attributes are valid (not expired, not revoked): N/A

Determination that the evidence is genuine (issued by recognized independent/authoritative sources):

Natural persons		
LoA Low	**LoA Substantial**	**LoA High**
The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.	Same as Low + the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person; and steps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence.	Same as Substantial + Where the person has been verified to be in possession of photo or biometric identification evidence recognized by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source.
Legal persons		
The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source.	Same as Low + the claimed identity of the legal person is demonstrated on the basis of evidence recognized by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable) its registration number; and the evidence is checked to determine whether it is genuine, or known to exist according to an authoritative source, where the inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector.	Same as Substantial + the claimed identity of the legal person is demonstrated on the basis of evidence recognized by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context; and the evidence is checked to determine that it is valid according to an authoritative source.

5.2.1.6.4 Attribute binding

Table 1

Natural persons		
LoA Low	**LoA Substantial**	**LoA High**
It may be assumed that the person claiming the identity is one and the same.	Same as Low + the person has been verified to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made; or an identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it.	Same as Substantial + The applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source.
Legal persons (including binding between the electronic identification means of natural and legal persons)		
The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.	Same as Low + Steps have been taken to minimize the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents.	Same as Substantial.
The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above. The binding has been established on the basis of nationally recognized procedures. The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.	The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high. The binding has been established on the basis of nationally recognized procedures, which resulted in the registration of the binding in an authoritative source. The binding has been verified on the basis of information from an authoritative source.	The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high. The binding has been verified on the basis of a unique identifier representing the legal person used in the national context; and on the basis of information uniquely representing the natural person from an authoritative source.

5.2.1.6.5 Requirements of the process

Requirements on the process

CIR 2015/1502 [i.3] also contains LoA-dependent provisions dealing with the characteristics and design of electronic management means, their issuance, delivery and activation, as well as renewal and replacement. In addition, specific authentication requirement are set out, linking the ability to defeat moderate/high potential attacks to the Substantial/high LoA.

CIR 2015/1502 [i.3] also contains a number of general provisions on security management, record keeping, facilities, technical controls and staff as well as compliance and audit matters, but these tend to be defined in fairly general terms, which although still LoA-dependent, are not fully differentiated.

Security requirements: Yes

5.2.1.6.6 Reference material

Title	URL
Commission Implementing Regulation setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002

5.2.1.6.7 Reviewer note and conclusion

This is of course an extremely relevant document for the present document, providing substantially more information on identity-proofing requirements for eIDAS electronic identification means than what currently exists for eIDAS Trust services.

The importance of CIR 2015/1502 [i.3] cannot be overstated as it has considerable liability implications for notifying States in respect of electronic identification means that would fail to 'uniquely represent the person in question in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in CIR 2015/1502 [i.3], article 11.1 of eIDAS.

It should be noted, however, that contrary to NIST 800-63-3 [i.36], CIR 2015/1502 [i.3] offers LoA requirements that cover all key aspects of the management of electronic identification means and do not apply separately to the identity-proofing phase.

5.2.1.7 Guidance for the application of the levels of assurance which support the eIDAS Regulation

5.2.1.7.1 Short description

Purpose & context: The Guidance [i.22] is an interpretation document of the eIDAS Cooperation Network published in connection with the evaluation of digital identity schemes notified to the European Commission as part of the peer-review process. It interprets Implementing Regulation 2015/1502 [i.3] setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of eIDAS ('Regulation 2015/1502') and can only be read in conjunction with it. In line with Regulation 2015/1502, the Guidance applies criteria that are LoA-tiered in accordance with the eIDAS Low, Substantial and High LoA requirements.

The Guidance [i.22] provides illustrations and security considerations meant to apply to a large variety of situations, country infrastructures and environments for the assessment of pre-notified electronic identification schemes. It aims to offer a line-by-line reasoned commentary of Regulation 2015/1502 [i.3] with a number of good practice examples illustrating 'how things could be done' and viewed as meeting a verifyer's reasonable expectations, rather than detailing prescriptive steps for the deployment of identity-proofing processes.

ID type: as per Regulation 2015/1502 [i.3] - The Guidance [i.22] applies to both natural and legal persons, although in practice the Guidance appears to primarily focus on natural persons.

Expected outputs: The Guidance [i.22] purports to offer practical guidelines for, and greater visibility on, the key requirements needed for the assessment of digital identity solutions notified to the EU Commission as part of the eIDAS regulation [i.1].

Sector: The Guidance [i.22] applies to electronic identification schemes presented by Members States - it is up to each presenting Member State to determine for which sector(s) the electronic identification scheme should be used.

Legal background: Although not a binding document, the Guidance [i.22] is part of the eIDAS environment and is publicly available.

5.2.1.7.2 Attribute collection

Attributes to be collected: The Guidance [i.22] does not address which attributes are to be collected - this is dealt with by Implementation Regulation 2015/1501 [i.2] on the eIDAS interoperability framework.

Type of evidence to be/that can be presented: The Guidance [i.22] offers a definition of 'Authoritative sources' - a term used in the eIDAS regulation [i.1]

Type of presentation: The Guidance [i.22] highlights the need to have secure communication channels as well as the risks involved in the communication of attributes and states that *'presentation attacks pose a significant risk to identity proofing based on video-based communication channels as well as face to face sessions'.*

5.2.1.7.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked), **the Guidance [i.22]** offers a detailed LoA-tiered description of the various validity checks to be implemented for physical as well as electronic evidence. For example, for electronic evidence, the Guidance [i.22] suggests that verification should whenever possible be based on automatic checks (for example via digital signatures or by online verification of the evidence against an authoritative source).

Determination that the evidence is genuine (issued by recognized independent/authoritative sources), the Guidance [i.22] offers a detailed LoA-tiered description of the various genuineness checks to be implemented for physical as well as electronic evidence.

5.2.1.7.4 Attribute binding

The Guidance [i.22] offers a detailed LoA-tiered description of the various checks to be implemented to link the ID attributes to the applicant. It stresses that this is commonly achieved through physical comparison of the applicant to their document and also includes the necessity to consider presentation attacks. Examples for presentation attacks include masks, makeup or (where applicable) digital manipulations like manipulations of ID documents or biometric characteristics, which apply to scenarios with physical presence as well as remote verification procedures.

The Guidance [i.22] suggests that a practical outcome-based test to be applied is the false-match/false positive rate - meaning that processes showing a low false-match/false positive rate should be deemed sufficient. For example, for remote identity proofing and verification processes aiming for a High LoA, it stresses the need to demonstrate that possible manipulations of a video stream by attackers (e.g. real-time re-enactment, synthetic faces) relevant for this level of assurance can be reliably detected with high certainty. A way to show this is to demonstrate the resistance against attackers with high attack potential.

5.2.1.7.5 Requirements of the process

Process-related aspects (what needs to be done and why; how processes are implemented; security levels associated with the processes) are not addressed as specific chapters of the Guidance [i.22] but can be found as comments in relation to specific provisions of the 2015/1502 [i.3] Regulation.

The Guidance [i.22] also makes a number of references to ISO standards:

- ISO/IEC 19989-3 [i.23] for terminology;
- ISO/IEC 27001 [i.24] on requirements;
- ISO/IEC 15408 [i.25] "Information technology - Security techniques - Evaluation criteria for IT security" and ISO/IEC 18045 [i.26] "Information technology - Security techniques - Methodology for IT security evaluation".
- ISO 19011 [i.27] on auditing management systems;
- ISO/IEC 29115 [i.30] on "Information technology - Security techniques - Evaluation criteria for IT security;
- ISO/IEC 27007 [i.29] for external audits.

The Guidance [i.22] also refers to the Common Methodology for Information Technology Security Evaluation [i.44].

Lastly, the Guidance [i.22] contains no or very limited provisions on the following:

- description of customary compliance measures (traceable documentation, access policy, personel training and authorization, premises security, etc.); and
- description of customary auditing processes.

The Guidance [i.22] is currently under review and a number of changes have been suggested, notably to deal with 'full-remote' onboarding solutions as well as reflect the development of biometric identity-verification solutions which are having a significant impact on identity-proofing guidelines.

In line with the BSI approach (see Technical Guideline TR-03147 [i.64]), the Guidance [i.22] now aims to identify a number of dimensions that should be taken into account for identity proofing processes - these are:

- Reliable verification of the authoritative source(s) and the data provided by it.
- Correct collection of all necessary data.
- Reliable comparison of the biometric data of a person with data provided by the authoritative source(s), i.e. the biometric data if available.
- Secure communication channels.
- Integrity of the underlying processes.

The Guidance [i.22] does not provide explicit recommendations and is therefore not a framework against which conformity with a given LoA can be assessed. In addition, its non-binding status somewhat limit its.

5.2.1.7.6 Reference material

Title	URL
Guidance for the application of the levels of assurance which support the eIDAS Regulation Published but undated (January 2018?). Currently under review [i.22]	https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.pdf

5.2.1.7.7 Reviewer note and conclusion

The Guidance [i.22] is a highly relevant document for the present document in that it offers practical guidelines for identity proofing processes used in connection with the assessment of eID schemes notified under the eIDAS regulation [i.1], but does not extend or relate to eIDAS trust services. However, the current status of its revision process is unclear.

5.2.1.8 ENISA Repot: eIDAS COMPLIANT eID SOLUTIONS

5.2.1.8.1 Short description

Purpose and context: This report provides an overview of the legislative framework under eIDAS for electronic identification, presents the landscape of notified and pre-notified eID schemes and identifies key trends in the electronic identification field. Moreover, it discusses preliminary security considerations and recommendations related to the underlying technologies used for eID means.

The study also analyses a set of documents, in common to the present study:

- ISO/IEC 29115 [i.30].
- NIST SP 800-63 - Digital Identity Guidelines (multipart [i.43], [i.44], [i.45]).

CEN TR 419010 [i.51] "Framework for standardization of signature" - extended structure including electronic identification and authentication, analyses the impact of CIR 2015/1501 [i.2] and 2015/1502 [i.3] on the already published standards for electronic signature and if updates or further standards for identification and authentication are needed.

The report points the following **trends:**

- more eID means are based on mobile phones nowadays;
- biometrics are used more and more;
- with regard to Self-Sovereign Identities: trust in these Verifiable Claims is necessary for public and private services. Underlying this trust is the question of where the Personally Identifiable Information comes from and how it was imported. The maturity of Self-Sovereign Identities solutions and the amount of services using this technology will only grow once this question is addressed.

The report points the following **needs:**

- there are currently no standards or detailed requirements available to help identify how providers assess their process's compliance with a given Level of Assurance (LoA) based on the classification scale of Regulation CIR (EU) 2015/1502 [i.3]. However, remote identification requirements for each LoA are currently examined and expected to be formalized in future updates of the document "Guidance for the application of the Levels of Assurance which support the eIDAS Regulation" [i.1], as additional guidance and standardization is needed in this area;
- idem for remote identification processes for trust services (scope of the present document);
- specific certification scheme for devices used within eID means for LoA High;
- need to consider users' privacy;
- in the "related guidance for the application of the levels of assurance which support the eIDAS Regulation", best practices about trained and skilled staff are provided in the document, such as possessing knowledge of document design, security features, watermarks and printing techniques, and being able to identify forged and counterfeit documents. However, the current version of the guidance document [i.22] does not elaborate on best practices and requirements regarding remote identity proofing (performed for instance with videoconference or facial recognition), but a subgroup of the Cooperation Network is currently working on adding parts related to remote identity proofing.

ID type: natural and legal person.

Expected outputs: eIDAS eID means.

Sector: public sector.

Legal background: eIDAS.

5.2.1.8.2 Attribute collection

This is not addressed directly but by reference to CIR 1502 [i.3] (see related RS).

5.2.1.8.3 Attribute validation

This is not addressed directly but by reference to CIR or CIR 1502 [i.3] (see related RS). This is also addressed by reference to Peer Review feedbacks that have highlighted complexity for the verification and validation of identity documents, especially in the case of foreign identity documents that are used for a request of an eID (as it is the case for some of the already notified eID schemes). It recommends:

- International databases such as the Schengen Information System (SIS) or Interpol databases, PRADO [i.86] database for verification of optical/physical security features of identity documents, iFADO (Intranet False and Authentic Documents Online) should be used to confirm the documents' validity.
- If the verification is performed physically or if the identification is performed solely based on the picture of a document, a professional and trained agent should assess the validity of the document.

5.2.1.8.4 Attribute binding

This is not addressed directly but by reference to CIR 1502 [i.3] (see related RS), and to the related guidance for the application of the levels of assurance which support the eIDAS Regulation [i.1] (see related RS). This is also addressed by reference to Peer Review feedbacks.

Peer review feedbacks provide interesting warning for remote mapping (with regard to possible attacks, etc.).

The report also refers to the case of an identity proofing using a qualified electronic signature, it is relevant to note that Regulation eIDAS (Article 24) [i.1] allows the use of an eID means complying at least with LoA Substantial or High, but only if there was a physical presence during the enrolment. Therefore, in the case of identity proofing for LoA High, some complexity could arise as a qualified signature performed with a qualified certificate issued with a LoA Substantial eID means may not be accepted as proof of identity. This consideration is taken into account when relevant.

5.2.1.8.5 Requirements of the process

This is not addressed directly but by reference to CIR 1502 [i.3] (see related RS) and peer reviews. Peer review feedbacks provide interesting recommendations.

Security requirements: Not directly. But the annexes of the study analyses different tools like face recognition, etc. and their applicability to identity proofing process. This is interesting for ETSI DTS/ESI-0019461 [i.50].

The report points the following security consideration:

- a single biometric modality poses certain weaknesses, multimodal biometric systems and behavioural biometrics are gaining traction, However, it should be noted that behavioural biometrics are not among the authentication factors authorized for eID schemes according to CIR 2015/1502 [i.3].
- security flaws or vulnerabilities in the implementation of the interoperability framework (note : of the eIDAS eIDs) could endanger the whole electronic identification process.
- specifc elements raised above in clauses "attribute validation" and "mapping".

5.2.1.7.6 Reference material

Title	URL
ENISA Report -eIDAS COMPLIANT eID SOLUTIONS [i.53] Security Considerations and the Role of ENISA March 2020	https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions

5.2.1.7.7 Reviewer note and conclusion

ENISA report [i.53] identifies trends and points to needs and security consideration that the present study needs to corroborate and consider in its analyse and conclusions. It also provides interesting inputs for ETSI DTS/ESI-0019461 [i.50].

5.2.2 International

5.2.2.1 Draft provisions on the use and cross-border recognition of identity management and trust services

5.2.2.1.1 Short description:

Purpose and context: The Draft Provisions [i.54] and [i.55] intend to facilitate the international recognition of digital ID schemes as well as electronic trust services. They effectively replicate the eIDAS structure in a wider international context but are of limited value within the EU/EEA area where the eIDAS regulation [i.1] applies.

The Draft Provisions [i.54] and [i.55] draw heavily on the *Terms and concepts relevant to identity management and trust services* document also prepared by the United Commission on International Trade Law. It also defines the collection of attributes, the carrying out identity proofing and verifications processes and the binding of identity credentials to the applicant as key parts of the identity management responsibilities. However, it does not elaborate as to how these should be implemented in practice.

The draft provisions [i.54] and [i.55] on the use and cross-border recognition of identity management and trust services relies on the core notion of 'reliability' which is a key requirement for the cross-border recognition of identity management systems or trust services as well as lists factors deemed relevant to assess reliably. It should however be noted that these are defined in very general terms only and in a non-prescriptive manner. Guidelines in this respect only make general references to 'recognized international standards and procedures, including level of assurance framework', but do not elaborate further on these and remain indicative only. The official designation of a reliable identity management system or trust service, pursuant to the Draft Provisions, is required to be consistent with recognized international standards, including level of reliability frameworks.

Although work on the Draft Provisions [i.54] and [i.55] has been on-going for some time, it should be noted that the current version contains numerous paragraphs where alternatives and options are offered, therefore leaving a significant degree of uncertainty as to what their final outcome will be.

ID type: The Draft Provisions [i.54] and [i.55] are intended to apply to both natural and legal persons, but it is worth noting a suggested alternative is that they also apply to 'objects'.

Expected outputs: Although not directly specified in the Draft Provisions [i.54] and [i.55], the expected outcome is an international treaty subject to ratification by the member States of the United Nations.

Sector: All sectors - the Draft Provisions [i.54] and [i.55] are not confined to any specific industry sector and are intended to generally apply to any situation where a digital identity management or trust service can be used but are clearly focusing on cross-border situations where the international recognition is a key concern.

Legal background: The Draft Provisions [i.54] and [i.55] are a 2015 initiative of the United Commission on International Trade Law.

5.2.2.1.2 Attribute collection

Attributes to be collected: No specific provision.

Type of evidence to be/that can be presented: No specific provisions.

Type of presentation: No specific provisions.

5.2.2.1.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): No specific provision.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): No specific provisions.

5.2.2.1.4 Attribute binding

No specific provisions.

5.2.2.1.5 Requirements of the process

The Draft Provisions [i.54] and [i.55] broadly state how the identity management service is provided (identity-proofing and verification steps), but contain no or very limited provisions on any of the following:

- what needs to be done and why in relation to identity proofing;
- how identity-proofing processes are implemented in practice;
- possible security levels associated to one step or the whole identity-proofing process;

- description of customary compliance measures implemented (traceable documentation, access policy, personnel training and autorisation, premises security, etc.);
- description of customary technical standards applied if any;
- description of customary auditing processes if any.

Security requirements: No.

5.2.2.1.6 Reference material

Title	URL
UNCITRAL Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services A/CN.9/WG.IV/WP.168 Working Group IV (Electronic Commerce) Sixtieth session. New York, 6-9 April 20 [i.54]	https://undocs.org/en/A/CN.9/WG.IV/WP.162
UNICITRAL Draft Provisions on the Use and Cross border Recognition of Identity Management and Trust Services. Submission by the World Bank A/CN.9/WG.IV/WP.163 Working Group IV (Electronic Commerce) Sixtieth session. New York, 6-9 April 20 [i.55]	https://undocs.org/en/A/CN.9/WG.IV/WP.163

5.2.2.1.7 Reviewer note and conclusion

The Draft Provisions [i.54] and [i.55] in their current version are of limited use for the present document and should rather be viewed as an indication of a possible/likely development of public international law on the international recognition of identity management and trust services.

5.2.2.2 ISO/IEC 29115 on entity authentication assurance framework

5.2.2.2.1 Short description

Purpose and context: ISO/IEC 29115 [i.30] specifies levels of assurance for entity authentication and forms the main basis for the eIDAS assurance level definitions. The standard is "outcome based" in that various mechanisms may contribute together and as alternatives to achieve a given level. The standard [i.30] defines an "enrolment phase" consisting of application and initiation, identity proofing and identity information verification, record-keeping and recording, and registration. Along with other phases, this is subject to management and organizational requirements. As for ISO/IEC 29003 [i.16], the enrolment phase is defined as consisting of the processes application and initiation, identity proofing, identity information verification, and record-keeping/recording. Identity proofing and verification are described in general terms including a table for objective description, controls, and method of processing (local or remote). The only notable requirement is that LoA4 (very high) requires local processing, meaning personal appearance. Likely, this is because the document is old and thus cannot consider new technology for remote reading of identity documents. The management and organizational considerations clause has some requirements that can be considered by the present study, but stated at a very high level. The threats and controls clause is more specific on threats and countermeasures and should be consulted for ETSI DTS/ESI-0019461 [i.50].

ID type: "Entity" is used as a term, which may be natural person or some other entity.

Expected outputs: Identity proofing and verification ends up with an identity issued at a defined LoA.

Sector: The standard [i.30] is sector neutral but the statement is that it "is intended to be used principally by Credential Service Providers (CSPs) and by others having an interest in their services (e.g. relying parties, assessors and auditors of those services)".

Legal background: The document [i.30] is an approved ISO/IEC standard. It is fairly widely referred to.

5.2.2.2.2 Attribute collection

Attributes to be collected: The document [i.30] is not specific on attributes to be collected.

Type of evidence to be/that can be presented: Only mentioned in generic terms as identity documents and such.

Type of presentation (of the attributes): Mentioned only in general terms as remote or local (physical presence).

5.2.2.2.3 Attribute validation

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): Ranges from self-claimed at LoA1 through use of an "authoritative source" at LoA2, to authoritative source plus identity information verification at LoA3, and multiple authoritative sources plus identity information verification plus in-person appearance at LoA4.

Determination that the ID attribute are valid (not expired, not revoked): Same as previous.

5.2.2.2.4 Attribute binding

The expected result is an identity credential that is bound to certain information about the entity. The credential may be a certificate.

5.2.2.2.5 Requirements of the process

Identity proofing corresponds to the enrolment phase as defined by the standard, consisting of the processes application and initiation, identity proofing, identity information verification, and record-keeping/recording. The processes are described in very generic terms as is appropriate for a framework standard. The same goes for the descriptions of management and organizational considerations, which lists and briefly describes certain elements that are to be considered.

Security requirements:

Clause 10 of ISO/IEC 29115 [i.30] lists threats and required controls to achieve the different LoAs. This is relevant input to the work in ETSI/ESI but as the standard is fairly old, it should be used with some care.

5.2.2.2.6 Reference material

Title	URL
ISO/IEC 29115 [i.30]: "Information technology -- Security techniques -- Entity authentication assurance framework" First edition April 2013	https://www.iso.org/standard/45138.html

5.2.2.2.7 Reviewer note and conclusion

Likely, the standard does not add that much to the work in this study, but one should consider checking out requirements for compliance. Except that the "local only" requirement for LoA4 is outdated. Instead of 4 levels, one should start from the 3 levels of ISO/IEC 29003 [i.16], or even from 2 levels.

5.2.2.3 ISO/IEC 29003 on Identity proofing

5.2.2.3.1 Short description

Purpose and context: The standard relates to the ISO/IEC 24760 series [i.122] that specifies a general framework for identity management, and ISO/IEC 29115 [i.30], which specifies levels of assurance for entity authentication. The standard gives guidelines for identity proofing of a person (meaning natural person) and specifies levels of identity proofing and requirements to achieve these levels. Overall, the standard defines terms, concepts, and what it is covered by an identity proofing function. An identity proofing includes steps to collect the proofing information, determine the veracity of identifying attributes towards defined objectives, determine that the identifying attributes meet the required Level of Identity Proofing (LoIP), and bind the subject to the claimed identifying attributes. The standard defines three LoIP (LoIP 1 - low, LoIP 2 - moderate, LoIP 3- high) in very broad terms. A documented identity proofing policy is required by the standard, and minimum requirements for content are stated. Some requirements, in broad sense, for achieving a given LoIP are stated. An annex provides examples from various countries on identifying attributes and authoritative and corroborative sources of the information, and examples of binding person to identity information with achieved LoIA, Another annex provides information on contra-indications and fraud detection, meaning ways to detect attempts at attacking the identity proofing.

ID type: natural persons.

Expected outputs: Identity proofing according to the standard should result in an identity verified to a defined LoIA. How this identity is represented, e.g. means of authentication, is not mentioned.

Sector: The standard is sector neutral. The introduction merely mentions "a number of industry and government organizations" and support "across supply chains and global commons".

Legal background: ISO/IEC 29003 [i.16] is a technical specification and not a full ISO standard. It may be adopted as national standard by national bodies, but no information exists on this issue.

5.2.2.3.2 Attribute collection

Attributes to be collected: The document defines identifying attributes as one or more attributes that, when combined, uniquely identifies the subject in a context. Then, examples of such attributes are given. The document also defines supporting attributes as attributes that contribute to identity proofing (but not to unique identification) and gives some examples of such attributes.

Type of evidence to be/that can be presented: Only mentioned in generic terms with some examples in an annex.

Type of presentation (of the attributes): Mentioned only in general terms, e.g. physical presence, over the phone, or online.

5.2.2.3.3 Attribute validation

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): For higher LoIA, such check is needed. Only described in rather abstract terms, plus annex with examples.

Determination that the ID attribute are valid (not expired, not revoked): Same as previous.

5.2.2.3.4 Attribute binding

Again abstract terms, but LoIP states that at LoIP 1 the subject is assumed to be bound to the identity, LoIP 2 the subject has some binding to the identity, LoIP 3 the subject has a strong binding to the identity.

5.2.2.3.5 Requirements of the process

The standard is mainly a source of definitions and concepts. This includes definition of some processes that are needed but not much on requirements to the processes.

The policy requirements stated and the generic concepts defined may be used as a basis in ETSI DTS/ESI-0019461 [i.50].

Security requirements:

There is not much on security but the standard's Annex B has material on contra-indications and fraud detection.

5.2.2.3.6 Reference material

Title	URL
ISO/IEC 29003 [i.16]: "Information technology -- Security techniques -- Identity proofing". First edition March 2018	https://www.iso.org/standard/62290.html

5.2.2.3.7 Reviewer note and conclusion

As this is an existing technical specification, this study should use this as a starting point for ETSI DTS/ESI-0019461 [i.50] together with ETSI EN 319 401 [i.9]. That is the definitions and concepts, possibly the LoIAs, and the policy requirements.

5.2.2.4 ISO/IEC 30107 on biometric presentation attack detection

5.2.2.4.1 Short description

Purpose and context: The standard part 1 [i.32] sets up a framework for detection of biometric presentation attacks, meaning attacks specifically on the capture of biometrics at the point of presentation. Attack detection is to be automated. Part 2 [i.31] defines data formats for conveying mechanisms used in biometric presentation attack detection and the results from applying the mechanisms. Part 3 [i.118] establishes principles and methods for performance assessment, reporting of testing results, and classification of known attack types (informative annex). Part 4 [i.28] profiles part 3 [i.118] specifically for testing of biometric presentation attack detection on mobile devices where biometric presentation is done on the mobile.

ID type: biometrics is only relevant for natural persons.

Expected outputs: through testing and reporting, the quality of a biometric capture solution can be measured.

Sector: the standard is sector neutral and is not targeted at specific use cases for biometrics.

Legal background: the document is an approved ISO/IEC standard.

5.2.2.4.2 Attribute collection

Attribute collection is out of scope of this standard. It is only about security of biometrics systems.

5.2.2.4.3 Attribute validation

Attribute validation is also out of scope, except validation that captured biometric information is correct.

5.2.2.4.4 Attribute binding

This is out of scope of the standard.

5.2.2.4.5 Requirements of the process

The standard is important when biometric mechanisms are used in identity proofing as it describes attacks and countermeasures in place for biometric systems.

Security requirements:

The standard describes and categorizes types of attacks and countermeasures and specifies how to measure reliability of the results from specific solutions.

5.2.2.4.6 Reference material

Title	URL
ISO/IEC 30107: "Information technology -- Biometric presentation attack detection".	
Part 1: Framework (first edition, January 2016) [i.32]	https://www.iso.org/standard/53227.html
Part 2: Data formats (first edition, December 2017) [i.31]	https://www.iso.org/standard/67380.html
Part 3: Testing and reporting (first edition, September 2017) [i.118]	https://www.iso.org/standard/67381.html
Part 4: Profile for testing of mobile devices (first edition, June 2020) [i.28]	https://www.iso.org/standard/75301.html
Other sources of biometrics attack detection and use of biometrics:	
• Biometrics institute	https://www.biometricsinstitute.org/
• Morphing Attack Detection (MAD) project	https://christoph-busch.de/projects-mad.html

5.2.2.5 CA/Browser forum requirements

5.2.2.5.1 Short description

Purpose and context: the Baseline Requirements (BR) for the Issuance and Management of Publicly-Trusted Certificates describe a subset of the requirements that a certification authority should meet to issue digital certificates for SSL/TLS servers to be publicly trusted by browsers. Building on this:

There are also requirements for code signing certificate issuance to be publicly trusted by browsers, that builds on the BR.

- Building on BR, EVG identify the legal entity that controls a web site by providing reasonable assurance that a web site is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information. EVGcontain a set of steps required to validate entity identity information.

- Similarly, building on EVG, EV guidelines [i.56] and for code signing provides assurance that the code signing certificate is issued to legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information.

ID type:

- BR: natural person, device, system, unit, or legal entity;

- Code signing: natural person or organization (i.e. private and public corporations, LLCs, partnerships, government entities, non-profit organizations, trade associations, and other legal entities);

- EVG: Private Organizations, Government Entities, Business Entities and Non-Commercial Entities (i.e. as above excepted natural persons).

NOTE: If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA should use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request. I.e. the validation of authority natural person associated to legal person.

Expected outputs: certificates for SSL/TSL of different levels (DV, OV, EV), or code signing certificates.

Sector: Browsers.

Legal background: NA.

5.2.2.5.2 Attribute collection

Attributes to be collected:

All (BR):

a) Organization: Identity, Address (optional), DBA (optional), Country, Domain/IP address (optional).

b) Individual: Applicant's name, Applicant's address, Authenticity of the certificate request.

c) Code signing:

- Legal person: Legal identity, whenever available, a specific Registration Identifier assigned to the Applicant by a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition; DBA; Certificate Requester authority to request a Code Signing Certificate; (cond.) identity of the Certificate Requester.

- Natural persons: Identity and authenticity of identity.

d) EV: as BR plus: Proof of identity existence of the applicant, reliable means of communication with the entity to be named as the Subject, applicant'sauthorization for the EV Certificate, and proof that applicant is a registered holder, or has control, of the DomainName(s) to be included in the EV Certificate.

Type of evidence to be/that can be presented:

All (BR):

Organization: using documentation provided by, or through communication with, at least one of the following:

a) a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

b) a third party database that is periodically updated and considered a Reliable Data Source;

c) a site visit by the CA or a third party who is acting as an agent for the CA; or

d) an Attestation Letter.

NOTE: The CA may use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address. Alternatively, the CA may verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

Individual:

a) Name: using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type).

b) Applicant's address: using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. The CA may rely on the same government-issued ID that was used to verify the Applicant's name.

c) Certificate request: with the Applicant using a Reliable Method of Communication.

Code signing: as BR and in addition, for natural person identity:

a) CA should obtain a legible copy, which discernibly shows the Requester's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). The CA should also verify the address of the Requester using:

(i) a government-issued photo ID;

(ii) a QIIS or QGIS; or

(iii) an access code to activate the Certificate where the access code was physically mailed to the Requester; or

b) CA should have the Requester digitally sign the Certificate Request using a valid personal Certificate that was issued under one of the following adopted standards: Qualified Certificates issued pursuant to ETSI TS 101 862 [i.33], IGTF, Adobe Signing Certificate issued under the AATL or CDS program, the Kantara identity assurance framework at level 2, NIST SP 800-63 (multipart [i.43], [i.44], [i.45]) at level 2, or the FBCA CP at the Basic or higher assurance.

EV: for individual:

a) A Personal Statement that includes the following information: Full name or names by which a person is, or has been, known (including all other names used); residential Address at which he/she can be located; date of birth; and an affirmation that all of the information contained in the Certificate Request is true and correct.

b) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as a passport; a driver's license; a personal identification card; a concealed weapons permit; or a military ID.

c) At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which is from a financial institution:

   (i) Acceptable financial institution documents include:

      1) A major credit card, provided that it contains an expiration date and it has not expired.

      2) A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired.

      3) A mortgage statement from a recognizable lender that is less than six months old.

      4) A bank statement from a regulated financial institution that is less than six months old.

   (ii) Acceptable non-financial documents include:

      1) Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill).

      2) A copy of a statement for payment of a lease, provided that the statement is dated within the past six months.

      3) A certified copy of a birth certificate.

      4) A local authority tax bill for the current year.

      5) A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

Type of presentation (of the attributes): Direct inspection or Indirect presentation of the ID attributes (e.g. have the Requester digitally sign the Certificate Request using a valid personal Certificate):

- EV: most of the element to be proved with regard to organization are to be verified directly with official source.
- EV for individual: The CA may rely on electronic copies of the documentation, provided that:

   (i) the CA confirms their authenticity (not improperly modified when compared with the underlying original) with the Third-Party Validator; and

   (ii) electronic copies of similar kinds of documents are recognized as legal substitutes for originals under the laws of the CA's jurisdiction.

5.2.2.5.3 Attribute validation

Determination that the evidence is genuine (issued by recognized independent/authoritative sources).

All (BR):

The CA inspects any document relied upon (see above) for alteration or falsification.

Prior to using any data source as a Reliable Data Source, the CA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. The CA should consider the following during its evaluation:

a) The age of the information provided.

b) The frequency of updates to the information source.

c) The data provider and purpose of the data collection.

d) The public accessibility of the data availability.

e) The relative difficulty in falsifying or altering the data.

NOTE: Reliable Data Source. An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Code Signing (individual): the CA inspects the copy for any indication of alteration or falsification.

EV: the validator should:

(i) attest to the signing of the Personal Statement and the identity of the signer; and

(ii) identify the original Vetting Documents used to perform the identification.

Other checks: All (BR):

To verify the authenticity of the Applicant Representative's certificate request:

a) The CA may use the sources listed in section 3.2.2.1 of CA/Browser forum requirements [i.120] to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA may establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

b) In addition, the CA establishes a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA will not accept any certificate requests that are outside this specification. The CA will provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

To verify the organization attributes:

a) If address is certified: include the name or address of an organization, the CA will verify the identity and address of the organization and that the address is the Applicant's address of existence or operation.

b) If DBA is to be certified: the CA will verify the Applicant's right to use the DBA/tradename using at least one of the following:

1) Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;

2) A Reliable Data Source;

3) Communication with a government agency responsible for the management of such DBAs or tradenames;

4) An Attestation Letter accompanied by documentary support; or

5) A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.

c) Country;

(a') the IP Address range assignment by country for either:

(i) the web site's IP address, as indicated by the DNS record for the web site; or

(ii) the Applicant's IP address;

(b') the ccTLD of the requested Domain Name;

(c') information provided by the Domain Name Registrar; or

(d') a method identified in Section 3.2.2.1 of CA/Browser forum requirements [i.120]. The CA should implement a process to screen proxy servers to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

d) Domain/IP address: section 3.2.2.4.5 of CA/Browser forum requirements [i.120] defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain/IP address.

e) EV: there are many checks that are preformed to verify the legal, physical and operational existence of an organization (and thus its identity), officila communication means with the applicant, etc. Also, as for BR, verification of Name, Title, and Authority of Contract Signer and Certificate Approver is required. Diverse methods are possible, e.g. a Verified Professional Letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of the Applicant; reliance on a properly authenticated corporate resolution, a contract between the CA and the Applicant, etc.

5.2.2.5.4 Attribute binding

Face to face interactions or Digital interactions are allowed.

Code Signing: the authenticity of identity requires:

- having the Requester provide a photo of the Requester holding the submitted government- issued photo ID where the photo is of sufficient quality to read both the name listed on the photo ID and the issuing authority; or
- having the CA perform an in-person or web camera-based verification of the Requester where an employee or contractor of the CA can see the Requester, review the Requester's photo ID, and confirm that the Requester is the individual identified in the submitted photo ID; or
- having the CA obtain an executed Declaration of Identity of the Requester that includes at least one unique biometric identifier (such as a fingerprint or handwritten signature). The CA should confirm the document's authenticity directly with the Verifying Person using contact information confirmed with a QIIS or QGIS; or
- verifying that the digital signature used to sign the Request under Section 11.2.1(2) of CA/Browser forum EV Guidelines [i.56]) is a valid signature and originated from a Certificate issued at the appropriate level of assurance as evidenced by the certificate chain. Acceptable verification under this section includes validation that the Certificate was issued by a CA qualified by the entity responsible for adopting, enforcing, or maintaining the adopted standard and chains to an intermediate certificate or root certificate designated as complying with such standard.

EV: individual associated with the Business Entity are validated in a face-to-face setting before either an employee of the CA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator).

5.2.2.5.5 Recommendation on the process

What needs to be done:

The CA should verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

Beyond the above requirements, for issuing EV certificate, it is required to verify the applicant's existence and identity, including:

(A) verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 of CA/Browser forum EV Guidelines [i.56]);

(B) verify the Applicant's physical existence (business presence at a physical address); and

(C) verify the Applicant's operational existence (business activity).

How this needs to be done:

- verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA inspects the copy for any indication of alteration or falsification;
- verify the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. The CA MAY rely on the same government-issued ID that was used to verify the Applicant's name.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

General requirements:

- Possible security levels associated to one step or the whole process: there are two levels: BR and EV.
- Compliance measures implemented: the generic requirements on the CA (see below) cover traceable documentation, access policy, personnel training and authorization, premises security, audit requirement, etc.

Besides the identity proofing requirements here described, there are requirements on the CA operation (HR, network, etc.).

Security requirements: Yes.

5.2.2.5.6 Reference material

Title	URL
CA/Browser forum requirements. V 1.7.1 [i.120] CA/Browser forum EV Guidelines v1.7.4 [i.56]	https://cabforum.org/baseline-requirements-documents https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.7.4.pdf

5.2.2.5.7 Reviewer note and conclusion

The CA/B-forum requirements in matter of identity proofing are very detailed and complete. They cover both the identity proofing of natural persons and of organizations. They are a very good source of inspiration for the ETSI DTS/ESI-0019461 [i.50], especially in matter of evidence to be collected for legal persons. However, there are a large variety of cases and sub-cases, probably too complex for ETSI DTS/ESI-0019461 [i.50].

5.2.3 National

5.2.3.1 UK: Guidance on Identity proofing and authentication

5.2.3.1.1 Short description

Purpose and context: Set of guidance on how to prove natural and legal identity or give them access to services or organizations that include:

- Good Practice Guide 45 [i.58] on natural person ID proofing, that helps on how to check physical person's identity.
- Good Practice Guide 46 [i.59] on organizations or individuals acting on behalf of those organizations ID proofing. It relates to establishing the identities of organizations or individuals acting on behalf of those organizations (legal persons and its proxies).
- Good Practice Guide 44 [i.60], on using authenticators to protect an online service.
- Good Practice Guide 43 [i.61] "Requirements for Secure Delivery of Online Public Services".

- Good Practice Guide 53, "Transaction monitoring for HMG online service providers", sets out the role of transaction monitoring in helping to counter electronic attacks against online public services.

These guidances were written by the UK Government Digital Service with help from organizations across the public and private sectors (such as Department for Work and Pensions; Driver and Vehicle Licensing Agency; HM Revenue and Customs; Home Office; Ministry of Defence (MoD); National Cyber Security Centre; Barclays; Digidentity; Experian; IDEMIA and Post Office.

This guidance does not include specific tools or processes for each implementation.

ID type: Natural, legal person and its representatives.

Expected outputs: Identity validation.

Sector: Public and private sectors, with no limitation to any particular activity.

Legal background: This guidance is aligned with the following international standards and regulations: Digital ID and Authentication Council of Canada (DIACC), Pan Canadian Trust Framework Model, the eIDAS regulation [i.1]; ISO/IEC 29115 [i.30] and NIST 800-63C [i.45].

5.2.3.1.2 Attribute collection

Attributes to be collected: For natural person could include:

- the claimed identity's name;
- the claimed identity's date of birth;
- the claimed identity's place of birth;
- the claimed identity's address;
- the claimed identity's biometric information (these are measurements of biological or behavioural characteristics, like an iris or fingerprint);
- a photo of the claimed identity; or
- a reference number.

Type of evidence to be/that can be presented: Depends on the specific implementation. The guidance include a score system from 1 to 5 depending on the pieces of information (at least 2 of the above for **score 1**) and the organization issuing the evidence.

For **score 2,** it will need to get a score of 1 and it includes information that's unique to either the identity and that piece of evidence. If the evidence includes a name, it should show the person's full name instead of any pseudonyms, aliases or nicknames. If the evidence is a physical document, it should be protected by physical security features. These features will stop it from being reproduced without specialist knowledge or information. If the evidence includes digital information, it should either be protected by: cryptographic security features that correctly identify the person or organization that issued it; and **processes** that make sure only authorized users can create, update and access it

Examples of evidence that have a score of 2 include a firearm certificate; a Home Office travel document (convention travel document, stateless person's document, one-way document or certificate of travel); a birth or adoption certificate; an older person's bus pass; an education certificate from a regulated and recognized educational institution; a rental or purchase agreement for a residential property; a proof of age card recognized under the Proof of Age Standards Scheme (PASS); a Freedom Pass; a marriage or civil partnership certificate; a building, contents or vehicle insurance policy; a gas or electric account; or **a 'substantial' electronic identity from a notified eIDAS scheme.**

Score 3 requires a score of 2 and includes information that's unique to both the identity and that piece of evidence; the organization that issued the evidence made sure it was received by the same person who applied for it; the organization that issued the evidence checked the person's identity in a way that follows the 2017 Money Laundering Regulations. It has also:

- to show the person's official name instead of their initials or synonyms, for example 'Julian' instead of 'Jules' (if the evidence includes a name); and

- to be protected by physical security features that stop it from being reproduced without specialist equipment (if the evidence is a physical document);

The evidence should also include one of the following:

- a photo of the person;
- biometric information that uses cryptographic security features to protect its integrity;
- cryptographic security features that can be used to identify the person who owns the evidence (this includes evidence with cryptographic chips and digital accounts that are protected by cryptographic methods).

Some examples of evidence that will have a score of 3 include: passports that meet the International Civil Aviation Organization (ICAO) specifications for machine-readable travel documents; identity cards from an EU or European Economic Area (EEA) country that follow the Council Regulation (EC) No 2252/2004 standards [i.49]; UK photocard driving licences; EU or EEA driving licences that follow the European Directive 2006/126/EC [i.34]; a Northern Ireland electoral identity card; a US passport card; a bank, building society or credit union current account (which the claimed identity can show by giving a bank card); a student loan account; a credit account; a mortgage account (including buy to let mortgage accounts); a digital tachograph driver smart card; an armed forces identity card; a proof of age card recognized under PASS with a unique reference number; a loan account (including hire purchase accounts); **a 'high' electronic identity from a notified eIDAS scheme.**

Score 4 requires to get a score of 3 and:

- biometric information;
- all digital information (including biometric information) is protected by cryptographic security features;
- the cryptographic security features can prove which organization issued the evidence;
- the organization that issued the evidence proved the person's identity by comparing and matching the person to an image of the claimed identity from an authoritative source.

Some examples of evidence that will have a score of 4 include:

- biometric passports that meet the ICAO specifications for e-passports;
- identity cards from an EU or EEA country that follow the Council Regulation (EC) No 2252/2004 [i.49] standards and contain biometric information; or
- a UK biometric residence permit.

Type of presentation: Depends on the specific implementation and score. See above.

5.2.3.1.3 Attribute validation

The guideline set out checks to validate (validity check) that the evidence presented:

- is genuine (not forged or counterfeit);
- is valid (records can be found that show the piece of evidence has been issued);
- has not expired;
- has not been cancelled or reported as lost or stolen.

For score 1, the physical features of the evidence has to appear to be genuine.

For the score 2, it has to be verified that the evidence has not expired.

For score 3, it should be confirmed that:

- the evidence is valid or check the evidence has not been cancelled, lost or stolen;
- the visible security features are genuine;

- the UV or IR security features are genuine;
- the evidence has not expired.

For score 4, it should be confirmed that:

- confirm the visible security features are genuine;
- confirm the UV or IR security features are genuine;
- confirm the cryptographic security features on the evidence are genuine;
- check the evidence has not been cancelled, lost or stolen;
- check the evidence has not expired;
- check the visible security features are genuine.

The evidence can be checked in person or remotely.

For score 1of the validity check.

- check an original, certified copy or scan of the evidence;
- no errors on the evidence, like wrong paper type, spelling mistakes, irregular use of fonts or missing pages;
- the details, layout or alignment of the evidence look the way they should;
- any logos look the way they should; and
- any references to information are the same across the evidence (for example if the body text of a letter references an address, this should match the address shown at the top of the letter).

For score 2 (expiration) of the validity check:

- confirm the evidence is valid;
- confirm the visible security features are genuine (these are security features that can be seen without using specialist light sources);
- confirm the ultraviolet (UV) or infrared (IR) security features are genuine.

It recommends the use of PRADO [i.86], the EU and EEA driving licence handbook, or EdisonTD.

5.2.3.1.4 Attribute binding

See above.

5.2.3.1.5 Requirements on the process

The ID proofing process for **natural persons** or, as it is called by the document, the process of 'identity checking' is made up of 5 parts:

a) To get evidence of the claimed identity: use an 'authoritative' source (the integrity of the information is protected; the information is up to date).

b) To check the evidence is genuine or valid: use an 'authoritative' source (the integrity of the information is protected; the information is up to date).

c) To check the claimed identity has existed over time.

d) To check if the claimed identity is at high risk of identity fraud.

e) To check that the identity belongs to the person who's claiming it.

The different steps of the ID proofing process can be performed at once or over any period of time. In the latter, the confidence on a given ID is built up gradually.

Each part of the identity checking process provides a score. The different combinations of scores are known as 'identity profiles'. These profiles and its trustworthiness depends on how many pieces of evidence are collected; which parts of the identity checking process is performed; and what scores one gets for each part of the identity checking process.

Each identity profile relates to one of the following levels of confidence:

- low confidence;
- medium confidence;
- high confidence;
- very high confidence.

The process approach in 5 parts is modular and made possible to reuse identity checks done by another organization/administration.

The guidelines aim to established a scoring system were the higher level of confidence is related to a high risk of identity-related crime or ID forged or counterfeit.

The **ID proofing process for legal person and it representative** is as follows:

a) The identity of the applicant is to be proven in accordance with Good Practice Guide 45 [i.58], Identity Proofing and Verification of an Individual.

b) The applicant declares the organization for which they are a responsible officer. Where details of an organization are held on a register, the applicant provides the registered details which should, as a minimum, contain the organization details, the registered address and, where applicable, the organization identifier.

c) Checks are to be performed to determine that the applicant is a responsible officer of the organization.

d) At the end of the process a relationship has been established between the applicant and an organization that describes the level of confidence that the applicant is a responsible officer of that organization and, by inference, that the organization is a legal entity.

Security requirements:

No specific security requirements for the Identity Checking process are set out. This process is viewed as a part of a risk assessment/risk management approach of online public services.

Good Practice Guide 44 [i.60] sees authenticators as a security mean to protect an online service.

Good Practice Guide 43 [i.61] sets out a six step process is introduced that provides a systematic process to help inform the risk management of online public services. This process is:

- aimed at those providing online public services;
- provides a means to understand what is needed to securely deliver online public services;
- takes a transactional viewpoint of services basedon distributed delivery models;
- encourages an informed risk management approach whilst taking into account stakeholder expectations and concerns; and
- produces a security case that transparently demonstrates that stakeholder expectations and information risk have been appropriately considered.

Good Practice Guide 53 [i.62], sets out the role of transaction monitoring in helping to counter electronic attacks against online public services. It provides a means for online Service Providers to think about and analyse the security needs of their service and produces a security profile that sets out the security aims for the online service.

5.2.3.1.6 Reference material

Title	URL
UK guidance on Identity proofing and authentication [i.57]	https://www.gov.uk/government/collections/identity-proofing-and-authentication
Good Practice Guide 45 on natural person ID proofing [i.58]	https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual
Good practice Guide 46 on organizations or individuals acting on behalf of those organizations ID proofing [i.59]	https://www.gov.uk/government/publications/identity-assurance-organisation-identity
Good Practice Guide 44, on using authenticators to protect an online service [i.60]	https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services
Good Practice Guide 43 "Requirements for Secure Delivery of Online Public Services" [i.61]	https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services
Good Practice Guide 53, "Transaction monitoring for HMG online service providers" [i.62]	https://www.gov.uk/government/publications/transaction-monitoring-for-hmg-online-service-providers

5.2.3.2 UK: Draft BSI 8626 Design and operation of online user identification systems

5.2.3.2.1 Short description

Purpose and context: The Draft BSI 8626 [i.63] purports to give recommendations and supporting guidance for the design and operation of Online User Identification Systems (OUISs) operated by digital identity providers (IdPs) for one or more relying parties. It sets comprehensive guidelines for OUISs covering functional, organizational as well as technical aspects. These notably cover identity proofing processes by indicating *inter alia* the entities authorized to undertake identity proofing processes, the acceptable form of evidence and how data are verified as well as the rules for administrators and/or processes to follow. The Draft BSI 8626 [i.63] adopts a holistic approach identifying in detail all aspects and dimensions needing to be considered for OUISs. In particular, recommendations are given for:

a) establishing or revising an OUIS, including:

   1) business objectives and recommendations for an OUIS;

   2) recommendations for protecting the life cycle management of digital identities associated with individuals;

   3) recommendations for protecting data used specifically for the processes of identifying or authenticating individuals;

   4) recommendations for protecting against attacks on specific types of user identification methods (including biometrics) and modes of operation.

b) the controls for managing the life cycle of users' digital identities for an OUIS.

However, the Draft BSI 8626 [i.63] does not define any particular threshold or minimum outcome for these, which leaves significant flexibility for IdPs. When it comes to identity proofing, the Draft BSI 8626 [i.63] defines a general principle ("*the Identity proofing process should enable a legitimate applicant to prove their identity in a straightforward manner while creating significant barriers to those claiming to be somebody they are not*".) It also includes in its Annex a description of the leading levels of assurance and of biometric performance metrics but seldom explains how these are related to the various recommendations outlined in the document.

ID type: Natural persons and natural persons acting on behalf of a third party (natural person or legal person).

5.2.3.2.2 Attribute collection:

Attributes to be collected: The Draft BSI 8626 [i.63] requires identity providers to "collect sufficient identifying information from the applicant to make the identity uniquely identifiable. Depending on the context, the exact information needed can vary and may be driven by what information the identity provider holds or has access to determine whether an identity is likely to be unique". However, the given, family names and dates of birth appear to be required in all cases.

Type of evidence to be/that can be presented: The Draft BSI 8626 [i.63] directs IDPs to collect "appropriate evidence, which may be physical or digital, to prove the identity of the person" and requires IDPs to ensure that "the spread of identity information and evidence provided is sufficient to uniquely identify the applicant and protect the person from impersonation".

Type of presentation: Not directly addressed by the Draft BSI 8626 [i.63], but all communication channels are eligible as a matter of principle.

5.2.3.2.3 Attribute validation:

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): The Draft BSI 8626 [i.63] requires IdPs to "*determine whether the evidence is likely to be genuine and valid, taking into the risk of lost, stolen, suspended, revoked or expired evidence*" as well as "*mitigate the risks to services from fabricated, duplicated or altered evidence through the inspection of the security features and/or corroboration of its authenticity with authoritative sources*". It offers an extensive list of tests to this effect.

Other checks implemented if any: The Draft BSI 8626 [i.63] also offers guidance with respect to 'counter identity fraud mitigation measures' but only in fairly general, non-specific terms: "*The IdP should ensure that the claimed identity is not at a higher than usual risk of identity fraud, such as a public figure, or likely to be synthetic. The IdP should take steps to minimize the risk from compromised identities and identity data, especially from known data breaches and cyber attacks, even if those details have not been used fraudulently".*

5.2.3.2.4 Attribute binding

The Draft BSI 8626 [i.63] distinguishes 'Knowledge-based verification' - where the binding process is based on knowledge of shared information and 'physical or biometric verification', where the binding process is based on a physical characteristic. It defines a series of useful requirements for Knowledge-based verification methods and offers detailed guidance for physical or biometric verification. This implies notably mitigation measures, assessing vulnerabilities and other relevant aspects.

Face to face interactions not directly addressed by the Draft.

5.2.3.2.5 Requirements on the process

As mentioned earlier, the Draft BSI 8626 [i.63] contains numerous recommendations that are relevant for all or most steps, notably with respect to manageability, reliability and sustainability as well as usability requirements.

5.2.3.2.6 Reference material

Title	URL
Draft BSI 8626 Design and operation of online user identification systems - Code of practice Available online as of July 2020 [i.63]	https://standardsdevelopment.bsigroup.com/projects/2018-01712

5.2.3.2.7 Reviewer note and conclusion

The Draft BSI 8626 [i.63] is unquestionably a very useful document for this study covering all key aspects of identity proofing and reflecting the latest trends in identity proofing processes. It includes numerous specifications and recommendations covering most, if not all aspects of identity proofing. There are however two limitations that can be mentioned:

- the Draft BSI 8626 [i.63] is a proposal currently subject to review/comments. It is therefore difficult to predict how its content will evolve after the consultation process;
- the Draft BSI 8626 [i.63] offers numerous specifications or recommendations, i.e. expressions of possible courses of actions deemed particularly suitable, with few appearing to be defined as requirements for which no deviation is permitted if compliance with the document is to be claimed, leaving significant implementation discretion to OUIS operators and IdPs. In addition, the Draft BSI 8626 [i.63] appears to take no view as to what is required to achieve a specific assurance level but simply offers guidelines for the description of assurance requirements for OUISs.

In addition, the Draft BSI 8626 [i.63] discusses in considerable detail some identity-proofing topics - for example biometric verification processes discussed in Section 8 as well as Annex B, but is less developed with respect to other aspects - there are only general indications as to which attributes are to be collected as well as to how these are to be received.

5.2.3.3 US. NIST Special Publication 800-63 Digital Identity

5.2.3.3.1 Short description

Purpose and context: The 800-63 series ([i.43], [i.44], [i.45]) are guidelines providing technical requirements for federal agencies implementing digital identity services. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. The series is thus not dedicated to identity proofing as this is only an element of the global picture in digital identity services.

NIST SP 800-63 ([i.43], [i.44], [i.45]) provides an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels. It defines 3 components of identity assurance:

- IAL refers to the identity proofing process.
- AAL refers to the authentication process.
- FAL refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a Relying Party (RP).

NIST SP 800-63-A [i.43] addresses how applicants can prove their identities and become enrolled as valid subscribers within an identity system. It provides requirements by which applicants can both identity proof and enroll at one of three different levels of risk mitigation (see below) in both remote and physically-present scenarios. It defines 3 levels of assurance for identify proofing and provides the procedures:

- Required for IAL2, requiring identifying attributes to have been verified in person or remotely.
- Required for IAL3, requiring identifying attributes to be verified by an authorized CSP representative through examination of physical documentation.

NIST SP 800-63B [i.44] addresses Authentication and Lifecycle Management (for services in which return visits are applicable).

NIST SP 800-63C [i.45] provides requirements when using federated identity architectures and assertions to convey the results of authentication processes and relevant identity information to an agency application. In addition, this volume offers privacy-enhancing techniques to share information:

- ID type: natural persons.
- Expected outputs: an individual, referred to as an *applicant* at this stage, opts to be identity proofed by a CSP. If the applicant is successfully proofed, the individual is then termed a subscriber of that CSP. The CSP establishes a mechanism to uniquely identify each subscriber, register the subscriber's credentials, and track the authenticators issued to that subscriber. The subscriber may be given authenticators at the time of enrolment.

In other words, the enrollment and verification of an identity for use in digital authentication. To do so, when a subject is identity proofed, the expected outcomes are:

- Resolve a claimed identity to a single, unique identity within the context of the population of users the CSP serves.
- Validate that all supplied evidence is correct and genuine (e.g. not counterfeit or misappropriated).
- Validate that the claimed identity exists in the real world. Remote or physically-present identity proofing.
- Verify that the claimed identity is associated with the real person supplying the identity evidence.

The document specifies this process according to 3 levels:

- self assertions;
- real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity;
- as above + physical presence.

NIST SP 800-63 (multipart [i.43], [i.44], [i.45]) offers very good definitions and correctly sets the scene between ID proofing and other, related, processes like authentication or tools like federation of identities.

NIST SP 800-63 (multipart [i.43], [i.44], [i.45]) has a valuable risk management section. From the perspective of an identity proofing failure, there are two dimensions of potential failure:

1) The impact of providing a service to the wrong subject (e.g. an attacker successfully proofs as someone else).
2) The impact of excessive identity proofing (i.e. collecting and securely storing more information about a person than is required to successfully provide the digital service).

Clause 6.1 in particular offers a practical tool to select the Identify Proofing Assurance Level.

Also interesting, clause 7 on the rationales to rely or not, on federated attributes.

NIST SP 800-63A [i.43] is almost the TS the STF is expected to produce, specifying policy and requirements for "CSP" practicing identity proofing services, with the aim to enrol a subject.

Parts B and C address tools for authentication and assertions respectively. Such tools are to be used as inputs for identity proofing processes. Parts B and C are particularly interesting because authentication and assertions tools are rated according to 3 levels of assurance. In particular, for services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the subscriber accessing the service today is the same as that which accessed the service previously. NIST SP 800-63B [i.44] describes the strength of the authentication process by an ordinal measurement called the AAL. AAL1 requires single-factor authentication and is permitted with a variety of different authenticator types. At AAL2, authentication requires two authentication factors for additional security. Authentication at the highest level, AAL3, additionally requires the use of a hardware-based authenticator and verifier impersonation resistance.

Specifying authentication/assertions tools and rating them is outside the scope of the present study, but selecting the right level is well in scope (e.g. it is likely to be the case that a best practice will exclude AAL1), so reliance on rating will be of great interest.

Sector: principally relationships with governmental agencies, but broadly applicable (e.g. KYC).

Legal background: not driven by a legal background but link to PIV (eID credentials for US civil servants).

5.2.3.3.2 Attribute collection

Attributes to be collected: different sets of attributes (depends on the business). Also, The CSP is required to collect and record a biometric sample at the time of proofing (e.g. facial image, fingerprints) for the purposes of non-repudiation and re-proofing.

Type of evidence to be/that can be presented: different types of evidence are allowed, and according to the IAL, some strength is required. The document specifies the criteria to reach a certain strength. This depends amongst other on the trust and issuing process of the issuing source.

Type of presentation (of the attributes): Direct inspection and/or Indirect presentation of the ID attributes are allowed (depends on the type of evidence).

5.2.3.3.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): different ways of validation are allowed, and according to the IAL, some strength is required. The document specifies the criteria to reach a certain strength.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources):

- checking an authoritative source;
- checks the images of the license and the passport, determines there are no alterations, the data encoded in the QR codes matches the plain-text information, and that the identification numbers follow standard formats;
- queries the issuing sources for the license and passport and validates the information matches.

As for different determination that the ID attribute are valid, different ways of validation are allowed, and according to the IAL, some strength is required. The document specifies the criteria to reach a certain strength.

5.2.3.3.4 Attribute binding

Face to face interactions and remote interactions: both are allowed for IAL2. For IAL3 remote interaction are possible but the applicant needs to be present "in person" (i.e. "supervised remote mode").

The document provides detailed requirements to perform a remote "in person" identity proofing.

It is possible to rely on trusted referees (requirements to do so are specified).

5.2.3.3.5 Requirements on the process

What needs to be done:

The document provide security and policy requirements for each steps of the process, and this is instantiated for the 3 IALs.

Elements common to all steps:

Possible security levels associated to one step or the whole process: 3 levels of IAL. 5 levels of strength (unacceptable, weak, fair, strong, superior) for the quality of evidence, validation, verification of evidence.

Clause 4.2 in NIST SP 800-63 A provides very useful general requirements for being a CSP active in identity proofing, respect of privacy (need to know basis), etc. This addresses e.g. the need for policies and practices, and similar general requirements.

NIST SP 800-63A [i.43] provides general requirements on log and tracing, as well as considerations on privacy and on security in general.

Security requirements: Yes

5.2.3.3.6 Reference material

Title	URL
NIST Special Publication 800-63 Digital Identity	https://www.nist.gov/itl/tig/projects/special-publication-800-63
NIST Special Publication 800-63A Digital Identity Guidelines. Enrollment and Identity Proofing [i.43]	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf
NIST Special Publication 800-63B Digital Identity GuidelinesAuthentication and Lifecycle Management [i.44]	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
NIST Special Publication 800-63C Digital Identity GuidelinesFederation and Assertions [i.45]	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf

5.2.3.4 Germany: BSI TR-03147 on Assurance Level Assessment of Procedures for Identity Verification of Natural Persons

5.2.3.4.1 Short Description

Purpose and Context: The technical guideline outlines a threat/risk perspective to identity proofing. Based on threats to the identity checks, requirements for the identity checks have to be defined and implemented.

Document provides the technical guideline for minimum levels of assurance for E-Government/Business functions (Bundesamt für Sicherheit in der Informationstechnik).

This is a complimentary document to guideline BSI TR-03107-1 (Electronic Identities and Trust Services in E-Government)

Assessment of identity verification procedures, same assurance levels as BSI TR-03107-1 and eIDAS LoA:

- eIDAS LoA framework is relative to Germany's regulations in government and e-business practices.
- eIDAS: Low, Substantial, and High.
- Germany: Normal, Substantial, and High.

The Guide is meant to go in conjunction with BSI TR-03107-1 and examines threats and requirements for identity proofing and verification procedures which are based on the usage of ID documents (e.g. ID cards or passports).

This document does not discuss determination of said assurance levels, and does not discuss service availability or non-reputability of ID or registration process.

ID Type: Natural person.

Expected Output(s): Clarification of Germany's position on how eIDAS framework is incorporated into technical standards.

Sector(s): Government and E-Business.

Legal Background: Not applicable, but the document covers eIDAS application inside German framework**.** The document provides tables and specifications for definitions and assessment methodology, proof of Identity, trustworthiness of ID documents**,** security of transmission channels, checking of ID documents, comparison of persons with ID document data, correct registration of the required ID attributes, and safeguarding process integrity.

5.2.3.4.2 Attribute Collection

Attributes to be collected:

Identity, any applicable attributes of the subject. The actual set of ID attributes that is required for a proof of identity depends on the specific application. If required by the application, the set of ID attributes has to allow a unique identification. This point is not related to technical security aspects and not listed in the technical guideline.

Type of evidence to be/that can be presented:

Proof of identity and identity checks:

- The basis for a regular ID verification have one trustworthy ID document that allows for authoritative verification of the authenticity and integrity of all relevant ID attributes.
- The overall assurance level is determined based on ID document providing the lowest assurance level for a specific ID check.

5.2.3.4.3 Attribute Validation

D**etermination that the ID attribute are valid (not expired, not revoked):**

- ID attributes are up to date
- Available lost, stolen, or revoked reports are checked
- Periodic check of the set of admitted ID documents
- Authoritative source
- Provides a sufficient set of ID attributes
- Protected against forgery and manipulation

- Security features are known and effectively verifiable
- Affords reliable check against its legitimate owner (allows to detect illegitimate usage)

FAR is pre-defined for an ID check (or its related e-government/business processes). Exceed the pre-defined FAR is not permitted.

Technical Guideline Biometrics for Public Sector Applications TR -03121-3 states that the FAR for biometric threshold is 0,1 % (1:1,000).

5.2.3.4.4 Attribute binding

Checking of ID documents: for a specific type of ID document: The lowest assurance level of all authorized combinations of ID proofing and verification procedures determines the resulting assurance level for the ID check.

Comparison of persons with ID documents data: the guidance given in this clause assumes that the ID verification is based on multifactor authentication and verified from two different categories with a positive match (i.e. document and knowledge or inherent factor).

5.2.3.4.5 Requirements on the process

Requirements for assurance level assessment normal, medium, high: A secure verification of ownership of the ID document requires some kind of interaction with the person to be identified. The requirements are differentiated according to the assurance levels.

As a general safeguard for the integrity of all IT based processes, an ISMS according to ISO/IEC 27001 [i.24] and ISO/IEC 27002 [i.35] or equivalent is required to be implemented. The ISMS scope will include all IT components and processes that are directly or indirectly used for the ID verification, storage or transmission of captured ID attributes and related data.

The ID proofing process for natural persons is described from a security perspective and is the basis for secure ID proofing and the verification procedures outlined in the document. These requirements are broken up into 5 process requirements:

- Checking the authenticity of the document and not manipulated.
- Validity Check.
- Ensuring the ID has not been stolen, lost, or manipulated.
- Security Features are checked.
- Comparison of Person with the ID.

Compliance to the ID checking procedures can be ensured through technical measures, organizational measures or combinations of both. The measures may include the requirement for traceable documentation of all checks that have been performed. The basis of this requirement is the set of checks that have to be done for each ID document:

Security Requirements: Yes.

The threats related to the security objectives are analysed top-down and the resulting requirements are evaluated according to the assurance levels *normal*, *substantial*, *high*. The relevance of the security objectives will depend on the intended use for which the ID checking is required. All relevant security objectives and the related threats and requirements are taken into consideration and measures are ensured.

Existence: Existence of an entity (natural person) to which all claimed ID attributes apply.

Legitimacy: All stated ID attributes apply to the natural person claiming them.

Uniqueness: No two persons have identical values for all captured ID attributes.

5.2.3.4.6 Reference material

Title	URL
Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons (V1.0.4). [i.64]	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03147/TR03147.pdf?__blob=publicationFile&v=1

5.2.3.5 Romania. Communication for Qualified Trust Service Providers

5.2.3.5.1 Short description

Purpose and context: eIDAS Article 24 1. (d). In Romania there is no regulation to define "identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence". The Supervisory Body published on their website the following announcement. Under the provisions of the European Regulation 910/2014, following public consultations held at Ministry of Communication and Information Society, with the attendance of all qualified trust service providers in Romania, the following were agreed upon:

- technical mechanisms for remote video identification to be implemented/used by qualified trust service providers in Romania will be certified, based on technical standards adopted at European Commission level, only by auditors accredited at European Union level;
- the responsibility for the safe and error-free use of remote video identification mechanisms rests solely with qualified trust service providers in Romania, jointly with the accredited European auditors who certified the technical solution following the audit report;
- Ministry of Communication and Information Society will mention in all the documents issued to the qualified trust service providers in Romania, the following note: "The Ministry is not responsible for any damages caused/produced by using the remote video identification mechanisms").

ID type: specified by eIDAS - legal person, natural person, or website.

Expected outputs: qualified certificates.

Sector: N/A.

Legal background: eIDAS Article 24 1 (d)

5.2.3.5.2 Attribute collection

Attributes to be collected (specified by eIDAS):

- For natural persons: at least the name of the signatory.
- For legal persons: at least the name of the creator of the seal and, where applicable, registration number as stated in the official records.
- For webiste:
  - for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym clearly indicated;
  - for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;
  - elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;
  - the domain name(s) operated by the natural or legal person to whom the certificate is issued.

Type of evidence to be/that can be presented: not specified.

Type of presentation (of the attributes): not specified.

5.2.3.5.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): not specified.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): not specified.

5.2.3.5.4 Attribute binding

Regulation eIDAS requires as follows:

a) by the physical presence of the natural person or of an authorized representative of the legal person; or

b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or

c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

d) by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. A Conformity Assessment Body will evaluate that th level of assurance is equivalent;

e) Romania request, when this is done by means of video, a safe and error-free use of remote video identification mechanisms.

5.2.3.5.5 Requirements on the process

The document does not cover the identity proofing process. As it fits within the eIDAS framework, one may suppose that:

- Compliance measures implemented follows Article 19, 20 (audit) and 24 (trustworthy systems) of eIDAS apply.
- In the absence of technical standards adopted at European Commission level specifying mechanisms for remote video identification, technical standards that apply can be ETSI EN 3x1 4y1 series.

Security requirements: No

5.2.3.5.6 Reference material

Title	URL
Communication for Qualified Trust Service Providers in Romania [i.65]	https://www.comunicatii.gov.ro/comunicat-de-informare-pentru-prestatorii-de-servicii-de-incredere-calificati-din-romania/

5.2.3.6 France. ANSSI: Référentiel d'exigences de sécurité - Moyens d'identification électronique

5.2.3.6.1 Short description

Purpose and context: The Référentiel d'exigence de securité - Moyens d'identification électronique (the 'Référentiel') [i.66] is a document released on an ad-hoc basis by ANSSI, the French cyber-security agency, focusing on security requirements for electronic identification means and aiming to facilitate the assessment of processes deployed by ID and identity-proofing services providers in need of ANSSI certification. The Référentiel [i.66] is aligned with the eIDAS regulation [i.1], including Implementation Regulation 2015/1502 [i.3], and defines operational requirements for Low, Substantial and High levels of assurance.

It is an important document as the eIDAS Substantial LoA level is now treated as the threshold requirement for AML regulatory purposes in the French financial & monetary code and the ANSSI certification of French digital identity schemes at such level is also officially recognized as valid for such purpose. However, the Référentiel [i.66] remains in draft form (the latest draft is dated August 29, 2018 - version 1.0.d), is not publicly available - it is not listed on the ANSSI website - and is presented as 'subject to changes at any time'.

The Référentiel [i.66] is not the only ANSSI document dealing with identity-proofing - other identity proofing provisions exist in relation to eIDAS trust services (see for example 'Service de délivrance de certificats qualifies de signature électronique, de cachet électronique et d'authentification de site internet - critères d'évaluation de la conformité au règlement eIDAS') but these tend to focus on 'on-premise' identity proofing and are only cursorily defined for non-face-to-face situations.

ID type: The Référentiel [i.66] covers both natural and legal persons. In the latter case, the Référentiel defines LoA-dependent requirements for the identification of the natural person acting on behalf of the legal person as well as for the corporate authority of the natural person.

Expected outputs: The Référentiel [i.66] outlines the ANSSI policies in relation to the assessment of electronic identity services offered by services providers as part of their ANSSI certification process.

Sector: The Référentiel [i.66] is aimed primarily at Trust service providers and ID providers in need of ANSSI certification.

Legal background: See above.

5.2.3.6.2 Attribute collection

Attributes to be collected: The *Référentiel* [i.66] makes no reference to specific ID attributes but assumes that all ID data should be verified

Type of evidence to be/that can be presented: The *Référentiel* lists the ID documents recognized as 'authoritative for identity-proofing matters, uments, meaning for natural persons ID cards, residence cards or passports (for non-French document, as defined in the PRADO registry [i.86]).

Type of presentation:

For level substantial: Remote verification of authenticity of an identity document, when this identity document is never physically present at any step of the verification process, can be considered as sufficient only if it is demonstrated that technical and organizational measures are in place and reduce the risk of fraud with an efficiency at least equal to physical presentation of an identity document. These measures should in particular cover the risks linked to the presentation of counterfeit or forged identity documents, as well as the risks linked to the manipulation of image capturing devices or communication channels (for example, substitution of a modified picture of an identity document to the picture captured by the device). These requirements can be satisfied in the following three cases:

1) the identity document contains security characteristics that can be verified through picture or video (the PRADO register [i.86], available on this website https://www.consilium.europa.eu/en/documents-publications/publications/prado-do-you-check-identities-or-identity-documents/ identifies some security characteristics of identity documents that are to be verified). The picture or video is sufficiently accurate and allows the verifier to perform all necessary controls. In particular, it is required to be in color, and with a document resolution equivalent to 400 DPI; or

2) the identity document embeds an electronic chip which contains all the necessary information for the identification of the applicant, and authenticity of these information can be proven through the use of cryptographic means (for example, verification of electronic signatures on the basis of the MasterList published by a State, or the ICAO PKD registry for passports); or

3) the identity document contains machine readable information, containing all the necessary information for the identification of the applicant, and authenticity of these information can be proven through the use of automated means performing cryptographic verifications (for example, a QR Code containing electronically signed data).

For level high, only cases 2 and 3 are accepted. It is not possible, in ANSSI's opinion to validate the genuineness of an identity document through sole visual inspection with sufficient reliability to meet the requirements of level of assurance high.

- Each communication channel is LoA-dependent. Note that the lack of electronic functionalities of the current French ID card means that its remote presentation can at best achieve a Substantial (and not High) LoA.

5.2.3.6.3 Attribute validation

Determination that the ID attribute are valid: The Référentiel contains prescriptive provisions addressing the security checks and validation of the identity document presented on a face to face or remote basis. These provisions vary according to the contemplated LoA.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): The Référentiel contains prescriptive provisions addressing the genuineness of the identity document when presented on a face to face or remote basis. These provisions vary according to the contemplated LoA.

5.2.3.6.4 Attribute binding

Face to face interactions. The Référentiel contains a general description of the linking process implemented in connection with face to face interactions. These provisions vary according to the contemplated LoA.

Digital interactions:

The Référentiel contains some description of the processes and key requirements involved but these tend to be assessed on a case by case basis, meaning that no detailed specifications are provided. However, the Référentiel generally mentions two High LoA outcome-based criteria to be taken into account:

(i) the false positive rate of the solution used; and

(ii) its ability to withstand moderate or high potential attacks.

5.2.3.6.5 Requirements on the process

As mentioned earlier, the Référentiel covering all phases of the digital identity services, including authentication, revocation, employee management and training processes.

5.2.3.6.6 Reference material

Title	URL
ANSSI: Moyens d'identification electronique - Référentiel d'exigences de sécurité Draft dated August 29 2018 - version 1.0.d [i.66]	(unpublished - available upon request from ANSSI)

5.2.3.6.7 Reviewer note and conclusion

The Référentiel is no doubt relevant for this study in that it addresses some of the key identity-proofing matters but two mitigating aspects are to be mentioned:

- parts of the document are designed to give ANSSI flexibility in its assessment of presented solutions - especially for the 'Mapping ID attributes to applicant' phase for which few practical guidelines are provided; and

- the document is not officially published and inherently subject to changes. It is expected adjustments in the near future to reflect the anticipated ANSSI policy regarding remote identification of ID documents.

5.2.3.7 Germany: BNetzA 126/2017

5.2.3.7.1 Short description

Purpose and context: In 2016, national and EU level regulators made the concerted effort to share and exchange information to further fight international terrorism. As a result, a revised German Telecommunications Act (TKG) was subsequently adapted. Included in the Act is the requirement to collect specific subscriber data for prepaid mobile communications services (i.e. SIM Cards). Specific subscriber data means the customer should now present proof of their identity prior to purchase of any SIM card.

Verification can now be carried out by other "suitable methods", including digitally. The remote video identification verification procedures are specified in detail through the Federal Network Agency (BundesNetzAgentur) as Gazette 126/2017 [i.67]. The TKG regulation directs that these procedures come from the Federal Network Agency under paragraph § 111.

ID type: natural person.

Expected outputs: procedures for a video identification.

Sector: Telecommunications.

Legal background: Federal Network Agency decree 126/2017, per the German Telecommunications Act 2017, § 111.

5.2.3.7.2 Attribute collection

Attributes to be collected: Identity, any applicable attributes of the subject. In the case of natural person: full name (surname and given names) date and place of birth.

Type of evidence to be/that can be presented: Directly by physical presence of the person (not in the scope of this document).

Type of presentation of the attributes: Digitally, interaction by remote video identification: "*using means which provides equivalent assurance to physical presence" needs to be "using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the service provider can prove the equivalence.*"

5.2.3.7.3 Attribute validation

Determination that the ID attributes are valid (not expired, not revoked): A verification of the validity and plausibility of the data and information contained on the identity document is performed.

The employee review that the photograph and personal description on the identity document match the person to be identified. Photograph, issue date and date of birth are required to be consistent.

The automated calculation of the check digits in the machine-readable zone and the cross-check of information provided there with the information visible on the identity document are required to match. The orthography of the digits, the authority code and the typefaces used are also examined to ensure that they are correct.

The person to be identified is required to share the full serial number of their identity document during the video transmission.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): By a comparison with still images selected by the employee as part of the identification process. In addition, the employee always checks that the identity document used is undamaged and not manipulated and, in particular, that it does not contain a pasted image.

By means of enlarged still images, the employee has to verify that the identity document and the security features that can be visually recognized in white light are completely covered at the appropriate place and that the transitions do not show any artifacts that indicate a corresponding manipulation.

The optical security features include:

- Diffractive features: Holograms, identigram and kinematic structures.
- Personalization technology: Tilted laser images and typography.

- Material: Window (e.g. personalized), security thread (personalized), optically variable ink.
- Security printing: Microlettering and guilloche structures.

A match is to be assumed if the verification criteria of at least three of the security features randomly selected from different categories in the above list for the purposes of identification and possessed by the identity document are met.

The employee also ensures that the document used as proof of identity possesses the other formal features visually identifiable in white light and accessible for the purposes of inspection (including layout, number, size and spacing of characters, as well as typography) that a document of this kind typically possesses.

5.2.3.7.4 Attribute binding

Face to face interactions: Digital video interactions - during the visual inspection, the person to be identified is required to perform certain movements and answer some phycological questions by the employee.

5.2.3.7.5 Requirements of the process

What needs to be done:

The video agent verifiesthe identity of the subscriber and subject, and check that they are accurate, authorized, and complete according to the collected evidence of the identity document.

Employees need to be familiar with the features of the documents permitted in the video identification procedure as well as common counterfeiting possibilities. They should be familiar with relevant anti-money laundering and data protection regulations and the requirements set out in the Circular. Applicant provides suitable documentation on the accepted documents, including verifiable features and the corresponding training measures.

Employees are trained on these requirements before they take up their identification duties and afterwards at regular intervals, at least once a year and when the need arises.

During the identification process, the employees is situated in separate premises with restricted access.

At the beginning of the video identification, the person to be identified gives its explicit consent to the entire identification process as well as to photos or screenshots of them and their identity document being taken. This consent needs to be explicitly logged/recorded.

Video identification is performed in real-time and without interruption. The integrity and confidentiality of the audiovisual communication between the employee and the person to be identified is adequately ensured; for this reason, only end-to-end encrypted video chats are permitted.

The image and sound quality of the communication is required to be sufficiently adequate to allow unrestricted identification beyond doubt. These include the examinations of the security features which have been categorized as being visually verifiable in white light as well as the examination carried out to check if the document has been damaged or manipulated. To evaluate the quality of the image transmission, suitable informative image elements such as guilloche structures and microlettering are defined.

The employee is required to be certain that the photograph and the description of the person on the identity document used match the person to be identified.

During the video transmission process, the respective employee captures photos/screenshots which clearly show the person to be identified as well as the front and reverse of the identity document used by this person for identification purposes and the information held on the BNetzA 126/2017 [i.67].

The employee verifies that all of the details on the person to be identified provided on the identity document match those known to the obliged entity and available to the employee (where applicable).

During the video transmission, the person to be identified directly types online a sequence of numbers (TAN) which is valid only for this purpose, centrally generated and delivered to this person (by email or SMS) by the employee, that is return to the employee electronically. Once the person to be identified has entered the TAN, subject to successful confirmation of this TAN in the system, the identification procedure is completed.

The entire video identification process is recorded and retained by the obliged entity for internal and external audit and for BaFin. The records is retained for five years.

Why this needs to be done:

The recordings shows not only that the general requirements for identification under anti-money laundering law are fulfilled, but also that the minimum requirements for video identification set out in the Circular are met.

An agent check that the necessary procedures to ensure that the ID document is valid, the user is real, and that the data on the ID document corresponds with the user has been followed.

How this needs to be done:

Within the scope of the video identification procedure, a validity and plausibility check of the data and information contained on the identity document is carried out. This includes checking whether the date of issue and the validity date of the identity document match. In particular, the date of issue will not be included in the future.

Any substitution/manipulation of parts or elements of the identity document is required to be counteracted by appropriate measures. For this purpose, the person to be identified is to be asked to hold a finger in front of security-relevant parts of the identity document at a suitable (variable, randomly determined by the system) location, (e.g. a finger in front of security-relevant parts of the identity document or move one hand across their face).

During the visual inspection, the person to be identified is required to perform certain movements when requested by the employee i.e. move a hand in front of his face, the user is required to tilt the used identity document horizontally or vertically in front of the camera as instructed, and to also perform certain other movements when requested by the employee, as well as answer randomized psychological questions for plausibility.

Questions may also be asked, for example, with regard to the age of the person to validate the identity document photograph as well as the date and place of birth stated on the identity document. The reason for the identification needs to be confirmed by the person to be identified, not least so that the person is aware why such an identification procedure is necessary. The employees are trained so that they can determine beyond doubt that the person to be identified is purchasing the respective product from the provider in question of their own volition (risk posed by phishing, social engineering, behaviour when under pressure by another person, etc.).

An obligatory part of the verification is also an automated calculation of the check digits contained in the machine-readable zone and a cross-check of the information contained in it with the information in the field of vision of the identity document. In addition, the correctness of the numerical orthography, authority identification number and the fonts used is checked. The person to be identified also provides the complete serial number of his identity document during the video transmission.

5.2.3.7.6 Reference material

Title	URL
1 Konsolidierte Fassung der geänderten Verfügung der Bundesnetzagentur gemäß §111Absatz1Satz4 Telekommunikationsgesetz (Stand: 22.11.2017) [i.67]	https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Verfuegung111/verfuegung.pdf

5.2.3.7.7 Reviewer note and conclusion

The Gazette [i.67] details what needs to be validated for the specific purpose of identity verification in relation to a specific sector namely digital interactions in telecommunications. The document supports remote identity verification procedures consistent with the research of this study.

5.2.3.8 Germany. BNtAg 208/2018 on eIDAS

5.2.3.8.1 Short description

Purpose and context: The German law implementing the EU eIDAS regulation [i.1] was laid out and approved jointly by the Federal Network Agency and the Federal Office for information Security (BSI). It is known as the eIDAS Implementation Act of July 2017. The core part of the law is known as the "Confidence Services Act" (VDG), and it replaces the previous German Signature Act (SigG).

The VDG is the German law for the application of electronic signatures, seals and time stamps (trust services). The VDG gives the BundesNetzAgentur and BSI the right to determine which other identification methods within the meaning of eIDAS Article 24 (1) d are recognized and the required procedures that apply.

The hearings between BSI and the Federal Network Agency on identification methods were published as a ruling to endorse the eIDAS Regulation [i.1] and this document outlines specifications under Section 11 (1) of the VDG as an Official Gazette 11/2018 (notification no. 208). The Video identification requirements for issuing qualified web authentication certificates or qualified certificates for electronic signature are usable for a single transaction. The provisions are similar to the BaFin 03/2017 Circluar on Video identification requirements. This document does not provide complete procedural details like the BaFin Circular; rather it endorses the procedures and lists requirements.

ID type: Natural person applying for a qualified certificate using video transmission (video identification).

Expected outputs: procedures for a video identification for trust services extended until 12/2021.

Sector: Public and private sectors.

Legal background: eIDAS Regulation [i.1].

5.2.3.8.2 Attribute collection

Attributes to be collected: Natural person: simply states in the context of applying for a qualified certificate using video transmission (video identification).

Type of evidence to be/that can be presented: Digital interaction by remote video identification: specifics not detailed in this endorsement.

Type of presentation of the attributes: Not included.

5.2.3.8.3 Attribute validation

Determination that the ID attributes are valid (not expired, not revoked): The comparison of the person with an identification document are subject to relevant review criteria.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): no specification beyond the fact that documentation comes from an appropriate and authorized source.

5.2.3.8.4 Attribute binding

Only identity documents that have sufficient forgery-proof security features that can be verified in the procedure are permitted for identity verification.

5.2.3.8.5 Requirements of the process

What needs to be done: The authenticity of the identity document and the affiliation with the person to be identified is required to be reliably verified. The provider is required to take appropriate measures to detect any manipulation of the video image or identity document or person.

This can include organizational measures that make manipulation recognizable by interaction with the identification document. The agent can take technical measures to detect a change in the video stream.

Why this needs to be done: The appropriate implementation of the requirements laid down in the order is assessed by a conformity assessment body in the context of point (d), of Article 24(1) of Regulation (EU) No 910/2014.

How this needs to be done: The document [i.68] does not describe in detail how this is done. The outset is that a reliable verification fulfils appropriate measures to detect any manipulation of the video image or identity document or person.

5.2.3.8.6 Reference material

Title	URL
Verfügung gemäß § 11 Absatz 1 VDG [i.68]	https://www.buzer.de/11_VDG_Vertrauensdienstegesetz.htm

5.2.3.8.7 Reviewer note and conclusion

The document [i.68] is an endorsement for video identification, and outlines in broad terms the technical and procedural requirements for the identification of an applicant using trust services. This document is not comprehensive enough for identity verification procedures.

5.3 Banking and financial services

5.3.1 G20 Digital Identity Onboarding

5.3.1.1 Short Description

Purpose and Context: The UN has acknowledged the importance of legal identity through the Sustainable Development Goals, which calls all UN Member States to "provide legal identity for all, including birth registration by 2030." The paper makes the case for Digital Identities in developing countries.

National governments play the primary role in the registration and recognition of a legal identity. Without a formal or legal basis of an ID document, the authenticity of an identity is at risk. The inability to credibly prove one's identity can lead to economic and social exclusion and within the financial sector, it can hinder access to basic services like bank accounts or loans.

By introducing a legal, digital ID, this could potentially increase the adoption of financial services to underserved economies and geographies. A digital ID can help reduce fraud and duplication of government assistance to displaced persons or help drive the socio-economic development of minorities, often women or young girls.

The report [i.69] analyses the role that robust, inclusive and responsible ID systems can play in enhancing financial access and inclusion and outlines key policy considerations for developing nations, and takes a close look at how financial services can leverage digital ID systems to increase efficiency, enhance effectiveness, and enable new ways to conduct existing business processes in the financial sector and across government services.

ID Type: Natural person, Digital ID

Expected Output(s): A roadmap for digital identity infrastructure and policy making in developing countries.

Sector(s): E-Business, E-Government.

Legal Background: N/A.

5.3.1.2 Attribute Collection

Attributes to be collected: A person's digital identity may be compromised of a variety of attributes, including biographic data (e.g. name, age, gender, address) and biometric data (e.g. fingerprints, iris scans, handprints).

Type of evidence to be/that can be presented: Characteristics of an identification system that matter most for financial services are a legal basis, uniqueness, and the ability to exist in a digital format. The ID is required to be secure and robust and provide remote assurance that the person can be validated:

- Credentials issued by a service provider (unique ID number, eDocument, eID, mobile ID) should be used as authentication factors.

5.3.1.3 Attribute Validation

Determination that the ID attribute are valid:

An important application of digital identity for the G20 report [i.69] is account opening. Recommendations from this report highlight recommendations for an effective ID system to operate in the financial system. Attribute ***Validation*** is not described in detail here. Rather the report recommends that the authenticity, validity, and accuracy of the identity information the applicant provides relate to a living person.

Concept of Level of Assurance (LoA) is not analyzed in this report, rather highlighted as a means of achieving graded security for various e-services based on low, substantial, and high.

5.3.1.4 Attribute binding

Not in the scope of the present document.

5.3.1.5 Requirements on the process

Digital IDs are important to public policy and service delivery.

Digital infrastructure requires significant investment and support.

A digital identification system should be integrated with civil registration, with official recording of birth, death, and other vital events.

Once verification is established, a biometric registration ought be considered to bind the applicant to the identity claim:

- Registration
- Validation
- Verification
- Risk Assessment
- Maintenance
- Authentication
- Revocation

The ID proofing process for a natural person is based on a collection of various G20 country studies for a natural person. It can be broken up into 6 common requirements:

a) Registration: The registration process involves an applicant providing evidence of his or her identity to the issuing authority.

b) Validation: Where the authority determines the authenticity, validity, and accuracy of the identity information the applicant has provided and relates it to a living person.

c) Verification: Establishing of a link between a claimed identity and the real-life subject presenting the evidence.

d) Vetting/Risk Assessment: Assessing the user's profile against a watch- list or a risk-based model.

e) Issuance: The process of creating and distributing virtual or physical credentials like e-passports, digital ID cards and driver's licenses and a unique identifier (with central biometric authentication), such as the Aadhaar system in India.

f) Authentication: The process of verifying an identity claim against the registered identity information. Such information could be a personal identification number (PIN), a password, biometric data such as a fingerprint, a photo or a combination of these.

The document [i.69] does not outline at which point or when the various ID proofing steps are taken.

Each identity profile relates to one of the following topics: Identity Assurance Level, Authentication Assurance Leve, and Federation Assurance Level. These can be compared to the eIDAS LoA low, substantial, high.

Security requirements for this report are not specified. A collective set of good practices includes:

- Issuance or Credential management: Creating and distributing virtual or physical credentials like e-passports, digital ID cards and driver's licenses and a unique identifier (with central biometric authentication), such as the Aadhaar system in India
- Identity Authentication: Verifying an identity claim against the registered identity information. Such information could be a personal identification number (PIN), a password, biometric data such as a fingerprint, a photo or a combination of these.
- Authorization: Authorization takes place after an individual's claim of identity is authenticated and access rights of a 'relying party' are defined.
- Identity Management and Maintenance: Retrieving, updating, and deleting identity attributes or data fields and policies governing users' access to information and services.

5.3.1.6 Reference material

Title	URL
G20 Digital Identity Onboarding [i.69]	https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

5.3.1.7 Reviewer Note and Conclusion

The G20 report [i.69] is a case study of digital identity as a concept, policy recommendation geared towards developing countries. By reducing the digital identity gap between income wealthy nations and developing countries, the report highlights various applications that exist in several countries and points out issues such as data privacy, interoperability, challenges to displaced persons, and trends in innovation.

The document is technology neutral and simply highlights various case studies from Mexico, Peru, India, Pakistan, Estonia, and the UK.

5.3.2 BITS: Norway: Requirements for secure digital verification of identity

5.3.2.1 Short description

Purpose and context: BITS is the financial infrastructure company of the joint Norwegian banking and finance industry. BITS' purpose is to ensure a safe and efficient payment infrastructure. The former banking standardization agency is a part of BITS, meaning standards for the banking and financial sector is an important purpose. The requirements document (not available online) is the result of a broad consultation among interested parties in Norway. It represents a proposal for remote identity verification for onboarding to financial services and for issuing of eID (BankID is the common eID scheme for Norwegian banks covering 95 % of the adult population). The document [i.70] does not explicitly mention qualified certificates, but as BankID consists of authentication certificates (level high assumed) and qualified signing certificate issued in the same process, the requirements proposed for issuing of BankID are assumed to cover qualified certificate issuing for natural persons. The progress of the document [i.70] should be as a proposal from Finance Norway to the Financial Supervisory Authority, the government, and the National Communications Authority (supervisor for eID issuers and trust services). While there seems to be broad approval of the document's contents, the pace of eventual progress to guidelines approved by authorities is not known.

ID type: natural persons.

Expected outputs: The document [i.70] has concrete recommendations for remote identity verification mechanisms that are proposed to be accepted as sufficient relatively to "profiles" of intended use cases.

Sector: The document [i.70] defines several "profiles" with different requirements, divided into financial sector, public sector, and private sector. Financial has three profiles with different strengths, the other two have two profiles each.

Legal background: The document [i.70] is currently only a recommendation. Further progress to Norwegian authorities towards an official status is not known.

5.3.2.2 Attribute collection

Attributes to be collected: This is not a topic of the document [i.70]. Probably because the requirements are well-known and established for financial services: Full name, national ID number, date of birth, postal address. For financial services, and for eID and qualified certificates, information is verified against the population register, where official address is fetched. The other attributes are obtained from the identity document used and verified against the population register.

Type of evidence to be/that can be presented: Primarily passport or national ID card but other documents can be in scope.

Type of presentation (of the attributes): The document [i.70] describes a client-side application, which usually will be an app on a mobile phone but that also may be a self-service kiosk or similar. Documents are read (NFC reading or optical scanning) by use of this application. This application also provides a "selfie" picture used for facial biometrics comparison with picture from the document.

5.3.2.3 Attribute validation

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): The document [i.70] describes a server-side application in a secure environment. This application analyses the document presented to determine that the document is real and not tampered with.

Determination that the ID attributes are valid (not expired, not revoked): Common practice in Norway is to check attributes towards the national population register based on the national ID number obtained from an identity document. The BITS document [i.70] lists this check/lookup as optional, stating that attributes gathered from a genuine, official ID document may be considered to be true. A lookup in the population register is necessary if verified physical address is needed since this attribute is not present for ID documents.

5.3.2.4 Attribute binding

Done by use of facial biometrics to verify that the identity document, and hence the information obtained from the document, are for the person present. Additional attributes can be obtained from the population register or from other sources, usually based on lookup using the national ID number.

5.3.2.5 Requirements on the process

The document's main purpose [i.70] is to pose security and functional requirements to obtain as outcome a verified identity at a certain level, defined as a set of profiles. The document does not outline in detail process requirement but briefly assumes a general process for a server-based implementation.

Security requirements:

The document [i.70] lists many security and functional requirements, some common to all profiles, other specific to certain profiles:

- Requirements for optical scanning of documents are posed, with validation requirements.
- Requirements to NFC reading of documents are posed, with validation requirements.
- Requirements for subject biometrics capture with liveness detection are posed.
- Resistance against biometric attacks is described, referring ISO/IEC 30107 ([i.32], [i.31], [i.118] and [i.28]) series of standards on biometric presentation attack detection.
- Requirements for (security of) the client-side application (usually mobile app) are posed.
- Requirements for (security of) the server-side application are posed.

- Requirements for verification of identity by the server-side application are posed.
- Some best practices guidelines are described in appendixes, including measures to increase the probability of the existence of identity to increase the confidence level.

5.3.2.6 Reference material

Title	URL
BITS, Norway, Requirements for secure digital verification of identity November 2019 [i.70]	https://www.bits.no/en/about-bits

5.3.2.7 Reviewer Note and Conclusion

As the document [i.70] goes into details on security and policy requirements, it can be important input to this study. The document should be one of those used for ETSI DTS/ESI-0019461 [i.50].

The document [i.70] is very relevant to this study because it contains specifications of solutions that are suggested as sufficient for specific purposes, e.g. NFC reading of chip in identity document for eIDAS high eID (and qualified certificate) provided that certain security measures are in place. Optical remote reading of an official identity document is suggested as sufficient for eIDAS substantial, provided that certain security measures are in place.

5.4 Services subject to AML rules

5.4.1 Directive (EU) 2018/843 of the European Parliament and of the Council amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('AMLD5')

5.4.1.1 Short description

Purpose and context: As its name suggests, AMLD5 [i.71] is an EU instrument that updates and adjusts the existing EU anti-money-laundering framework, by *inter alia* extending the scope of persons subject to the anti-money laundering and counter terrorism financing requirements, addressing new technological evolutions, strengthening customer due diligence measures, introducing new transparency requirements and giving enhanced powers to supervisory authorities and EU financial intelligence units. Its purpose is therefore considerably wider than the topics considered by this study, which are only summarily considered by AMLD5 - see below. An important aspect of AMLD5 [i.71] is that it is closely related to the work of Financial Action Taskforce (FATF), the global money laundering and terrorist financing watchdog, and should be viewed in conjunction with the FATF Recommendations [i.124] in many ways, AMLD5 'imports' the FATF Recommendations into the EU legal framework on an 'as is' basis. Another key aspect of AMDL5 [i.71] is that it is a directive, not a regulation, and therefore has no direct effect on EU citizens - it is up to each Member State to ensure that its relevant provisions are incorporated into national law. Last but not least, AMLD5 is a 'minimum harmonisation' directive and leaves significant discretion to Member States in a number of key areas, including critically identity matters - a matter that has drawn criticism and may lead to regulatory changes in the future.

ID type: AMLD5 [i.71] applies to Obliged entities, meaning persons subject to AML/CFT requirements for the provision of professional services (including, but not limited to, financial sector entities) to clients, irrespective of whether these are natural or legal persons.

Expected outputs: AMLD5 [i.71] only cursorily addresses identity-proofing topics through the following sentence, amending article 13(1): "*Obliged entities shall identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source,* ***including, where available, electronic identification means, relevant trust services as set out in [the eIDAS] Regulation or any other secure, remote or electronic identification process regulated, recognized, approved or accepted by the relevant national authorities"***; (note that only the bold section is new).

Sector: AMLD5 [i.71] applies to Obliged entities, meaning persons subject to AML/CFT requirements for the provision of professional services (including, but not limited to, financial sector entities).

Legal background: AMLD5 [i.71] amends AMLD4, and has already been amended on minor points since its adoption.

5.4.1.2 Attribute collection

Attributes to be collected: No specific provision.

Type of evidence to be/that can be presented: No specific provisions.

Type of presentation: No specific provisions.

5.4.1.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): no specific provision.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): no specific provisions

Other checks implemented if any: no specific provisions

5.4.1.4 Attribute binding

No specific provisions.

5.4.1.5 Requirements on the process

No specific provisions.

AMLD5 [i.71] is the leading AML/CFT regulatory framework defining key EU regulatory requirement for Know-Your-Client ('KYC') processes, but the identity-proofing provisions of AMLD5 amending article 13(1) are designed to leave considerable discretion to Member States to define how identity proofing takes place. Indeed, there are no common AMLD5 requirements as to how identity proofing processes should be implemented nor as to which minimum level of assurance should be required. The acceptance of electronic identification means and digital trust services is a welcome development of AMLD5 [i.71] (AMLD4 only recognized electronic signature) but brings only limited clarity in that it defines no common recognition criteria and includes in addition a blanket acceptance of any eID scheme or trust service *regulated, recognized, approved or accepted by any relevant national authority*. It is indeed rather unusual for an EU harmonisation instrument (such as a Directive) to offer an unconditional acceptance and recognition of any decision of a member State without common requirements or criteria, but this should be viewed as reflecting a policy decision at the time as well as highlights the sensitivity and reluctance of member States when it comes to addressing identity matters at EU level.

As a result, operational guidance for the implementation of identity-proofing processes in line with AML/CFT requirements is to be found in the FATF Recommendations or, critically, in the national KYC framework of each members State, rather than in AMLD5 [i.71].

Although initially favourably received by the financial sector, the current wording is now widely viewed as in need of adjustment and a contributing factor behind the fragmentation of the KYC requirements within the EU. It is a also recognized as inconsistent with the single market and banking passport principles set out in EU regulations and facilitating regulatory arbitrage.

The ECOFIN has recently instructed the EU Commission to consider an AML Regulation replacing the current AML Directives and work is now starting on this, therefore opening the prospect of greater consistency of KYC processes throughout Europe.

5.4.1.6 Reference material

Title	URL
Directive (EU) 2018/843 of the European Parliament and of the Council amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ('AMLD5') [i.71]	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843

5.4.1.7 Reviewer Note and Conclusion:

Although an important piece of EU regulation for the financial sector in many respects (which are not relevant or discussed here), AMLD5 [i.71] brings only limited guidance on identity-proofing matters and highlights the fact that, for KYC matters:

- broad principles are to be found in the FATF Recommendation (and recent Digital Identity Guidance); and
- detailed rules are primarily to be found in national regulations.

5.4.2 EC Report on Existing Remote On-Boarding Solutions in the Banking Sector

5.4.2.1 Short Description

Purpose and Context: This report [i.72] assesses the risks, associated counter measures, and the interoperability of remote identification solutions in the banking finance sectors throughout the EU and EEA. The document provides an overview and detailed analysis of existing remote identification solutions, its use in banking, as well as perspectives on risks, mitigating risks, and their functionality.

The report [i.72] also makes recommendations for conformity assessment principles for onboarding systems and electronic identity management systems.

The report [i.72] offers perspectives on varying approaches toward identity verification to help the EU Commission's considerations for a more integrated identity verification system in the future.

ID Type: Natural and legal persons.

Expected Output(s): Identifying key finding as basis for policy decisions on greater EU interoperability and integration of verification systems.

Sector(s): banking finance sectors, e-commerce payment providers.

Legal Background: National EU AML Acts and AMLD 5 (taken into consideration as states transpose the Directive).

5.4.2.2 Attribute Collection

Attributes to be collected: Attributes such as name, DoB, and may include address.

An eID/KYC evaluation grid was created to support consideration of any remote on-boarding solutions based on EU 2015/1502 [i.3] and eIDAS Cooperation Network guidelines, EBA opinions, UK Joint Money Laundering Steering Group, and national AML laws.

An inventory list of existing remote onboarding solutions was compiled with vendor presentations.

Type of evidence to be/that can be presented:

a) Consideration of type and content of document:

- EBA considers high security features or biometric data including fingerprints and facial image (i.e. passports and eID);
- A QES created in line with eIDAS;

- A feature that links the innovative solution with trade registers or other reliable data sources such as the company registration office database.

b) Capture - Video & Photo Capture.

c) Verification- Authenticity and Validity of Documents:

- Electronic verification can also be run through private systems like Bank ID or Verimi and Deutsche Bank via video identification:
  - document valid;
  - eID has been set up by Verimi in less than 24 months;
  - communication handled via secure channel;
  - underlying documents are distributed
  - Not possible for a Verimi ID to be reused in a three party way where a different bank or system performed the identification and sends it to Verimi for further sharing.
- UK JMLSG example: Guidelines state that the firm should obtain the following information in relation to the private individual:
  - Full name.
  - Residential Address.
  - Date of birth.
- Video and Photo Capture example.

Under eIDAS regulation [i.1], when capturing photos and videos as part of the identification process, a number of considerations should be given including the image quality requirements (e.g. ISO/IEC 19795-1 [i.117], light quality, number of pixels, distance of subject from camera), the potential need for real time video analysis and how the image is stored. When using remote onboarding solutions, ways to make use of identity evidences containing a photo and where possible to make use of biometric algorithms to compare the applicant with the claimed identity should be considered.

5.4.2.3 Attribute Validation

Attribute validation for an identification should consider risks due to tampering during transmission.

Firms should have sufficient robust controls in place to reduce risk, such as:

- A feature whereby the customer is required to have a live chat to monitor unusual behavior.
- A built in computer application that automatically identifies and verifies a person from a digital image or a video source (i.e. biometric facial recognition).
- Requirement for a screen to be adequately illuminated when taking a person's photograph or recording a video during the identity verification process.
- A built-in security feature that can detect images that are or have been tampered with (e.g. facial morphing) whereby such images appear pixelated or blurred.

Attribute Validation for an identification should consider risks due to similarity fraud. An ID document displayed on the screen by a customer during the transmission belongs to another but similar looking person. ESA considers that firms should ensure that the CDD solution contains built in features that enable it to identify any discrepancies, or that staff responsible for the identity verification during the transmission have been trained.

Validity and Authenticity of Documents:

- Validity - a verification status of the document is made against an authoritative source (public or private).

- Authenticity - to verify, authenticate and validate documents used in remote on-boarding, there are considerations to be followed under eIDAS. A comparison to existing public sources (i.e. PRADO [i.86]) should be used:
  - Beneficial in identifying counterfeit documents.
  - Ensuring features are correct.
- ESA underlines that firms should have sufficient controls in place to prevent or reduce the risk of breaches like forgery or counterfeiting:
  - Built in features which enable then to detect fraudulent documents on the basis of security features (i.e. watermarks, biographical data, photographs, lamination, UV sensitive ink lines) and the location of these features (i.e. optical character recognition OCR).
  - Features that compare the security features ingrained in the identity document presented during the transmission with a template of the same document held in the firms' internal identity document database
  - Where the verification is not based on a government issued identity document, to the extent permitted by national law and money laundering risk, features that allow firms to verify the information received from the customers against a combination of multiple reliable sources and can be supplemented with data analysis, IP address analysis, and location or device analysis.

5.4.2.4 Attribute binding

Communications should be secured e.g. through Transport Layer Security (TLS) or cryptographic protocols to guarantee authentication and integrity of transactions and confidentiality.

5.4.2.5 Requirements on the process

Based on the analysis of the different approaches to identification means, the report mapped customer journeys into 7 main typical categories. The exact process/journey and the identity verification solutions employed will vary depending on the financial institution, maturity of the markets, and the countries in which they operate.

8 typical identification journeys listed:

- Cross Channel (Remote face to face).
- Remote onboarding based on enhanced KYC measures with or without e-signature.
- Entirely remote on boarding using video conference and biometric identification (optional).
- Entirely remote on boarding supported by selfie and biometric identification.
- Entirely remote on boarding resulting in trust services created.
- Entirely remote on boarding using digital identity.
- Remote onboarding employed by e-merchants using electronic wallet.
- Certification - The level of Assurance of remote identity registration solutions should be assessed by a conformity assessment body or equivalent and solutions should be certified (e.g. ISO/IEC 27001 [i.24], or other certification to be considered).

The ID proofing process for **natural persons** is compared through 7 different onboarding journeys with 3 comparable procedural requirements for an AML and eIDAs process. The process of each ID check journey is evaluated for their use of technical measures, organizational measures, or combinations of both:

a) Authenticity checks:
   - Comparison against reference databases (e.g. PRADO [i.86]) or other sources providing detailed information about identity documents.
   - All features (MRZ or not) correct.

- Syntax.
- Laminate- Physical security features in the documents, for e.g. ripples/backgrounds, holograms.
- Consistency (e.g. check-digit). Some attributes on an identity documents might include a 'check-digit'. This is often the last part of a numeric field which is derived from the first part (e.g. modulo '97).
- Is the photo the genuine?
- If not checked against an authoritative source how is this check for remote onboarding?
    - At High level, the photo has to be checked against an authorized source. That could be directly possible with the use of the chip containing the photo, or towards a national database.
    - Appropriate training of staff checking the physical documents with a good knowledge of the documents design and their security features; skills for identify forged documents, by inspecting them; and to use the equipment in an appropriated way (for example ultra violet lights).

b) Validity checks.

Under eIDAS regulation [i.1], the following criteria have to be met: status verification lost, stolen, expired against 'authoritative source' (private or public).

The Level of Assurance of remote identity registration solution should be assessed by a conformity assessment body (or equivalent) and solutions should be certified (e.g. ISO/IEC 27001 [i.24], or other certification to be considered).

c) Identity check of the applicant.

For remote registration of identities, the identity proofing should be based on more than one identity evidence. The claimed identity should be informed of the ongoing registration by an alternative channel (i.e. not specified by the applicant) to counter identity spoofing.

Regarding documents/ -capture -video/photo:

- Follow Commission implementing regulation (EU) 2015/1502 [i.3] requirements for level Substantial (steps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence"), and the comparison of physical characteristics of the applicant against the evidence.
- Image quality requirements (e.g. ISO/IEC 19794-5 [i.37], light quality, number of pixels, distance of subject from camera).
- Capture evidences (videos, selfies) record for future investigation. Real time (video) analysis is needed, with image quality requirements (e.g. ISO/IEC 19794-5 [i.37]) (light, pixels, distance camera toward object/subject).

The different parts of the Identity process can be performed at once or over a period of time, depending on the journey.

Each industry profile relates to one of the following levels of confidence for financial KYC/AML regulations, either substantial or high.

Security Requiremnts: Yes, under eID/KYC criteria, the report assesses KYC processes at eIDAS minimum levels substantial and substantial or high for digital eID processes. The report's statements on each achievable eIDAS LoA is only an estimation and should not be considered definitive. The assessment method for the ID proofing considers two identification steps: ID document verification (composed of ID document authenticity and validity verifications), and verification that the applicant has the claimed identity.

5.4.2.6 Reference material

Title	URL
Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions - December 2019 European Commission. Directorate-General for Financial Stability, Financial Services and Capital Markets Union [i.72]	https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/report-on-existing-remote-on-boarding-solutions-in-the-banking-sector-december2019_en.pdf

5.4.2.7 Reviewer Note and Conclusion

The scope falls within this study to collect and evaluate the various onboarding KYC methods that exist in relation to national EU AML laws as well as eIDAS regualtions for use with QTSPs for an identification and e-signature.

The Report [i.72] is quite relevant and useful as it lists and outlines the various KYC methods of different EU member states and lists risks associated with remote identification and counter measures. This report is not a "binding" document.

5.4.3 EU commission eID/KYC expert group '*assessing portable kyc/cdd solutions in the banking sector*' report ('report2')

5.4.3.1 Short description

Purpose and context: Report2 [i.73] is one of the two reports prepared at the request of the EU Commission by the eID/KYC Expert Group including representatives of EU regulatory authorities and IT agencies as well as private sector participants appointed in 2018 for the purpose of considering the ways and means of KYC portability within the EU financial sector. Report2 is focusing on the feasibility of an attribute-based framework for the banking sector leveraging the eIDAS levels of assurance and complements another report presenting existing remote onboarding solutions in the EU banking sector. Report2 discusses a proposal that has yet to be implemented and is therefore more prospective in nature. Generally speaking, Report2 makes the case for an attribute-based LoA-rated eKYC framework within the EU and discusses its features, technical requirements and structural implications. It does so by extending to customer due diligence attributes customarily used by the banking sector the LoA-rated approach used by eIDAS for customer identification. It should also be noted that Report2 [i.73] builds on the work of the 2018 PwC 'study on eID and digital onboarding' and aims to cover KYC portability requirements in general - a topic which is considerably wider than identity-proofing.

ID type: Report2 [i.73] applies both the natural and legal persons. It also addresses the situation of a natural person representing a legal person.

Expected outputs: Report2 [i.73] suggests an analytical framework for remote onboarding processes of the banking sector as well defines its key features but the practical implementation of the framework is entirely dependent upon actions of the EU Commission and other regulatory authorities.

Sector: Report2 [i.73] clearly applies to the banking sector and therefore discusses and integrates some of the key Anti-money-laundering requirements applicable to providers of financial services.

Legal background: Report 2 [i.73] was prepared by the EU Eid/KYC Expert Group created by EU Commission decision dated 14 December 2017 but, although officially approved by the EU Eid/KYC Expert Group, has no legal effect and does not bind the EU Commission in any respect.

5.4.3.2 Attribute collection

Attributes to be collected: Report2 [i.73] defines KYC attributes typically requested by providers of financial services and categories them in three main types (core identity attributes (individuals/legal entities); status or 'good standing' attributes and contact attributes). This reflects the fact that the banking sector needs, in order to comply with customer due diligence requirements, more attributes than core identity attributes - see page 22 of Report2 [i.73].

However, Core identity attributes are defined as date of birth, place of birth, given name, family name, gender, nationality and individual identifier (individuals) and legal name, legal form, registration authority and legal identity identifier (legal entities).

Report2 [i.73] recognizes that KYC attributes need to be 'refreshed' (reverified) from time to time and suggests a methodology primarily based on the risk-based approach advocated by the Financial Action TaskForce, the global forum in charge of coordinating anti-money-laundering requirements. It also offers a determination of various levels of assurance for the KYC attributes that mirrors the eIDAS classification (Low, Substantial & High) - see pages 26 to 30.

Type of presentation: Report2 [i.73] recognizes that identity attributes tend to be communicated as part of an existing eID (eIDAS or non-eIDAS) or extracted from an existing ID document presented remotely. It focuses on the latter alternative (remote presentation of ID documents) and suggests a LoA-sensitive approach which takes into account the ability to withstand 'basic', 'moderate' or 'high' potential attacks - see page 18.

5.4.3.3 Attribute validation

Report2 [i.73] offers a summary description of the customary document checks to be performed in connection with the remote presentation of ID document. For example, basic document checks are to be performed for all LoAs whereas advanced document checks (including the validation of the security element of the ID document or the electronic validation of the ID attributes) are to be performed for Substantial and High LoAs - see page 18.

5.4.3.4 Attribute binding

Report2 [i.73] also offers a summary description of the 'presence detection requirement' linking the ID document to the person purporting to be its legitimate holder. However, these tend to be defined in general terms and make reference to the corresponding eIDAS requirements as per EU Implementation Regulation 2015/1502 [i.3].

5.4.3.5 Requirements on the process

Apart as stated above in relation to page 18 of Report2, Report2 [i.73] does not address identity-proofing requirements as such.

Both reports of the EU eID/KYC expert group were approved and endorsed by its members in December 2019 and published in February 2020 by the EU Commission, but these are not binding on the EU Commission, which has complete freedom to decide what to do with them.

Security requirements: Y/N

5.4.3.6 Reference material

Title	URL
Banking Assessing portable KYC/CDD solutions in the banking sector: The case for an attribute-based & LoA-rated KYC framework for the digital age - December 2019 European Commission. Directorate-General for Financial Stability, Financial Services and Capital Markets Union [i.73]	https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/assessing-portable-kyc-cdd-solutions-in-the-banking-sector-december2019_en.pdf

5.4.3.7 Reviewer note and conclusion

Report2 [i.73] offers a far-reaching discussion as well as a structured proposal on KYC portability, a topic of key importance to the financial sector which includes a 'customer identification' dimension but only cursorily discusses identity proofing matters and has no regulatory impact per se. It should therefore be seen as a proposal document which may lead to regulatory changes but has no specific authority in itself.

5.4.4 FATF digital identity guidance

5.4.4.1 Short description

Purpose and context: The Guidance [i.74] defines broad principle-based recommendations for the regulatory recognition of digital identity solutions in connection with Anti-Money-Laundering/Combat Terrorism Financing ('AML/CFT') processes used by the financial sector and other regulated services. The document clarifies the use of the FATF Standards in a digital context, especially the requirement to '*Identify the customer and verify that customer's identity using reliable, independent source documents, data or information'* (Customer Due diligence - FATF Recommendation 10) and is a key milestone for the recognition of eID solutions in the financial sector. When robust digital ID solutions are available, the Guidance determines that the absence of face-to-face interactions is no longer a higher risk factor and puts considerable emphasis on the risk-based approach, leading it to recommend that regulated entities assess the robustness/assurance level of a contemplated digital ID solution and satisfy themselves that it be sufficient for the risk profile of the contemplated client relationship.

ID type: natural persons only (the Guidance [i.74] does not address the situation of legal persons' representative(s)).

Expected outputs: The guidance [i.74] offers 'recommendations', in practice broad guidelines, to regulatory authorities, regulated entities as well as digital ID service providers for the KYC recognition of digital ID systems.

Sector: All entities subject to AML/CFT requirements, especially financial sector entities.

Legal background: The FATF is the international organization coordinating AML/CFT processes and issuing AML/CFT recommendations for regulatory authorities.

5.4.4.2 Attribute collection

Attributes to be collected: The Guidance [i.74] does not mandate (or make recommendations as to) which attributes are to be collected but notes that:

(i) governments have considerable flexibility in determining the attributes and evidence required to prove official identity; and

(ii) attributes are customarily biographic (e.g. name, age and date of birth), but also 'static' biophysical biometric (e.g. fingerprints, iris patterns, voiceprints and facial recognition) and increasingly 'dynamic' biomechanical biometric (e.g. keystroke mechanics).

Type of evidence to be/that can be presented: The Guidance [i.74] does not mandate (or make recommendations as to) how attributes are to be presented but notes that the presentation process can either be physical (documentary) or purely digital, or a digital representation of physical attribute evidence (e.g. a digital representation of a paper or plastic driver's license). It also notes that certain situations require significant flexibility in the deployment of identity-proofing processes (for example migrants and refugees)

Type of presentation (of the attributes): The Guidance [i.74] does not mandate (or make recommendations as to) how attributes are to be presented but notes that with the development of digital technologies and 'open data' interactions, identity evidence can be remotely verified and validated against third party digital databases.

5.4.4.3 Attribute validation

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): The Guidance [i.74] does not mandate (or make recommendations as to) how attributes are to be validated but notes that this process customarily takes place by checking the identity information/evidence against an acceptable (authoritative/reliable) source to establish that the information matches reliable, independent source data/records.

Determination that the ID attribute are valid (not expired, not revoked): not addressed or discussed by the Guidance [i.74].

5.4.4.4 Attribute binding

The Guidance [i.74] does not mandate (or make recommendations as to) how attributes are to be related to applicants but notes this can occur by asking the applicant to take and send a mobile phone video or photo with other liveness checks; compare the applicant's submitted photo to the photos on the passport identity evidence or the photo on file in the government's passport or license database; and determine they match to a given level of certainty. In order to tie this identity evidence to the actual real-person applicant, an enrolment code can be sent to the applicant's validated phone number which is tied to the identity, with the applicant having to provide the enrolment code, therefore verifying that the applicant is a real person, in possession and control of the validated phone number.

5.4.4.5 Requirements on the process

See mapping ID attributes.

5.4.4.6 Reference material

Title	URL
FATF digital identity guidance MARCH 2020 [i.74]	https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

5.4.4.7 Reviewer Note and Conclusion

The Guidance [i.74] is an important milestone document - the first with a global impact to consider the implications of digital ID solutions on KYC rules as applied by the financial sector and other entities subject to AML/CFT requirements. However, its use for this study is limited in that it puts considerable emphasis on the risk-based approach and does not dictate any particular outcome or requirement for identity proofing processes.

The Guidance's [i.74] purpose is not to assess or regulate digital ID systems per se but clarify how they can be meaningfully used as part of Customer Due Diligence requirements by entities subject to AML/CFT requirements. Its presentation of digital ID systems therefore tends to be mainly descriptive.

The Guidance [i.74] recognizes that identity-proofing processes can be delivered by a single or multiple service providers acting as 'Identity Service Providers' (IDSPs) that are key participants in digital ID systems.

The Guidance [i.74] was prepared with the assistance of the World Bank teams involved in ID4D projects and includes a description of the leading eID schemes as well as a presentation of the key structure and components of customary digital ID solutions and systems.

Although technically non-binding, FATF guidelines and recommendations (including the Guidance [i.74]) are usually recognized as authoritative and often reflected verbatim in AML/CFT regulations, especially by the EU Anti-money-laundering directives.

As a non-binding document intended to be used in all jurisdictions and regulatory frameworks, the Guidance [i.74] refrains from adopting a prescriptive approach for identity-proofing processes and has clear focus on financial inclusion, leading it to focus on a risk-based approach, where lower risk situations can lead to using less stringent digital ID solutions with lower assurance levels. This is one of the reasons why the Guidance does not include minimum requirements for AML/CFT processes.

5.4.5 National Bank of Belgium Object of the identification and identity verification: Comments and recommendations

5.4.5.1 Short description

Purpose and context: this information [i.75] gathers the comments and recommendations of the National Belgian Bank on how to perform identification and identity verification in the framework of the anti-money laundering and fighting terrorism legislations.

ID type: "customers" i.e. natural or legal persons

Expected outputs: KYC - new and existing financial institution customers

Sector: bank and finance

Legal background: Anti-Money Laundering Regulation of the National Bank of Belgium: of 21 November 2017 and eIDAS

Anti-Money Laundering Law: the Law:

(i) defines the objectives to be achieved when performing these obligations;

(ii) establishes the level of requirements in cases of "standard risk";

(iii) requires these requirements to be strengthened in high-risk situations; and

(iv) allows them to be relaxed in low-risk situations.

In accordance with Articles 26, § 1, and 27, § 1, of the Anti-Money Laundering Law, see [i.75], fulfilling the obligations to identify and verify the identity of the persons involved requires:

- collecting relevant information on these persons that enables them to be distinguished from any other person with reasonable certainty, as well as;
- checking all or part of the identification data collected against one or more supporting documents or reliable and independent sources of information which enable this data to be confirmed, in order to have a sufficient degree of certainty regarding the identity of the persons involved.

These objectives should be pursued regardless of the level of money laundering risks associated with the business relationship or transaction concerned, but the degree of certainty to be achieved is determined according to the risk level assigned on the basis of the individual risk assessment.

NOTE 1: Neither the Anti-Money Laundering Law nor the Anti-Money Laundering Regulation of the National Bank of Belgium lists the supporting documents or the reliable and independent sources of information that can or should be used to fulfil the obligation to verify the identity of the persons involved. Consequently, each obliged financial institution is required to incorporate in its money laundering. risk management policy an appropriate reference framework For this purpose the National Bank of Belgium recommends that the procedure relating to the customer and transaction due diligence measures (the part on *"identification and verification of the identity of customers, agents and beneficial owners"*) include a correlation table of the supporting documents accepted for each risk class, as well as a list of the circumstances in which certain supporting documents need not be submitted.

NOTE 2: The studied document makes a reference to the *ESA opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process*. This document is also considered in the present analysis. It offers a method to assess the risks inherent to non-face-to-face verification solutions. It also provide factors to consider to assess transmission of customer's ID documentation, data or information via video conferences, mobile phone apps or other digital means.

5.4.5.2 Attribute collection

Attributes to be collected: see [i.75], Article 26, § 2, of the Anti-Money Laundering Law of the 18/09/2017:

- Natural persons: last name, first name, date and place of birth and, to the extent possible, address
- Legal person: corporate name, registered office, the list of his directors and the provisions governing the power to make binding agreements on behalf of the legal person
- Trust or a similar legal arrangement: corporate name, the information referred to in 1°or in 2°regarding its trustee(s), its founder(s) and, where appropriate, its protector(s), as well as the provisions governing the power to make binding agreements on behalf of the trust or similar legal arrangement

The identification data relating to the **address** of natural persons and to the place and date of birth of beneficial owners need only be collected "to the extent possible".

The European Regulation on transfers of funds (Article 4(1)) see [i.75], requires transfers of funds to be accompanied by specific identification information, namely:

(i) the payer's name;

(ii) the payer's payment account number; and

(iii) one of the following additional information elements: the payer's address, official personal document number, customer identification number or date and place of birth.

Type of evidence to be/that can be presented: Neither the Anti-Money Laundering Law nor the Anti-Money Laundering Regulation of the National Bank of Belgium lists the supporting documents or the reliable sources of information that may be used to verify the identification data of the person concerned. **Consequently, each financial institution should include this list in its internal procedures** relating to the identification and verification of the identity of the persons concerned. This list should be based on an assessment of the level of reliability of each supporting document or source of information. The National Bank of Belgium recommends:

a) Verification of the identity of natural persons:

   1) Identity card and passport : these supporting documents should include a photograph of their legitimate holder and thus enable a visual check to reduce the risk of identity theft.

   2) Other official documents : this is for customer without an identity card or a passport - temporary and/or to be corroborated by other supporting documents.

   3) eIDAS "electronic identification means" can be used in standard-risk situations- taking account of the conditions relating to the identification of the person concerned upon the creation of the electronic identification means, of the specific qualities of the service provider who issued the electronic instrument concerned, of the instrument's "assurance level" and of any other relevant element.

   4) Use of other innovative technological instruments: based on a prior analysis conducted by the financial institution itself of the reliability of these new instruments with regard to the objective set out in Article 27, § 1, of the Anti-Money Laundering Law (see [i.75]). The National Bank of Belgium expects this analysis to be correctly documented and recommends taking full account of the Opinion of the ESAs dated 23 January 2018 on the use of innovative solutions. Innovative solutions can be:

      - involve non-face-to-face verification of customers' identity on the basis of traditional identity documents (e.g. a passport, a driving licence or a national identity card) through various portable devices such as smartphones;

      - enable the verification of customers' identity through other means, e.g. central identity documentation repositories (often referred to as 'KYC utilities').

   5) Copies of supporting documents and consultation of the National Register (ndlr to check that the document is not revoked): possible but there is no face 2 face check.

   6) Consultation of the register of beneficial owners: requires to take additional measures to corroborate the data obtained by consulting the register.

b) Verification of the identity of companies and legal persons : using documents that are generally accepted in Belgian law as proof of their existence, such as the latest coordinated statutes or the updated statutes of the company or legal person that have been lodged with the Commercial Court or published in the annexes of the Belgian Official Gazette.

c) Natural persons in association with legal person:

   - As regards the list of directors of companies and legal persons governed by Belgian Law, financial institutions should make use of the publication of their appointment in the Belgian Official Gazette. Other documents can also be accepted, such as the publication in the Belgian Official Gazette of notarial deeds in which these persons are mentioned as directors, or the annual accounts filed with the National Bank of Belgium.

   - Provisions governing the power to make binding agreements on behalf of the company or legal person governed by Belgian law should be established using the latest publication of the representational powers of this company or legal person in the Belgian Official Gazette.

- These supporting documents can be obtained from the customer himself, from official sources such as the Belgian Official Gazette or any other sources of information that can be considered reliable such as the Crossroads Bank for Enterprises established by the Law of 16 January 2003, or from other sources of the same nature created by the Member States governing the foreign companies and legal persons.

- Financial institutions can also use the "electronic identification means" issued to companies and legal persons in accordance with Regulation (EU) No 910/2014 of 23 July 214 and with Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 [i.3] on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of the aforementioned Regulation (EU) No 910/2014. As is the case for the verification of the identity of natural persons, the NBB expects institutions that authorize the use of these instruments to fix the terms and conditions for their use based on an analysis of the level of reliability.

Type of presentation (of the attributes): Direct inspection and Indirect presentation of the ID attributes.

5.4.5.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): In case of doubt regarding the legitimacy of an identity card presented, it is however recommended to verify that it has not been registered as stolen or lost in the ad hoc database of the Home Affairs.

Determination that the evidence is genuine:

- All identification data collected on the person concerned should be checked against supporting documents or reliable and independent sources of information to confirm their accuracy.

- When financial institutions verify the customer's identity by electronically reading the data registered on the microprocessor of his identity card, there should also be a simultaneous electronic verification to ensure that the data included on the chip was signed electronically by the National Register (i.e.this is feasible for all ICAO 9303 [i.87] MRTD SoD's signature provided the CSCA cert. and CRLs are available). This implies CRL check.

5.4.5.4 Attribute binding

If the person to be identified is a natural person subject to a face-to-face identification, his identity should generally be verified using his valid official identity documents such as his identity card or, where appropriate, his passport. It should be noted that these supporting documents should include a photograph of their legitimate holder and thus enable a visual check to reduce the risk of identity theft.

When using eID cards identification data can also be verified remotely through the information registered on the microprocessor of the Belgian electronic identity card. However, it should be noted that this verification may be less reliable than a face-to-face verification as it does not allow for a visual check using the photograph included in the supporting document to ensure that the person using it is indeed its legitimate holder. A financial institution using this method of verifying the identity of the persons involved should implement measures that enable it to ensure that the objective set out in Article 27, § 1, of the Anti-Money Laundering Law (see [i.75]) will be met notwithstanding the lack of a visual check, where appropriate by implementing an additional verification means.

If a financial institution intends to make use of innovative technology, the National Bank of Belgium recommends taking full account of the ESA's opinion on innovative technologies that asks that the following risks are considered:

a) A risk that the customer's image visible on the screen is being tampered with during the transmission.

b) Risk that an ID document displayed on the screen by a customer during the transmission belongs to another but similar-looking person?

c) Risk linked to non-face to face (intimidation, etc.).

d) Geographical risks.

e) Controls in place to ensure that identity documents produced during the transmission have not been altered:

   1) built-in features which enable them to detect fraudulent documents;

2) features that compare the security features ingrained in the identity document presented during the transmission with a template.

3) limiting the type of acceptable identity documents to those that contain:

   - high security features or biometric data;
   - a qualified electronic signature;
   - a feature that links the innovative solution with trade registers;
   - a feature that adjoins the innovative solution with the government-established CDD data repository or the notified e-ID scheme.

4) where the verification is not based on a government-issued identity document, to the extent permitted by national law and commensurate with the ML/TF risk, features that allow firms to verify the information received from their customers against a combination of multiple reliable and independent sources (including, but not limited to, government registers and databases), which can be supplemented with data mining and social network analysis, IP address analysis, and location or device analysis;

5) to identify suspicious transactions:

   - available data and information used in this process, and are they considered reliable;
   - controls are provided to counter the non face to face situation (live chat, multiple factors and data sources).

5.4.5.5 Requirements on the process

What needs to be done (and why):

Fulfilling the obligations to identify and verify the identity of the persons in accordance with Articles 26, § 1, and 27, § 1, of the Anti-Money Laundering Law by:

a) collecting relevant information on these persons that enables them to be distinguished from any other person with reasonable certainty, as well as;

b) checking all or part of the identification data collected against one or more supporting documents or reliable and independent sources of information which enable this data to be confirmed, in order to have a sufficient degree of certainty regarding the identity of the persons involved.

How this needs to be done:

Besides the recommendation on identity attributes and evidence collection and mapping with the applicant, the document does not specify a procedure to perform the identity proofing process.

Elements common to all steps:

Possible security levels associated to one step or the whole process: **the degree of certainty to be achieved is determined according to the risk level, i.e. low, standard or high.** E.g for low risk, financial institutions are authorized to verify a smaller amount of the information collected & may choose to accept certain documents that they consider to have insufficient probative value to be accepted in standard-risk situations.

Compliance measures implemented: In accordance with Article 60 of the Anti-Money Laundering Law, financial institutions should keep the following documents and information, using any type of record-keeping system: the identification data of customers, agents and beneficial owners, where appropriate updated in accordance with Article 35 of the Anti-Money Laundering Law, and a copy of the supporting documents or of the result of consulting an information source, **for a period of ten years** from the end of the business relationship with the customer.

Security requirements: Yes, under the form of recommandations.

5.4.5.6 Reference material

Title	URL
National Bank of Belgium Object of the identification and identity verification: Comments and recommendations [i.75]	https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/customer-and-transaction-du-7

5.4.5.7 Reviewer Note and Conclusion

The National Bank of Belgium document [i.75] provides a sort of policy quite well addressing identity proofing, quite well structured, that financial institution can use to write their practices and procedures. This is relevant for ETSI DTS/ESI-0019461 [i.50] especially for inspiration on the documentation and the authoritative sources selection.

5.4.6 Spain: SEPBLAC Video Identification procedures

5.4.6.1 Short description

Purpose and context: The Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses (SEPBLAC) is the Spanish Financial Intelligence Unit and AML Supervisory Authority.

In 2016 and 2017, the SEPBLAC approved two documents [i.76] and [i.77] that allow the subjects bound by the money laundering prevention regulations to verify the identity of their clients in a non-face-to-face way, specifically, through videoconference.

The 2016 document [i.76] establishes an assisted video identification procedure, while the 2017 document [i.77] establishes an unassisted video identification procedure.

In accordance with the Eleventh Additional Provision of Royal Decree-Law 11/2020 and during the Covid19 Spanish state of alarm, the issuance of qualified certificates with assisted video identification was allowed in accordance with the SEPBLAC document of 2016 [i.76]. After the end of the state of alarm, the Royal Decree-Law 11/2020 was rendered ineffective, so the Spanish eIDAS Supervisory authority issued a draft ministerial order to regulate digital ID proofing processes. This draft is in consultation with the industry at the time of closing the present document.

ID type: Natural and legal person.

Expected outputs: client on boarding.

Sector: AML.

Legal background: AML Directive and national law.

5.4.6.2 Attribute collection

Attributes to be collected: It will depend on the identification obligations of each obligated subject.

Type of evidence to be/that can be presented:

The client should be provided with reliable identification documents (article 6 of Spanish Law 10/2010).

For natural persons: Identification documents in force at the time of establishing business relationships or executing occasional operations:

- Spanish: DNI (national identity card)
- Foreigner:
  - or the Residence Card;
  - or the Foreigner Identity Card;
  - or Passport;

- citizens of the European Union or the European Economic Area, the document, letter or official personal identity card issued by the authorities of origin;
- the identity document issued by the Ministry of Foreign Affairs and Cooperation for the personnel of diplomatic and consular representations of third countries in Spain will also be a valid document for the identification of foreigners.

Exceptionally, the obliged subjects may accept other personal identity documents issued by a government authority provided that they enjoy adequate guarantees of authenticity and include a photograph of the holder.

For legal persons: In the case of legal persons, the validity of the data consigned in the documentation provided is accredited by a responsible statement from the AML subject.

Public documents that prove their existence and contain:

- company name;
- legal form;
- address;
- identity of its administrators;
- statutes; and
- tax identification number.

Spanish: admissible, for the purposes of formal identification, certification from the provincial Mercantile Registry provided by the client or obtained through electronic consultation.

In cases of legal or voluntary representation, the identity of the representative and of the person or entity represented, will be documented:

- A copy of the reliable document from both the representative and the person or entity represented, as well as the public document certifying the powers conferred.
- The verification by means of a certification from the provincial Mercantile Registry, provided by the client, or obtained by electronic consultation will be admissible.

Entities without legal personality: Obliged subjects will identify and verify by means of reliable documents the identity of all participants in entities without legal personality.

In the case of entities without legal personality that do not carry out economic activities, it will be sufficient, in general, with the identification and verification through reliable documents of the identity of the person acting on behalf of the entity.

Investment funds: The obligation to identify and verify the identity of the participants will be carried out in accordance with the provisions of article 40.3 of Law 35/2003, of November 4, on Collective Investment Institutions.

Anglo-Saxon trusts ("trusts") or other similar legal instruments that, despite lacking legal personality, can act in economic traffic They will require the constitutive document, without prejudice to proceeding to identify and verify the identity of the person acting on behalf of the beneficiaries or in accordance with the terms of the trust, or legal instrument:

- For these purposes, the trustees will communicate their condition to the obligated subjects when, as such, they intend to establish business relationships or intervene in any operations.
- In those cases in which a trustee does not declare his condition as such and this circumstance is determined by the obligated subject, the business relationship will be terminated, proceeding to carry out the special examination referred to in article 17 of Law 10/2010, of April 28.

Type of presentation: Photograph or snapshot of the front and back of the identification document used.with the quality and clarity conditions that allow its use in research or analysis. The mere capture of frames of the video-identification process is not considered valid for these purposes.

5.4.6.3 Attribute validation

The documents [i.76] and [i.77] require that the obligated subject implant:

- technical controls to verify the authenticity, validity and integrity of the identification documents used;
- measures to verify the falsity or manipulation of the identity document;
- measures to verify the correspondence between the holder of the document and the client to be identified;
- measures to ensure that the conditions of the transmission do not prevent or make it difficult to verify the authenticity and integrity of the identification document and the correspondence between the holder of the document and the customer being identified.

In the assisted process, the fulfillment of a good part of the requirements depends on the adequate training of the evaluator, on his technical knowledge, and ethical behavior, although the recordings are subject to annual audit.

5.4.6.4 Attribute binding

See below.

5.4.6.5 Requirements on the process

Any AML obliged subject, before implementating a procedure for verifying the identity of the clients, shoul:

- Test the procedure and document it;
- Perform a risk analysis. Prior to the effective implementation of a video-identification procedure, the obliged subject should carry out the specific risk analysis that will identify and assess the risks of the obligated subject by types of clients, countries or geographical areas, products, services, operations and distribution channels, taking into consideration variables such as the purpose of the business relationship, the level of client assets, the volume of operations and the regularity or duration of the business relationship. The risk analysis will be reviewed periodically and, in any case, when a significant change is verified that could influence the risk profile of the obliged subject. Likewise, it will be mandatory to carry out and document a specific risk analysis prior to the launch of a new product, the provision of a new service, the use of a new distribution channel or the use of a new technology by the subject. Required, and appropriate measures are to be applied to manage and mitigate the risks identified in the analysis.

As indicated, there are two different processes although they have common elements in their performance.

The 2016 document [i.76] establishes an assisted video identification procedure in which the presence of a duly trained verifier is required to carry out the recording, request consent for it to be carried out, make the legal data protection precautions and guide the client through the process -established internal procedure-. After requesting consent for the recording and for the processing of personal data, the client is requested to provide their data and to show the valid document that proves their identity. The client has to show the document on its front and back side to the camera within a field that allows the capture of her face and the document to make a comparison between one and the other. With this gesture a proof of life is also obtained. The verifier ask the applicant to perform some random gestures to check whether it is a living person or not. After this process and in accordance with the rules established above, the verifiers will positively or not identify the client.

The system should keep evidence of the complete process, of its integrity (that the recording has not been stopped, resumed, cut or edited) and of the integrity of the documents collected.

The 2017 document [i.77] establishes a procedure for unassisted videoID in which the client follows the steps that indicates the system, going through a similar protocol to that of the 2016 document. In this case, some documentation verification processes, mapping the client's identity with the documents, etc, can be carried out using automatic tools.

The recording should meet the same integrity requirements as in the assisted system and be reviewed by internal or external personnel *a posteriori* to consider the client to be positively identified. The 2017 system is designed for a 24/7 operation that does not depend on the working hours of the evaluators.

Thus, the process is divided into the following steps:

- Presentation of evidence of the attributes;

- Verification of attributes;
- Mapping;
- Positive/negative assessment of the identification process;
- Conservation.

Security requirements:

Together with the security measures on the process itself (integrity, availability and confidentiality), the documents establish that the operator should implement:

- Measures that ensure transmission security;
- Measures to ensure the authenticity and integrity of the recording;
- Measures to verify that the broadcast is in real time and in full, that the images and sound are immediately transmitted to the obliged subject in digital format, without alteration and live ("streaming"). This includes measures to ensure that the use of pre-recorded files by the client or other persons outside the obligated subject is not allowed;
- Traceability and reproduction in frame by frame; and
- Customer device verification: The process is performed by the customer from a single device.

5.4.6.6 Reference material

Title	URL
Autorización de procedimientos de vídeo-identificación (March 2016) [i.76]	https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf
Autorización de procedimientos de identificación no presencial mediante videoconferencia (2017) Remote clients identification procedures [i.77]	https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_identificacion_mediante_videoconferencia.pdf https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_procedimiento_identificacion_no_presencial.pdf

5.4.7 Italy: Provision of Bank of Italy on arrangements for appropriate customer verification to combat money laundering and terrorist financing

5.4.7.1 Short description

Purpose and context: This document [i.78] provides AML internal control system for the prevention of money laundering to combat the financing of terrorism and the role of corporate bodies together with due diligence obligations.

The AML subject defines the risk profile attributable to each customer, on the basis of the overall evaluation elements and risk factors. The development of the risk profile is based, as far as possible, on computer algorithms and procedures. The recipients ensure that the risk class proposed automatically by the IT systems is consistent with their knowledge of the customer, applying, where appropriate, higher risk classes.

In order to analyse clients' risk, the AML subject should performe "customer due diligence" that includes the following activities:

a) identification of the customer and any executor;

b) identification of any beneficial owner;

c) verification of the identity of the customer, any executor and any beneficial owner on the basis of documents, data or information obtained from a reliable and independent source;

d) acquisition and evaluation of information on the purpose and nature of the ongoing relationship as well as, in the presence of a high risk of money laundering and terrorist financing, of the occasional transaction;

e) exercise of constant control during the ongoing relationship.

ID type: Legal and natural person.

Expected outputs: Proof the identity of AML subject to minimize the risk of money laundering.

Sector: Banking and other AML subject sectors.

Legal background: AML regulation.

5.4.7.2 Attribute collection

Attributes to be collected:

- Natural person: identity document or other equivalent identification document under the law (in paper or electronic format).
- Legal person: identification on the type, legal form, purposes pursued and activities carried out and, if any, of the details of the registration in the register of companies and in the registers kept by the supervisory authorities sector:
  - In the case of non-profit organizations, information is also requiered on the class of beneficiaries to whom the activities carried out are addressed (eg victims of natural disasters and wars).
  - In the case of a trust, copy of the latest version of the trust deed, the identity of the beneficiaries and the trustee, the modalities execution of the trust and any other characteristic of the same.

Type of evidence to be/that can be presented: The identification obligation is considered fulfilled, even without their physical presence, when the customer provides the following information:

- Public deeds, authenticated private deeds or qualified certificates used for the generation of a digital signature associated with IT documents.
- Minors: birth certificate or any provision of the tutelary judge.
- Digital identity, of maximum security level, or of a digital identity of maximum security level or of a certificate for the generation of digital signature, issued under an electronic identification scheme included in the list published by the European Commission pursuant to Article 9 of Regulation (EU) no. 910/2014 [i.1].
- Declaration by the diplomatic representation and by the Italian consular authority.
- Existing identification by the AML subject in relation to another ongoing relationship in place, provided that the existing information is updated and adequate with respect to the specific risk profile of the customer and the characteristics of the new relationship that is to be started.

Type of presentation: Physical presence and remote presentation.

5.4.7.3 Attribute validation

The verification of the data relating to the customer, the executor and the beneficial owner requires the verification of the veracity of the identification data contained in the documents above.

Natural person:

- The AML subject verifies the authenticity and validity of the identity document or other equivalent identification document and, for the executor, also ascertain the existence and extent of the power of representation under of which he operates in the name and on behalf of the client.

- Minors: the identification data are verified, in the absence of an identity document or recognition, through the birth certificate or any provision of the tutelary judge. Verification can also take place by means of an authenticated photo: in this case, the details of the birth certificate of the person concerned are recorded.

- For non-EU subjects, the AML subject verifies the authenticity and validity of the passport, residence permit, travel document for foreigners issued by the Police Headquarters or other document to be considered equivalent pursuant to Italian law.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources). When doubts, uncertainties or inconsistencies emerge from the investigations, the AML subject may carry out further verification. i.es consult the public system for the prevention of identity theft.5.4.6.4 Attribute binding

The AML subject verifies legal person's identity using information that can be inferred from reliable and independent sources. The AML subject may adopt measures proportionate to the risk to reconstruct, with reasonable reliability, the ownership and control structure. To this end, the subject may consult any useful information source until they identify, with reasonable certainty, the beneficial owner and verify the ID data, in light of the customer's risk profile, relationship or transaction.

5.4.7.4 Attribute binding

See below.

5.4.7.5 Requirements on the process

This regulation provides AML identification procedures and considers both:

- assisted video identification procedures (details are provided in Annex 3 and are very similar to the ones provided for by AgID in Italy to issue the digital identity SPID via video identification); and

- non-assisted procedures (Section VIII), in which context NFC/OCR tools, Liveness detection and Face Matching tools after positive assessment carried out by the the supervised subject.

Section VIII set outs specific provisions regarding remote operations.

Remote operations are those carried out without the physical presence of the customer (e.g. through communication systems, telephone or computer).

The AML subject should take into account the risk of fraud associated with identity theft and follows this process:

- Require and check client's identification data (fax, mail, in electronic format or with similar methods).

- Carry out further checks: i.e. telephone contact (welcome call); sending communications to a physical home with acknowledgment of receipt; bank transfer made by the customer through a banking and financial intermediary based in Italy or in an EU country; request to send countersigned documentation; verification of residence, domicile, activity; through requests for information to the competent offices or through on-site meetings.

This document [i.78] does not include security requirements.

5.4.7.6 Reference material

Title	URL
PROVVEDIMENTO 30 luglio 2019 Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo. (19A05172) (GU Serie Generale n.189 del 13-08-2019) [i.78]	https://www.gazzettaufficiale.it/eli/id/2019/08/13/19A05172/sg

5.4.8 Italy: IVASS (the Institute for the Supervision of Insurance) act no. 44/2019

5.4.8.1 Short description

Purpose and context: This document provides AML internal control system for the prevention of money laundering to combat the financing of terrorism and the role of corporate bodies together with due diligence obligations.

Under Section II (Customer due diligence obligations), the document set out some requirements on identification of the client, the beneficiary, the beneficial owner and the executor; verification of the identity of the customer, the beneficiary, the executor and the beneficial owner and acquisition of information on the purpose and expected nature of the relationship continuous and occasional transaction.

ID type: Legal and natural person.

Expected outputs: Proove the identity of AML subject to minimize the risk of money laundering.

Sector: Banking and other AML subject sectors.

Legal background: AML regulation.

5.4.8.2 Attribute collection

Attributes to be collected:

- Natural person: name and surname, place and date of birth.
- Legal person: the name, the registered office, the registration number in the business register or in the register of legal persons or, alternatively, the tax code number. In the case of non-profit organizations, the AML subject has to require information about the class of subjects who benefit from the activities carried out.

Type of evidence to be/that can be presented: Natural person: identity document that has not expired or other equivalent identification in paper or electronic format, provided that it cannot be modified.

In the case of a trust: copy of the latest version of the trust deed and collecting information regarding the purposes actually pursued by the parties, the identity of the trustee of the beneficiaries, the criteria for the unambiguous identification of the beneficiaries, the procedures for execution of the trust and any other characteristic of the same.

Type of presentation:

In paper or digitally.

5.4.8.3 Attribute validation

As in clause 5.4.6.3

5.4.8.4 Attribute binding

Face to face and remotely.

The organization can identify the customer or the beneficiary, in the case of natural persons, using digital audio/video recording tools, as long as a system is used which guarantees the encryption of the communication channel through the adoption of mechanisms, standards, applications and protocols updated to the latest version. The videoID requires that:

- the video images are in color and allow a clear view -in terms of brightness, sharpness, contrast, fluidity of images- of the client;
- the audio is clearly audible, free from distortion or noise;
- the audio/videoID is carried out in environments without disturbing elements.

During the video identification, the personnel request the presentation of a valid personidentity document, a copy of which cannot be changed in electronic format.

Personnel in charge will not initiate or suspend the audio/video call if the quality of the audio or video, including that referred to the document exhibited, are scarce or inadequate to allow identification of the customer or beneficiary.

5.4.8.5 Requirements on the process

The organization can identify the customer or the beneficiary, in the case of natural persons, using digital audio/video recording tools, as long as a system is used which guarantees the encryption of the communication channel through the adoption of mechanisms, standards, applications and protocols updated to the latest version. The video ID requires that:

- the video images are in color and allow a clear view -in terms of brightness, sharpness, contrast, fluidity of images- of the client;
- the audio is clearly audible, free from distortion or noise;
- the audio/video ID is carried out in environments without disturbing elements.

During the video identification, the personnel request the presentation of a valid personidentity document, a copy of which cannot be changed in electronic format.

Personnel in charge will not initiate or suspend the audio/video call if the quality of the audio or video, including that referred to the document exhibited, are scarce or inadequate to allow identification of the customer or beneficiary.

The organization has to define a written procedure for conducting the audio/video calls where requirement on the following are included:

- the clients' explicit consent to be recorded;
- confirmation of the date and time of registration, of the mobile telephone number and the e-mail address, identification data and other data previously provided via electronic form;
- the declaration by the interviewer of his/her personal details;
- the front and back of the ID and tax code shown;
- confirmation of the e-mail address.

For conservation, the organization should stored audio-video files, images and structured metadata in electronic format in a manner consistent with the relevant provisions provided for by the anti-money laundering legislation.

Security requirements: Yes see above.

5.4.8.6 Reference material

Title	URL
Regolamento IVASS n. 44 del 12 febbraio 2019 Regolamento IVASS recante disposizioni attuative volte a prevenire l'utilizzo delle imprese di assicurazione e degli intermediari assicurativi a fini di riciclaggio e di finanziamento del terrorismo in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela, ai sensi dell'articolo 7, comma 1, lettera a) del Decreto legislativo 21 novembre 2007, n. 231. [i.79]	https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2019/n44/Regolamento_IVASS_44_2019.PDF

5.4.9 Germany: BaFin Circular 03/2017 on Video Identification

5.4.9.1 Short description

Purpose and context: The German Federal Financial Supervisory Authority (BaFin), working under the auspices of the Federal Ministry of Finance, published its second circular [i.80] on the requirements for the use of video identification procedures in 2017. It replaces the guidance given in item III of Circular 1/2014. The current Circular is presently under review by the Federal Ministry of Finance, Ministry of the Interior, and Ministry of Economic Affairs and Energy to evaluate the necessity of incorporating new amendments.

According to the current 2017 circular [i.80], the video identification procedure may be used by all entities obliged under the German Money Laundering Act (Geldwäschegesetz, GwG) and subject to supervision by BaFin. The requirements meets reliable verification procedures for the identity of natural persons pursuant to the Money Laundering Act as well as technically provide end-to-end encryption for all domestic and foreign identity documents with a machine-readable zone and verifiable optical security features within different categories of the ID document.

ID type: Natural person. Identification of legal persons or partnerships through video identification is not possible or in the scope of the document. The video identification procedure can, however, be used for identity of a legal or appointed representative verification.

Expected outputs: procedures for a video identification.

Sector: Anti-Money Laundering Compliance for all obliged entities under the German Money Laundering Act.

Legal background: German Anti-Money Laundering Act (GwG).

5.4.9.2 Attribute collection

Attributes to be collected: Any applicable attributes of the natural person.

Type of evidence to be/that can be presented: Documentation from an appropriate and authorized source. Only identity documents with security features that are sufficiently forgery-proof, clearly identifiable and therefore verifiable both visually in white light and using the available image transmission technology as well as having a machine-readable zone may be used during the video identification process.

Type of presentation of the attributes: Digitally, interaction by remote video identification: « using means which provides equivalent assurance to physical face to face presence" needs to be "using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the service provider can prove the equivalence. Video identification may only be carried out by appropriately trained employees.

5.4.9.3 Attribute validation

Determination that the ID attributes are valid (not expired, not revoked): Both national and foreign documents that have a machine-readable zone and contain sufficiently tamper-proof and verifiable optical security features in different categories are valid for such a process. The document should:

- contain optical security features visually identifiable in white light that a document of this kind typically has.

A match is to be assumed if the verification criteria of at least three of the security features randomly selected from different categories for the purposes of identification and possessed by the identity document are met.

Other formal features visually identifiable in white light and accessible for the purposes of inspection (including layout, number, size and spacing of characters, as well as typography) that a document of this kind typically possesses.

A verification of the validity and plausibility of the data and information contained on the identity document should be performed as part of the video identification procedure. Amongst other things, this includes a check of whether the date of issue and the date of expiry of the identity document match each other (i.e the date of issue is not be in the future).

In addition, the period of validity of the identity document presented does not contravene the norms for identity documents of this kind.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): Only identity documents with security features that are sufficiently forgery-proof, clearly identifiable and therefore verifiable both visually in white light and using the available image transmission technology and have a machine-readable zone are to be used during the identification process.

5.4.9.4 Attribute binding

Face to face interactions or digital interactions: no specification. ETSI EN 319 411-1 [i.10] is referred for guidance. A mapping between the applicant and its certificate is required (see above).

5.4.9.5 Requirements of the process

What needs to be done: secure user's enrolment, mapping between the identity of enrolled subject and the subject certificate information.

Why this needs to be done: to ensure the (sole) control on the signing key by the right subject and ensure the correct identification through the right certificate.

How this needs to be done: a series of security requirements are specified. For the user's identification reference is made to CIR 1502 [i.3] (see related reading sheet for more information).

Elements common to the whole process

- Possible security levels associated to one step or the whole process: the TSP can host a SCD or a QSCD, specific requirements are provided for the later case.
- Compliance measures implemented: no.
- Technical standards applied if any; ETSI EN 319 411-1 [i.10] and CIR 1502 [i.3].

Security requirements: Yes**.**

5.4.9.6 Reference material

Title	URL
BAFin Circular 3/2017 (GW) - video identification procedures [i.80]	https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html

5.5 SSI and blockchain

5.5.1 SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market

5.5.1.1 Short description

Purpose and context: this document [i.81], after an introduction on the concept of identity, provides a comprehensive picture of Self Sovereign Identity (SSI) (a use cases of DLT proposed as the next step in the evolution of the identity management practice), and of the two eIDAS Regulation pillars - eIdentification and Trust Services. It indicates the bridges between the two eIDAS pillars and then analyzes how SSI and eIDAS can work together and support each other, or, could work together provided there are modifications to the legal framework. Different scenarios are analysed:

a) Use of notified eIDAS eID means and qualified certificates to issue verifiable credentials (so that the verifiable credential inherits the level of assurance of the eIDAS electronic identification information).

b) eIDAS Bridge: increasing verifiable credentials' legal value and cross-border recognition. The idea of is to enhance the legal certainty of any class of verifiable credential, by incorporating the issuer's advanced or qualified electronic signature (if the verifiable credential issuer is a natural person) or seal (if the verifiable credential issuer is a legal person) person. They may also contain other identity attributes, such as mandates. This scenario has been conceived as a transitory one, until a solution for managing trusted issuers completely on the SSI system, with the same legal recognition, is available (see below).

c) Use current eID nodes to issue a SAML assertion based in verifiable credentials/presentations (It is a transitory scenario, whilst the scenario described below is not implemented).

d) Use of Verifiable IDs as eIDAS electronic identification means. To assess the feasibility, the document analyses how a SSI solution can fulfil eIDAS and eIDAS Security Regulation, article per article.

e) Issuance of qualified certificates based on a specific DID method and verifiable credential: the idea is not to use SSI VC in an identity proofing process to issue abclassical X509 certificate, but rather to issue a qualified certificate under the form of a specific DID method plus a specific type of verifiable credential. The idea is that a qualified certificate, in this view, would be an attestation composed of

   (1) a subject's DID Document;

   (2) an issuer's DID Document;

   (3) an issuer's Verifiable ID; and

   (4) a subject's verifiable ID.

   This verifiable credential could be designated as a "SSI eIDAS qualified certificate". A table (P118) maps an electronic signature certificate required contents as defined by eIDAS with the above SSI artefact where specific information should be contained.

f) Extend the eIDAS notification mechanism to Verifiable Attestations: enhanced Trusted Issuers management (here it is about attestation that go beyond the identity as covered by eIDAS. e.g. it can be a professional attestation (being a doctor).

g) Regulate the issuance of Verifiable Attestations as a trust service difference with the above, mainly oriented to cover Verifiable Attestations issued by public sector bodies, according to public procedure legislation. This scenario considers the possibility of other entities, public or private, acting as issuers of Verifiable Attestation.

h) Regulate the activity of Identity Hubs as a trust service, in support of SSI-based Once Only Principle. Identity Hubs would store verifiable credentials and presentations, DID documents, manage permissions, generate information with legal relevance (e.g. access logs), all of it on behalf of the subject.

i) Regulate delegated key management as an independent trust service, in support of remote wallets.

j) Regulate a specific type of DLT node as a trust service tailored for the generation of electronic evidences.

k) ID type: A priori a legal person, natural person, natural person acting on behalf of a legal person are concerned, but there is a strong focus on a natural person due to the fact that the EBSI ESSIF in which the study frames, is limited to natural persons.

l) Expected outputs: several scenarios are studied, in which there is either no output, or where the output is a (qualified) certificate, or where the output is an eIDAS eID means, etc.

Sector: this is a document generally applicable.

Legal background: eIDAS and the related secondary legislation. Other relevant legislation such as the AML regulations, etc.

5.5.1.2 Attribute collection

Attributes to be collected: n.a. directly as the document does not address identity proofing, but the attributes in SSI. They can be any kind of attributes, starting from the official identity data (i.e. minimal set of date as defined in CIR EU 2015/1501 [i.2]) up to professional attributes or the like (e.g. attestation of diploma).

Type of evidenc e to be/that can be presented: n.a. directly as the document does not address identity proofing.

Type of presentation (of the attributes): n.a. directly as the document does not address identity proofing, but the use of SSI is meant to be used in a remote process.

5.5.1.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): SSI verifiable credential (VC) are verifiable trough PK cryptography.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): some scenarios require the implication of Trusted Issuer (for confirmation of authority to issue a particular claim with respect to a subject).

5.5.1.4 Attribute binding

SSI are meant for digital interactions. The appurtenance of attributes to a person is done through VC are verifiable trough PK cryptography.

5.6.1.5 Requirements on the process

What needs to be done, why and how:

Not provided since the document is not addressing specifically identity proofing process.

Elements common to all steps**:** n.a.

Security requirements: No.

5.5.1.6 Reference material

Title	URL
SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market [i.81]	https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

5.5.2 NISTIR 8202: Blockchain Technology Overview

5.5.2.1 Short description

Purpose and context: This document [i.82] provides a high-level technical overview of blockchain technology. The purpose is to help readers understand how blockchain technology works.

This document [i.82] is very useful to understand the technology, but also possible use-cases behind blockchain. It does not really consider identity management as such a use-case; "Digital signatures are often used to prove identity in the cybersecurity world, and this can lead to confusion about the potential application of a blockchain to identity management. A blockchain's transaction signature verification process links transactions to the owners of private keys but provides no facility for associating real-world identities with these owners. In some cases, it is possible to connect real-world identities with private keys, but these connections are made through processes outside, and not explicitly supported by, the blockchain. For example, a law enforcement agency could request records from an exchange that would connect transactions to specific individuals. Another example is an individual posting a cryptocurrency address on their personal website or social media page for donations, this would provide a link from address to real world identity. While it is possible to use blockchain technology in identity management frameworks that require a distributed ledger component, it is important to understand that typical blockchain implementations are not designed to serve as standalone identity management systems. There is more to having secure digital identities than simply implementing a blockchain.

ID type: this is not applicable as the document [i.82] provides generic information not related to a specific context.

Expected outputs: this is not applicable as the document [i.82] provides generic information not related to a specific context.

Sector: this is not applicable as the document [i.82] provides generic information not related to a specific context.

Legal background: this is not applicable as the document [i.82] provides generic information not related to a specific context.

5.5.2.2 Attribute collection

Attributes to be collected: this is not applicable as the document [i.82] provides generic information not related to a specific context.

Type of evidence to be/that can be presented: this is not applicable as the document [i.82] provides generic information not related to a specific context.

Type of presentation: this is not applicable as the document [i.82] provides generic information not related to a specific context.

5.5.2.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked):

As the document [i.82] is on blockchains, this can done through classical data crypto validation pertinent to blockchains, knowing that the concepts of expiration or revocation is not handled by default in blockchains.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources).

As the document [i.82] is on blockchains, this can done through classical data crypto validation pertinent to blockchains, knowing that the concepts of expiration or revocation is not handled by default in blockchains.

The governance for blockchains is to be addressed by the related trust model. Depending how this is implemented, one can trust the information from being issued by an "authoritative source".

As mentioned above, this is to be made through processes outside, and not explicitly supported by, the blockchain.

Other checks implemented if any:

- This is not applicable as the document provides generic information not related to a specific context.

5.5.2.4 Attribute binding

As the document [i.82] is on blockchains, this can done through classical data crypto validation pertinent to blockchains, knowing that by default one can verify that a data belongs to a certain identifier, but the link between the identifier and the real person behind needs is managed according to the trust model.

As mentioned above, such connections are to be made through processes outside, and not explicitly supported by, the blockchain.

5.5.2.5 Requirements on the process

This is not applicable as the document [i.82] provides generic information not related to a specific context and the document is not specifically addressing an identity proofing process.

Security requirements: No.

5.5.2.6 Reference material

Title	URL
NISTIR 8202. Blockchain Technology Overview [i.82]	https://csrc.nist.gov/publications/detail/nistir/8202/final

5.5.3 ILNAS White Paper on Blockchain and distributed ledgers technology, economic impact and technical standardization

5.5.3.1 Short description

Purpose and context: The goal of this white paper [i.83] is to provide a comprehensive view of the developments around blockchain and distributed ledger technologies. To this aim, a systematic analysis of this domain is presented from three different perspectives: blockchain concepts and technology, economic and business impact, and technical standardization. It presents amongst other a use-case dedicated to digital identity and data exchange. It also provides a series of interesting references.

It presents the challenges in the existing identity management systems that are wide ranging and broken in three categories: challenges to the system itself (e.g. need for better trust models, streamlined service delivery, lack of transparency), challenges related to data management (e.g. security and privacy, increasing transactions volume), and challenges related to regulations.

It shows how blockchain could be used in identity applications as an information storage and transfer mechanism For instance, users could store their identity attestations on a ledger and share them with different service providers using the underlying distributed protocol. Similarly, in a private and permissioned blockchain where the ledger would be owned by a single entity, a consolidated view of the users' attestations would be provided for use in transactions, while concealing the information about the nature of the credentials; A blockchain-based identity management system could be viewed as a tool for cutting the paper process during verification of identity documents and a form of decentralized signature sharing to provide truly decentralized attestations.

This system would involve the following steps in executing a transaction:

- The first time/new usershould undergo an initial registration process, install relevant app and provide consent to manage her personal data. Thereafter:
- User clicks to subscribe and logs in to the blockchain-based identity and data management platform.
- User gives consent to sharing the existing attributes and proofs.
- If necessary, user enters the new requested attributes as well as supporting documentation and gives consent to sharing them.
- After providing consent, the user waits for a contract to be generated by the insurance company.
- When ready, user signs the contract and the SEPA agreement electronically.

It provides an example (Luxtust) and then shows possible business cases for identity providers.

NOTE: Interesting references are:

"A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity", World Economic Forum, 2016 [i.131], and the following standards:

ISO/NP TR 23246 [i.133] that will describe an overview of identity as it applies to DLT and Blockchain systems and the status of this document is uncertain; on the ISO portal it is still "under development".

ISO/TR 23244 [i.132] provides an overview of privacy and Personally Identifiable Information (PII) protection as they apply to blockchain and DLT systems.

ID type: this is not applicable as the document [i.83] provides generic information not related to a specific context.

Expected outputs: this is not applicable as the document provides generic information not related to a specific context.

Sector: this document [i.83] is not sector specific and can be interesting for all sectors.

Legal background: this is not applicable as the document [i.83] provides generic information not related to a specific context.

5.5.3.2 Attribute collection

Attributes to be collected: this is not applicable as the document [i.83] provides generic information not related to a specific context.

Type of evidence to be/that can be presented: this is not applicable as the document [i.83] provides generic information not related to a specific context.

Type of presentation: not specified.

5.5.3.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): As the document is on blockchains, this can done through classical data crypto validation pertinent to blockchains, knowing that the concepts of expiration or revocation is not handled by default in blockchains.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources):

As the document [i.83] is on blockchains, this can done through classical data crypto validation pertinent to blockchains, knowing that by default the verification is limited to the integrity of the data.

The governance for blockchains is to be addressed by the related trust model. Depending how this is implemented, one can trust the information from being issued by an "authoritative source".

This is to be made through processes outside, and not explicitly supported by, the blockchain.

Other checks implemented if any:

This is not applicable as the document [i.83] provides generic information not related to a specific context.

5.5.3.4 Attribute binding

As the document [i.83] is on blockchains, this can done through classical data crypto validation pertinent to blockchains, knowing that by default one can verify that a data belongs to a certain identifier, but the link between the identifier and the real person behind needs is managed according to the trust model.

5.5.3.5 Requirements on the process

This is not applicable as the document [i.83] provides generic information not related to a specific context.

Security requirements: No.

5.5.3.6 Reference material

Title	URL
ILNAS White Paper. Blockchain And Distributed Ledgers Technology, Economic Impact And Technical Standardization Version 1.0 - June 2018 [i.83]	https://portail-qualite.public.lu/dam-assets/publications/normalisation/2018/white-paper-blockchain-june-2018.pdf

5.5.3.7 Reviewer Note and Conclusion

It is an interesting document [i.83] per se that helps in understanding the applicability of blockchains. However, it does not focus on identity management, and even less on identity proofing.

As many other sources of information that relate to eID means, it shows how DLT may be used to provide identity information in an identity proofing process. This is one of the tools that this study should consider, as a "blackbox", provided one is able to assess the assurance or security level associated with the related ID provider.

The document [i.83] primarily addresses identity management as an example, and does not enter into technical or organizational details. With regard to the identity proofing process (or registration more precisely), which is mentioned to a lesser extent, is left outside the scope of the document.

5.5.4 Decentralized Identifiers (DIDs)

5.5.4.1 Short description

Purpose and context: The Decentralized Identifiers (DIDs) defined in this WC3's specification (Decentralized Identifiers (DIDs) v1.0) [i.84] presents a new type of globally unique identifier designed to enable individuals and organizations to generate their own identifiers using systems that they trust. The model proves control of the identifiers using cryptographic tools (i.e, digital signatures, privacy-preserving biometric protocols, etc.).

Tha community/nodes issue the ID-Identifier and the assertion issuers produces identifiers. Any person or item may have as many DIDs as he/she/it needs depending on differerent "identities", personas, and contexts. The identification vis a vis third parties is achieved thougth attestation of the attributes required in a sort of modular identity. Decentralized Identifiers are a component of larger systems -such as the Verifiable Credentials ecosystem - which drove the following design goals:

- **Decentralization.** Eliminate the requirement for centralized authorities or single point failure in identifier management, including the registration of globally unique identifiers, public verification keys, service endpoints, and other metadata.
- **Control**. Give entities, both human and non-human, the control on their digital identifiers without the need to rely on external authorities.
- **Privacy**. Enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
- **Security**. Enable security for requesting parties to depend on DID documents for their required level of assurance.
- **Proof-based**. Enable DID controllers to provide cryptographic proof when interacting with other entities.
- Discoverability: Make it possible for entities to discover DIDs for other entities, to learn more about or interact with those entities.
- Interoperability: Use interoperable standards so DID infrastructure can make use of existing tools and software libraries designed for interoperability.
- Portability: Be system- and network-independent and enable entities to use their digital identifiers with any system that supports DIDs and DID methods.
- Simplicity: Favor a reduced set of simple features to make the technology easier to understand, implement, and deploy.
- Extensibility: Where possible, enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity.

DIDs does not require any particular technology or cryptography to underpin the generation, persistence, resolution or interpretation of DIDs. It defines:

a) the generic syntax for all DIDs; and

b) the generic requirements for performing the four basic CRUD (create, read, update, deactivate) operations on the metadata associated with a DID (called the DID document).

This enables implementers to design specific types of DIDs to work with the computing infrastructure they trust (e.g. blockchain, distributed ledger, decentralized file system, distributed database, peer-to-peer network). The specification for a specific type of DID is called a DID method. Implementers of applications or systems using DIDs can choose to support the DID methods most appropriate for their particular use cases.

The specification [i.84] is aiming at helping:

- Developers who want to enable users of their system to generate and assert their own identifiers (producers of DIDs);
- Developers who want to enable their systems to accept user-controlled identifiers (consumers of DIDs);

- Developers who wish to enable the use of DIDs with particular computing infrastructure (DID method developers).

DID arquitecture is as follows:

- DIDs and DID URLs. A DID, or Decentralized Identifier, is a URI composed of three parts: the scheme "did:", a method identifier, and a unique, method-specific identifier generated by the DID method. DIDs are resolvable to DID documents. A DID URL extends the syntax of a basic DID to incorporate other standard URI components (path, query, fragment) to locate a particular resource - for example, a public key inside a DID document, or a resource available external to the DID document.

- DID Subjects:The subject of a DID is, by definition, the entity identified by the DID. The DID subject may also be the DID controller. Anything can be the subject of a DID: person, group, organization, physical thing, logical thing, etc.

- DID Controllers: The controller of a DID is the entity (person, organization, or autonomous software) that has the capability -as defined by a DID method- to make changes to a DID document. This capability is typically asserted by the control of a set of cryptographic keys used by software acting on behalf of the controller, though it may also be asserted via other mechanisms. Note that a DID may have more than one controller, and the controller(s) may include the DID subject.

- Verifiable Data Registries. In order to be resolvable to DID documents, DIDs are typically recorded on an underlying system or network of some kind. Regardless of the specific technology used, any such system that supports recording DIDs and returning data necessary to produce DID documents is called a verifiable data registry. Examples include distributed ledgers, decentralized file systems, databases of any kind, peer-to-peer networks, and other forms of trusted data storage.

- DID documents. DID documents contain metadata associated with a DID. They typically express verification methods (such as public keys) and services relevant to interactions with the DID subject. A DID document is serialized according to a particular syntax (Section 6 of DIDs. Core Representations [i.84]). The DID itself is the value of the id property. The generic properties supported in a DID document are specified in Section 5 [i.84]. Core Properties. The properties present in a DID document may be updated according to the applicable operations outlined in Section 7. Methods [i.84].

- DID Methods. DID methods are the mechanism by which a particular type of DID and its associated DID document are created, resolved, updated, and deactivated using a particular verifiable data registry. DID methods are defined using separate DID method specifications (Section 7. Methods [i.84]).

- DID resolvers and DID resolution. A DID resolver is a software and/or hardware component that takes a DID (and associated input metadata) as input and produces a conforming DID document (and associated metadata) as output. This process is called DID resolution. The inputs and outputs of the DID resolution process are defined in Section 8. Resolution [i.84].

- DID URL dereferencers and DID URL dereferencing. A DID URL dereferencer is a software and/or hardware component that takes a DID URL (and associated input metadata) as input and produces a resource (and associated metadata) as output. This process is called DID URL dereferencing. The inputs and outputs of the DID URL dereferencing process are defined in Section 8.2 [i.84] of DIDs-DID URL.

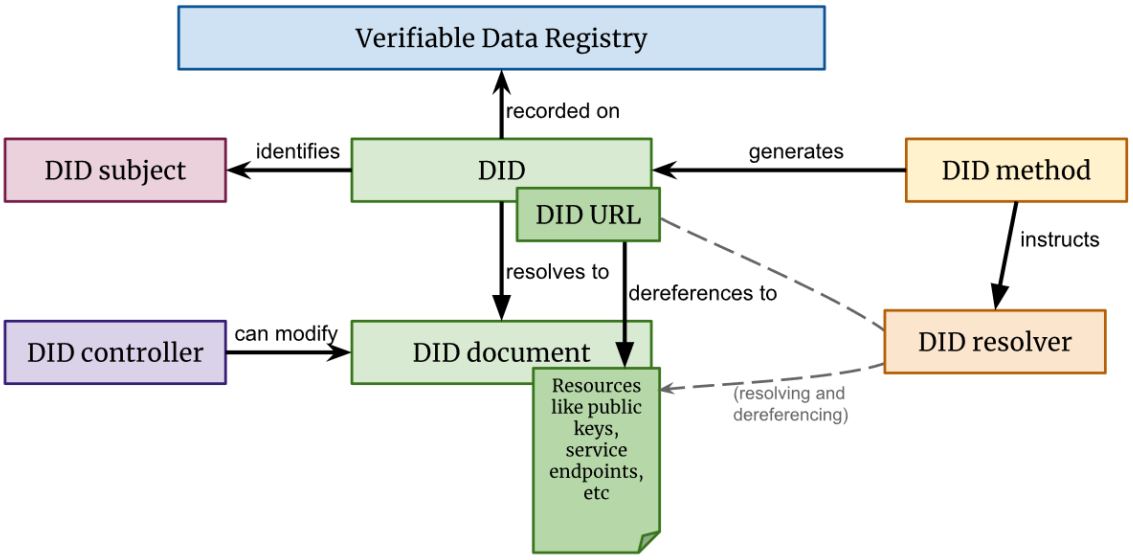


Figure 1: Basics components of DID architecture

ID type: Natural, legal person, any object.

Expected outputs: a DID.

Sector: Any.

Legal background: N/A.

5.5.4.2 Attribute collection

Attributes to be collected: Any.

A DID is a simple text string consisting of three parts:

- URL scheme identifier (did);
- Identifier for the DID method; and
- DID method-specific identifier.

The DID resolves to a DID document. A DID document contains information associated with the DID, such as ways to cryptographically authenticate the DID controller, as well as services that can be used to interact with the DID subject.

Type of evidence to be/that can be presented: Any.

Type of presentation: No specification included.

5.5.4.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): By the assertion issuers.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): By the assertions issuers.

5.5.4.4 Attribute binding

No requirements included.

5.5.4.5 Requirements on the process

A DID resolver is a software and/or hardware component that takes a DID (and associated input metadata) as input and produces a conforming DID document (and associated metadata) as output.

This process is called DID resolution. The inputs and outputs of the DID resolution process are defined in section 8 of [i.84].

The specific steps for resolving a specific type of DID are defined by the relevant DID method specification.

Security requirements: Some considerations are set out in section 9 of DIDs document [i.84].

5.5.4.6 Reference material

Title	URL
Decentralized Identifiers (DIDs) v1.0 Core Data Model and Syntaxes W3C Working Draft 09 December 2019 [i.84]	DID core: https://www.w3.org/TR/did-core/ DID WG site: https://www.w3.org/2019/did-wg/PublStatus

5.6 Tools and technical requirements

5.6.1 Face recognition

5.6.1.1 NISTIR Draft Ongoing Face RecognitionVendor Test (FRVT)

5.6.1.1.1 Short description:

Purpose and context: The NIST Face Recognition Vendor Test is an ongoing test programme where different algorithms and products from different commercial and research actors are tested on a huge picture database held at NIST. The idea is to detect resilience to both false acceptance and false rejection rates. The pictures and tests are conducted across a wide range of patterns, e.g. age, race gender. The latest report covers 127 algorithms from 45 different vendors. Tests show that a massive gain in accuracy is obtained between 2013 and 2018. This is attributed to use of neural network technology. Tests are run across photos of different quality. The first part (Part 1) verification document https://www.nist.gov/system/files/documents/2019/11/20/frvt_report_2019_11_19_0.pdf is a significant document in draft status visualizing the test results with over 600 pages. The second part (Part 2) identification document https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf is a summary of the tests with over 147 pages.

ID type: natural persons.

Expected outputs: Statistics on performance of different face biometrics algorithms and implementations.

Sector: Results can be applicable to identity proofing but also to criminal investigation and a range of other areas.

Legal background: Results of research presented as such.

5.6.1.1.2 Attribute collection

Attributes to be collected: The document covers face biometrics and matching.

Type of evidence to be/that can be presented: face matching.

Type of presentation (of the attributes): Not applicable.

5.6.1.1.3 Attribute validation

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): Not applicable.

Determination that the ID attribute are valid (not expired, not revoked): Not applicable.

5.6.1.1.4 Attribute binding

ID binding is not applicable except face recognition.

5.6.1.1.5 Requirements on the process

The document does not specify requirements on processes. The main purpose is to test different solutions and benchmark them against historical results as well as against one another.

Security requirements:

The test is done by use of existing picture databases, meaning the true result of the face matching is known. Based on this, requirements for ratio of false positive and false negative results are stated. Differences across algorithms and implementations can be noted. Other security features of biometric systems are out of scope.

5.6.1.1.6 Reference material

Title	URL
NISTIR Draft Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification	Part 1: Verification https://www.nist.gov/system/files/documents/2019/11/20/frvt_report_2019_11_19_0.pdf Part 2: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf
NISTIR Draft Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification	Project website: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

5.6.2 Transfer of ID attributes and related metadata

5.6.2.1 OpenID connect identity assurance working group (eKYC Project)

5.6.2.1.1 Short description

Purpose and context: the OpenID Connect Foundation is the sponsor of the leading IT protocol for the propagation and transfer of ID attributes, extensively used by federated identity schemes (sign-in with Apple®, Google Sing-in, Microsoft Sign-in, GSMA Mobile Connect, etc. are based on OpenID Connect). OpenID Connect can in many ways be seen as a modern, mobile and API-friendly version of SAML, the previous generation IT protocol used inter alia by the eIDAS interoperability framework. Through its eKYC Project, the OpenID Foundation is now working on specifications for the transfer of metadata in relation to ID attributes, such as *inter alia*, the applicable trust framework, the date of issuance of the attribute, its expiry date, the authoritative source issuing the attribute, the verification method, etc. Indeed, metadata are critically important for the propagation of 'verified attributes' as well as needed for the transfer of KYC profiles from OpenID Connect Providers (OPs) to Relying Parties (RPs).

ID type: The initial focus of the eKYC Project [i.85] is ID attributes & metadata for natural persons, but work has recently been started on ID attributes & metadata for legal persons.

Expected outputs: Set of technical IT specifications for the transfer of ID attributes and related metadata.

Sector: all sectors, but it is expected that OPs will tend to be from the financial sector and able to communicate 'AML-grade' verified ID attributes.

Legal background: the eKYC Project [i.85] is firmly technical/operational and separated from legal/regulatory considerations, which are no doubt relevant but beyond the scope of the project and therefore not addressed by them.

5.6.2.1.2 Attribute collection

Attributes to be collected: An initial set of ID Attributes (name, given name, middle name, birthday, place of birth, address, etc) has been prepared but it is expected that the list can, and likely will, be expanded in due course.

Type of evidence to be/that can be presented: The eKYC Project [i.85] currently contemplates the following types: id_document, utility_bill, notified eID system (eIDAS) and qes (eIDAS qualified electronic signature).

Type of presentation: The 'evidence method' is optional and may be required in certain situations but is secondary to the 'trust framework' claim, i.e. the identity assurance level for the relevant attributes communicated.

5.6.2.1.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): not directly addressed by the eKYC Project [i.85]

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): not directly addressed by the eKYC Project.

5.6.2.1.4 Attribute binding

Not directly addressed by the eKYC Project [i.85].

5.6.2.1.5 Requirements on the process

Not directly addressed by the eKYC Project [i.85].

The eKYC Project [i.85] is primarily designed to facilitate the re-use by RPs of ID attributes that have been identity-proven in the first place and therefore does not necessarily need to focus on all identity-proofing parameters. Indeed, what is usually critical for RPs is to know the attributes, their level of assurance (Trust Framework) as well as dates of issuance and expiry dates. Other metadata can no doubt be relevant in certain situations and be requested on an ad-hoc basis but are often viewed as less critical. For example, if an OP is willing to attest to the RP as to, say, the eIDAS High level of Assurance of a set of attributes, which ID document, communication and applicant-binding methods have been used as part of the identity-proofing method for these are information less likely to relevant for the RP, who is primarily going to rely on the 'Trust Framework' claim defining the overall level of assurance for the ID attributes.

The eKYC project [i.85] was initiated in January 2020 and still at an early stage. Although the final set of specfiications looks within reach, implementation is still some way off and there is room for adjustments and variations.

There are important considerations that are not directly covered and addressed by the eKYC Project [i.85] (especially with respect to liability and privacy protection). These aspects are viewed as 'implementation phase' developments better dealt with by forums outside of OpenID Connect which is focusing on technical specifications.

5.6.2.1.6 Reference material

Title	URL
OpenID connect identity assurance working group (eKYC Project) [i.85]	https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html
OpenID Connect for Identity Assurance 1.0 [i.39]	https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html#rfc.section.4.1

5.6.2.1.7 Reviewer Note and Conclusion

The eKYC Project [i.85] is a welcome and important, if not critical, development for the propagation of eKYC profiles between market participants and the deployment of KYC-related services which may well have a transformational impact on the financial sector, but its 'secondary market' focus implies that it puts emphasis on the overriding 'Trust framework' assertion and does not necessarily concern itself with all aspects of identity-proofing processes.

5.6.3 Document validation tools

5.6.3.1 PRADO

5.6.3.1.1 Short description

Purpose and context:

PRADO [i.86] is a public on-line authentic travel and identity documents database, provided by document experts in all UE Member States and Iceland, Norway and Switzerland.

PRADO [i.86] provides a glossary to explain technical terms used in ID document. The glossary is also intended to promote the use of consistent terminology as well as contribute to a common understanding, or a basis for effective communication and for police and administrative cooperation. The glossary is available in 24 official EU languages.

The glossary is also intended to help raise awareness among those having to check identities and ID documents. Document experts will not be able to decide on the authenticity of a questioned document unless suspicions are raised by PRADO users who ask their local police, or the responsible national contact point, for further guidance.

ID type: Natural persons.

Expected outputs: ID document authenticity validation.

Sector: National identity systems that can be used to identify subjects in the private sector.

Legal background: National legislation.

5.6.3.1.2 Attribute collection

Attributes to be collected: Passports, ID cards, travel document issued to non-nationals, visas, residence-related documents, driving licenses, vehicle licence/logbook, work permits, and other ID related documentation.

Type of evidence to be/that can be presented: For each type of ID document several pictures are provided. For a passport i.e.: outside front cover, inside front cover (UV feature), inside back cover (UV feature), Biodata page (UV feature), Inner page(s) (Watermark, Printing technique, UV feature). Some other information is included, such as title, issuing country, document Category, document type (temporary/provisional/emergency), document version number, valid (first issued on/not valid after) legal status/main purpose, overall construction (width, height, number of pages).

Type of presentation: Text and pictures.

5.6.3.1.3 Attribute validation

Determination that the ID attribute are valid (not expired, not revoked): To use PRADO [i.86] to verify the validity of a given ID Document, it provides some information: Validity qualifier, maximum validity, extension is possible, validity-additional information.

Determination that the evidence is genuine (issued by recognized independent/authoritative sources): The whole purpose of this data base is to provide relevant information.

Other checks implemented if any: no specific provisions.

5.6.3.1.4 Attribute binding

No specific provisions.

5.6.3.1.5 Requirements on the process

No process is described

Security requirements: No.

5.7.3.1.6 Reference material

Title	URL
PRADO - Public Register of Authentic travel and identity Documents Online [i.86]	https://www.consilium.europa.eu/prado/en/prado-start-page.html

5.6.3.2 Machine Readable Document (MRTD). ICAO 9303 (multipart)

5.6.3.2.1 Short description

Purpose & context: the ICAO 9303 series [i.87], issued by ICAO, specifies Machine Readable Document (MRTD) that can be used to travel worldwide. This includes the specification of security features to assure the:

(i) genuineness of the citizen identity (by diverse means, including a PKI (CSCA), allowing the issuing state to sign citizen identity); and

(ii) to support the mapping between a document and its owner, with facial recognition and possibly other biometrics, protected thanks to a PKI.

However, beyond the specification of the quality of the elements that needs to be integrated in the MRTD, the issuance of MRTD is a State responsibility. States are responsible for setting up an enrolment station with the proper environmental controls. Issuing States are required to build and maintain appropriate facilities for issuance systems, applicant enrolment, and safe storage of the associated data. In particular when a State elects to implement PKI, equipment and facilities to receive, store, and transmit information securely are required.

ID type: natural person

Expected outputs: MRTD (for worldwide use)

Sector: government

Legal background: no specific - states to states relationships prevail in ICAO [i.87] recognition and mutual recognition

5.6.3.2.2 Attribute collection

Attributes to be collected: official ID (i.e. 2 first names + initials of next ones, name, date & place of birth, city of issuance, national number, nationality), face picture, optional biometrics (fingerprint, iris).

Type of evidence to be/that can be presented: left to States.

Type of presentation (of the attributes): left to States for what constitutes relevant evidence to be presented. The outputs of the process are the picture of the citizen and its identity attributes available as printed (human readable) on the MRTD.

The identity attributes are also machine readable, in two ways:

(i) through an optical reading zone; and

(ii) in the contactless chip embedded in the MRTD [i.87].

In the second case the attributes are signed by the issuing states for proof of genuineness. If the reading station is entitled to, it may access the picture, fingerprints and/or iris scan of the citizen for ensuring belonging of the inspected MRTD to the inspected person by comparison with the person's actual biometrics.

5.6.3.2.3 Attribute validation

Left to States.

5.6.3.2.4 Attribute binding

Left to States.

5.6.3.2.5 Requirement on the process

Left to States.

Security requirements: no security requirements on the identity proofing process (but well on the MRTD itself [i.87]).

5.6.3.2.6 Reference material

Title	URL
Machine Readable Document (MRTD). ICAO 9303 (multipart) [i.87]	https://www.icao.int/publications/Documents/Forms/AllItems.aspx

5.6.3.2.7 Reviewer note and conclusion:

The ICAO 9303 [i.87] offers a set of definitions, some of which of interest for the STF (e.g. enrolment).

ICAO 9303 [i.87] compliant MRTDs are seen as tools to be used in an identity proofing process: ICAO 9303 defines the attributes that can be found in a MRTD and assigns the responsibility of the security to the issuing States. An identity proofing process can used and rely on the follwoing attributes:

- anybody can read the identity information printing on a MRTD and visually assess the genuineness of the document;
- any person equipped with an OCR reader can read the optical zone;
- any person equipped with a contactless reader can read the identity information stored in the chip, and validate the issuing state signature on this information;
- any entitled authority can read the biometric to compare with the owner of the MRTD (this is generally limited to foreign member states that are allowed to do so by the issuing member state, as well as entitled organization within the issuing states, such as police, border controls, etc.).

However, ICAO 9303 does not impose any ID proofing policy and security requirements to member states (that are left to the issuing States).

This said, the European regulation in matter of MRTD and/or eID cards relies on ICAO and further specifies it, for example, Regulation (EU) 2019/1157 Of The European Parliament And Of The Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement [i.41].

For example, regulation 2019/1157 requires identity attributes appearing on national ID and residence documents to comply with the applicable ICAO 9303 specifications, except for the gender attribute [i.41].

In addition regulation 2019/1157 clarifies that '*With a view to ensuring the consistency of biometric identifiers with the identity of the applicant, the applicant shall appear in person at least once during the issuance process' [i.41].*

5.6.4 FIDO Alliance White Paper: Using FIDO with eIDAS Services

5.6.4.1 Short Description

Purpose and Context: The FIDO Alliance is a non-profit industry alliance that aims to address both the lack of interoperability among strong authentication devices as well as the problems users face when creating and remembering multiple passwords. Members have developed technical specifications that define an open, scalable, interoperable set of mechanisms that can circumvent reliance on passwords to securely authenticate users for online services.

The paper [i.88] is aimed at government agencies that are interested in using FIDO2 as part of an eIDAS notified scheme, and Qualified Trust Service Providers (QTSPs) who are interested in deploying eIDAS remote signing services that leverage the FIDO2 standard. The white paper describes how to use the FIDO2 standard with eIDAS compliant schemes and QTSPs. The document does not detail identity proofing attribute collection, validation, or security requiremnts within such a process.

The document provides an overview on how FIDO2 might meet the eIDAS requirements for substantial and high. Web Authentication is a non phisible protocol and FIDO2 authenticators are tamper proof hardware devices. Proper registration, enrollment, and issuance processes can form the basis for eID schemes that can be notified by the EC.

ID Type: Natural person.

Expected Output(s): FIDO2 can be used as an authentication standard with high assurance to an eIDAS compliant QTSP with authentication to its Qualified Certificate's private key that resides in the QES device and operated by the TSP for a QES.

In this White Paper [i.88], an architecture for using FIDO2 to trigger a remote resigning process is illustrated. The architecture is compatible with the Committee European Normalization (CEN) standards for Qualified Signature Creation Devices.

Sector(s): Government and E-Business.

Legal Background: Not applicable, but the document [i.88] covers eIDAS application in relation to Commission implementing Regulations and Decisions:

- EU 2015/1501 [i.2]
- EU 2015/1502 [i.3]
- EU 2015/1505 [i.141]
- EU 2015/1506 [i.4]
- EU 2016/650 [i.5]

The document [i.88] provides tables and specifications for:

- eIDAS components
- How to use FIDO2 as Part of the eID Scheme
- Analysis for compliance substantial and high
- Using FIDO2 for Secured Access to QTSPs

5.6.4.2 Attribute Collection

Attributes to be collected. Not within the scope of the present document.

The present document addresses the eID national scheme and the following eIDAS Assurance Levels for Electronic Identification:

- Low: requires the electronic identification scheme to use at least one authentication factor, (e.g. username and password).
- Substantial: requires the electronic identification scheme to use at least 2 authentication factors from different categories (e.g. possession, knowledge, inherent).
- High: requires the substantial plus additional means to protect the scheme against duplication and tampering. Required- multifactor authentication, private data/keys stored on tamper resistant hardware tokens and cryptographic protection of personally identifying information (i.e. PKI based authentication scheme with a token such as a PKI certificate stored on a smart card plus PIN). See EU 2015/1502 [i.3].

Type of evidence to be/that can be presented: Natural persons are identified using their eID national card or eID smart card as authentication protocol (i.e. German eID card with Extended Access Protocol, Spanish National de Identidad electronico, Belgian Citizen eCard or Estonian eID card with TLS, SIM card, PKI keys).

The White Paper [i.88] describes eIDAS QTSPs that operates according to ETSI EN 319 403 [i.8] and national supervisory approval, and eIDAS Remote Signing and QSCDs for which each Member State have a certification body that is responsible for certifications of QSCDs.

Each EU Member State is able to submit a national eID scheme for notification and is required to operate an eIDAS Node (the interoperability framework is discussed in legal terms in implementing regulation EU 2015/ 1501 [i.2]).

Citizens authenticate at their domestic eID scheme, identification and authentication information is subsequently transferred from a domestic eID Node via the foreign eIDAS Node to the online foreign online service.

5.6.4.3 Attribute Validation

Determination that the evidence is genuine (issued by recognized independent/authoritative sources):

The identification process goes beyond the scope of the present document, but it should adhere to the requirements on a QTSP CA for issuing a Qualified Certificate.

FIDO meets eIDAS requirements for assurance levels depending on FIDO authenticators' security levels. Enrollment under FIDO WebAuth is agnostic with respect to the identification process of an individual.

Enrollment should comply with eIDAS requirements. Credentials for enrollment to the FIDO2 authenticator needs to be done by other means (e.g. by identifying the user with the national ID card during the initial identification process or when the user authenticates to the CA online by using their eID).

NOTE: The claims in the paper are only self-declared and not confirmed by the relevant authorities so far.

5.6.4.4 Attribute binding

The notified eID scheme used for identification in one EU country should have the same or higher assurance level than the one required by the requested online service in another EU country. Since FIDO2 has the potential to be notified as the authentication part of an eID scheme, it is suitable for authentication to an identity provider, which can in turn connect to the national eIDAS Node for issuance of a SAML v2 ticket. The SAML v2 ticket contains interoperable identity and authentication information and can in turn be used to access to a requested online service in another EU Member State.

5.6.4.5 Requirements on the process

Process steps for cross border interoperable model are listed.

The eIDAS Node is able to redirect the user to an identity provider.

The identity provider invokes the eIDAS node with a successful authentication response.

The identification process goes beyond the scope of the present document, but it should adhere to the requirements on a QTSP CA for issuing a Qualified Certificate.

The registration procedure of the WebAuthn protocol does not provide any details about how the user can be identified when enrolling for the FIDO2 credentials. When accredited CAs issue traditional eID cards, however, the user is identified according to the policies and practices stipulated by the CA.

Each identity profile relates to the eIDAS LoA (substantial, high) as FIDO2 meets the eIDAS requirements on eID schemes for the authentication mechanism with assurance substantial and high.

FIDO2 can also be used as an authentication standard to attain an authentication process with high assurance to an eIDAS compliant Qualified Trust Service Provider. More precisely, a user can use FIDO2 for strong authentication to its Qualified Certificate's private key residing in a centralized Qualified Signature Creation Device, which is operated by a Qualified Trust Service Provider. When the end-user is authenticated to her remote private key, it can be used for creating remote Qualified Electronic Signatures.

Security requirements: Yes.

The Security objective is not in the scope of the document [i.88]. It is the Member State that approves the eID scheme on a national level.

5.6.4.6 Reviewer note and conclusion

The paper [i.88] also only addresses authentication of already identified person and not the identity proofing process of these persons and is slightly out of scope of the present document.

5.6.4.7 Reference material

Title	URL
FIDO Alliance White Paper: Using FIDO with eIDAS Services Deploying FIDO2 for eIDAS QTSPs and eID schemes May 2020 [i.88]	https://media.fidoalliance.org/wp-content/uploads/2020/06/FIDO_Using-FIDO-with-eIDAS-Services-White-Paper.pdf

5.7 Main feedback from vendors and TSP

5.7.1 TSP

Five TSPs, most of them QTSPs, provided answers. The detailed responses can be found in Annex C and have been integrated in the findings presented in clause 6.

Identity proofing for legal person and natural person representing legal person are in scope for all respondents.

All use physical appearance, video interview, existing eIDs, and existing e-signature.

Two TSPs use NFC reading of ID documents, 1 use optical scanning of ID documents.

The main challenges pointed by TSP are, by order of importance:

- user friendliness and regulations;
- scaling, trust/security; and
- state of standardization.

Standards are sought for level of assurance requirements and security and policy requirements (and more).

Standards currently used by these TSP are ISO/IEC 27001 [i.24] and ETSI standards (used by all), and ISO 9001 [i.38].

5.7.2 Vendors

Nine vendors of identity proofing services or products provided answers. Some of these are also (Q)TSPs, most operate also outside of the EU.

The detailed responses can be found in Annex B and have been integrated in the findings presented in clause 6.

The vendors provided good input on best practices.

Legal person and natural person representing legal person in scope for a few only.

Seven respondents use NFC reading of ID documents with biometrics.

The main challenges pointed by vendors are, by order of importance:

- trust/security;
- user friendliness and regulations;
- state of standardization;
- scaling.

Standards are sought for level of assurance requirements and security and policy requirements (and more).

Standards ISO/IEC 27001 [i.24] and ETSI EN 319 401 [i.9] are in widespread use.

5.8 On-going initiatives: current trends in EU regulatory requirements

5.8.1 Intoduction

Two EU developments recently announced are likely to have a lasting and far-reaching impact on identity-proofing processes as currently considered by this Survey: one initiative is in relation to Know-Your-Costumer processes implemented by the financial sector; the second initiative is in relation to the revision process of the eIDAS Regulation [i.1].

Although preliminary announcements have been made, detailed policy developments are not available and not expected until later this year or early next year, therefore leaving an in-depth presentation of the contemplated changes to a later stage.

5.8.2 Know your Customer

One initiative is in relation to Know-Your-Costumer processes implemented by the financial sector, by far the most significant industry in need of robust identity-proofing processes which have to meet stringent anti-money laundering requirements. The EU Commission released its 'Digital finance strategy for the EU' document on September 24 2020 outlining four priorities, the first of which is to remove fragmentation in the digital single market by defining a new AML/CFT framework enhancing the financial service providers' ability to authenticate the identity of the customers and defining by means of technical standards of the European Banking Authority identification and authentication elements for customer on-boarding purposes.

In practice, this means *'ensuring greater convergence on the elements related to identification and verification needed for onboarding purposes […] without the need to apply different processes or comply with additional requirements in each member State', therefore 'making it easier to identify customers and check their credentials. […] this could be done by stating what ID documents are needed to establish a person's identity, and by clarifying which technologies can be used to check ID remotely'.*

The new AML/CFT framework is likely to lead to a new AML Regulation replacing parts of the current AML directives and providing a unified framework for customer due diligence processes, including Know-Your-Client requirements applicable to financial institutions. This would have a major impact on the way identity-proofing processes are implemented in practice, especially those meeting AML-CFT requirements within the EU.

5.8.3 eIDAS Regulation revision

In July 2020, the European Commission released an Inception Impact Assessment document outlining the following scenarios concerning how to address ID services/process regulation as a part of the eIDAS Regulation [i.1]:

- **The baseline scenario (Option 1):** Revising and complementing the eIDAS framework with, inter alia, additional implementing acts and guidelines (e.g. on identity verification for issuing qualified certificates).
- **Introducing new trust services for identification**, authentication and the provision of attributes, credentials and attestations and allowing the provision of identification for devices **(Option 2)**.
- **Creating a European Digital Identity scheme (EUid)** complementary with eIDAS for citizens to access online public and private services when identification is necessary **(Option 3)**.

The three scenarios are expressly stated as non-mutually exclusive - indeed a combination of them appears a likely outcome. On September 16, 2020 the President of the European Commission announced in her State of the Union address that the Commission would 'soon propose a secure European e-Identity', effectively endorsing Option 3, but gave no indications as to the other options.

This Survey is aimed as an input to ETSI DTS/ESI-0019461 [i.50], a TS on security and policy requirement for identity proofing service supporting enrolment of subject for trust service, i.e: issuance of certificates, enrolment to e-delivery and registered e-mail, signature creation component services. This fits within the current eIDAS regulation [i.1] (and future evolutions).

The specification to follow on from the present document is ETSI DTS/ESI-0019461 [i.50] can also be used for identity proofing as a component of a services for issuing national eIDs. This fits within the eIDAS revision process **option 1**.

ETSI DTS/ESI-0019461 [i.50] could help on the issuance of eIDAS eID means, e.g. in support of existing rules like EU CIR 2015/1502 [i.3] and related guidance (if needed by the expert group on eIDAS eID means). This also fits within the eIDAS revision process **option 2**, especially if eID means issuance become a new trust service (see hereafter).

ETSI DTS/ESI-0019461 [i.50] can thus also naturally support the issuance of an EU eID means, as proposed in the eIDAS revision **option 3**.

6 Analysis

6.1 Introduction

Next clauses look at each identity proofing process steps as identified in the methodology, as well as the process as whole:

- This clause begins with an introduction that fine-tunes the description of proofing process the steps as presented in the methodololy, supplemented with common elements or trends derived from clause 5.
- Then more detailed or technical findings relevant for ETSI DTS/ESI-0019461 [i.50] are presented.

6.2 ID Proofing process

6.2.1 Introduction

Identity proofing is crucial for trust in all digital services that require identification of a natural or legal person. eIDAS Regulation [i.1] and related ETS-ESI standards specify identity proofing only by generic requirements like "physical presence" or "means which provide equivalent assurance as physical presence". Equivalence to physical presence is not well-defined as no requirements are posed neither for the quality of (physical) identity documents nor for the competence or procedures to be carried out by the person performing the check.

6.2.2 Findings

Based on these premises and the review carried out, the following Findings have been reached.

Process.F1. The face-to-face identification process, both in the eIDAS Regulation model ([i.1], article 24.1.d) and in the AML regulation, are aimed at preventing one person from impersonating another and making use of that person's identity to register an account, obtain the issuance of a certificate, or buy a good or obtain the provision of a service and to prevent that fake/fantasy identies are used.

The identification, in short, allows us to attribute obligations and rights and demand their compliance. Misidentification can lead to the fraudulent use of identities to avoid or circumvent legal compliance, or the refusal of operation performed by someone posing as someone else. This endangers confidence in digital processes, online commerce, and in the possibility of digitizing entire business processes that continue to require a first face-to-face identification when the rest of the process is followed online.

The face-to-face identification process follows these general steps:

- Physical presence of the subject to be identified in the same place as the person who identifies him/her.
- Presentation of identity documents. In general, the document includes a photo to make a facial recognition.
- Verification of the authenticity of the document presented. This check is carried out by the natural person who performs the identifier work.

- Binding. This includes mapping documentation to natural persom or representative of a legal person to the individual (facial recognition, check against other registered biometrics, checks on the legal person power of attorney, etc.). Again, this verification is usually carried out by an employee who, after a quick observation of the photo and the face of the person being identified, decides whether they coincide in the essentials. It is worth noting that the poor quality of the photos of the usual identity documents, their age makes it difficult to identify them correctly. There are no specific requirements regarding training in this regard because most documents are indeed rather abstract or too generic.
- Archiving: evidence copy of the ID is not always kept.

Sources:

- ETSI EN 319 411-1 [i.10]
- ETSI EN 319 521 [i.15]
- EN 419 241-1 [i.40]/ETSI TS 119 431-1 [i.19]

Process. F2. An essential part of the present document is to analyze how the remote identification processes of natural persons is carried out- whether they are acting on their own behalf or as a representative of an organization- with the same guarantees as face-to-face identification.

Process.F3, The security offered by the processes relying on the physical presence is considered as a reference: ETSI DTS/ESI-0019461 [i.50] will specify acceptable remote processes with equivalent security.

Process.F4. The remote identification process follows in general the same steps that the face to face ID processes but requires process evidence (i.e. evidence generation, recording and record keeping and recording) and security measures. This doesn't apply to remote identification using eIDs.

Process.F5. Steps identified in 4.2.3 are applicable to all or most the identification processes.

Process.F6. The remote identification process requires integrity and recording the interaction, if any, is carried out without interruption.

Process.F7. Excluding eID schemes and telephone processes, remote identification processes are usually carried out through a videoconference, assisted or not by an operator.

There are three families of identity proofing processes for what regards the binding of the presented identity attributes with the applicant:

- Processes relying on the physical presence of the applicant in front of a registration officer.
- Attended by a person at the side doing the id proofing process remote processes.
- Unattended remote process purely based on electronic/digital interactions.

Process.F8. In attended videoconferencing processes, as for "face-to-face" processes, identification falls on the operator, as occurs in face-to-face identification. However, remote identification usually requires:

- Training of the operator.
- Follow a protocol or script for the entire process to ensure that each of the steps are followed and to interrupt it if they are not.
- That the operating environment is secure.
- That a record or evidence is kept of each of the steps taken.
- That certain tests are carried out to make sure that the person is alive, is not a recording, etc.

In short, in the face identification process and in some remote identification processes assisted the burden of matching lies with the skills of the person making the identification.

Sources:

- Spain: SEPBLAC Video Identification procedures [i.76] and [i.77].

- UK: Draft BSI 8626 Design and operation of online user identification systems [i.63].
- Germany: TR-03147 on Assurance Level Assessment of Procedures for Identity Verification of Natural Persons [i.64].
- Romania: Communication for Qualified Trust Service Providers [i.65].
- France: ANSSI: Référentiel d'exigences de sécurité - Moyens d'identification électronique [i.66].
- Germany: BNetzA 126/2017 [i.67].
- Germany: BNetzA 208/2018 on eIDAS [i.68].
- EC Report on Existing Remote On-Boarding Solutions in the Banking Sector [i.72].
- National Bank of Belgium: Object of the identification and identity verification: Comments and recommendations [i.75].
- Italy: IVASS (the Institute for the Supervision of Insurance) act no. 44/2019 [i.79].
- Germany: BaFin Circular 03/2017 on Video Identification [i.80].

Process.F9. In unattended remote processes, the process is conducted without human intervention and the various steps have to be performed using various verification tools:

- The person follows the directions that are given.
- The process is usually recorded and the decision on whether the identification is positive or not can be produced at the time of indetification.

Sources:

- Spain: SEPBLAC Video Identification procedures [i.76] and [i.77].
- German:. BNetzA 126/2017 [i.67].
- Germany: BNetzA 208/2018 on eIDAS [i.68].
- Italy: IVASS (the Institute for the Supervision of Insurance) act no. 44/2019 [i.79].
- Germany: BaFin Circular 03/2017 on Video Identification [i.80].

Process.F10. The application of security measures is required in the process and in the tools used to ensure:

- The integrity and confidentiality of the communication between the applicant and the ID proofing systems;
- The integrity, confidentiality and availability of the recordings;
- The integrity, confidentiality and availability of the documents, photos and files provided by the identified person;
- The traceability of the operations carried out to avoid documentary alterations;
- Physical and logical security;
- Trustworthiness of personnel; and
- The auditability of the process.

NOTE: This could be built on requirements in ETSI EN 319 401 [i.9].

Process.F11. The steps in the identification process may include some additional measures to prevent fraud or identity theft such as:

- The use of 'authoritative' source to ensure the integrity of the information , that the evidences presented is genuine or valid and that the information is up to date;

- The check of that the claimed identity has existed over time;
- The check of the authenticity and non-manipulation of the ID document presented;
- Mesures to ensure that the ID has not been stolen, lost, or manipulated;
- Different levels of strength (unacceptable, weak, fair, strong, superior) for the quality of evidence, validation, and verification of evidence.

Process.F12: Although the steps are repeated and they do so in the order described, the level of assurance and the techniques/tools used in each step differ, requiring a minimum standardization in:

- The general steps of the process;
- The elements of each step: allowed set of accepted ID documents or/and authoritative sources minimal set of ID attributes, type and nature of the attributes, collection methods, verification methods, harmonisation of metadata;
- Formats that allow portability and interoperability between processes/ID proofing providers.

Process.F13: Often, more than one level of identity proofing processes is identified in the information sources. It does not appear that there is consistency between the definition of these different levels.

Sources:

- Spain: SEPBLAC Video Identification procedures [i.76] and [i.77]
- Draft provisions on the use and cross-border recognition of identity management and trust services [i.55] and [i.55]
- ISO/IEC 30107 ([i.32], [i.31], [i.118] and [i.28]) on biometric presentation attack detection
- UK: Guidance on Identity proofing and authentication [i.57]
- UK: Draft BSI 8626 Design and operation of online user identification systems [i.63]
- US: NIST Special Publication 800-63 Digital Identity (multipart [i.43], [i.44], [i.45])
- Germany: TR-03147 on Assurance Level Assessment of Procedures for Identity Verification of Natural Persons [i.64]
- Romania: Communication for Qualified Trust Service Providers [i.65]
- France: ANSSI: Référentiel d'exigences de sécurité - Moyens d'identification électronique [i.66]
- Germany: BNetzA 126/2017 [i.67]
- Germany: BNetzA 208/2018 on eIDAS [i.68]
- BITS: Norway, Requirements for secure digital verification of identity [i.70]
- EC Report on Existing Remote On-Boarding Solutions in the Banking Sector [i.72]
- National Bank of Belgium: Object of the identification and identity verification: Comments and recommendations [i.75]
- Italy: IVASS (the Institute for the Supervision of Insurance) act no. 44/2019 [i.79]
- Germany: BaFin Circular 03/2017 on Video Identification [i.80]

Process.F14: Notified eIDAS eID means may be used in support of the identity proofing processes and will be particularly interesting for unattended remote processes.

6.3 Findings applicable to each steps of ID Proofing process

6.3.1 Attribute and evidence collection

6.3.1.1 Introduction

This clause provides an overview of the identity attributes and related evidence to be collected as well as their collection process as identified in the reading sheets.

It does not address the validation of the collected attribute, nor the mapping/binding of those identity attributes with the person to be identified (these aspects are analysed in ad-hoc next-clauses).

E.g. the freshness of collected identity attributes and evidence is required but this is covered in the clause "attribute validation".

In particular, the present clause will present customary identity attributes to be collected, the type of evidence to be presented for the identity proofing and the way this evidence needs to be presented, as well as the way the identity attributes are presented together with the constraints or requirement on their presentation.

The different aspects of identity attribute collection are presented as follows:

a) Identity attributes collected:

- for individuals
- for legal entities
- for individuals acting on behalf of legal entities

b) Type of evidence to be/that can be presented:

- Type of document or evidence (e.g. a passport)
- Customary trusted/authoritative sources for the ID attributes (Presentation of eligible issuers or trusted data sources of ID attributes)

c) Type of presentation of the attributes:

- collected as digital representation of an identity document (e.g. scan or photo of identity card or passport)
  - remotely
  - on site
- digitally extracted from an ID document (e.g. through (remote) access to the identity document chip)
- transmitted in purely digital form as an eID (or SSI)

d) Communication:

- In the event of remote collection, e.g.:
  - Presentation of the leading IT protocol and APIs used for the transfer of ID attributes (e.g. SAML or OpenID Connect);
  - Description of customary security measures deployed to protect the communication channels, such as integrity of the attribute transmission (e.g. end-to-end encryption);
  - Presentation of customary workflow/parties; e.g. are the identity attributes and related evidence remotely presented by the applicant or obtained from a third party independent of the applicant?
- In case of "on-premise" physical presentation, constraints to be observed e.g. by the personnel.

6.3.2 Findings

6.3.2.1 Customary ID attributes collected

6.3.2.1.1 Natural person

ACollection.NP1: The minimal set of identity attributes to be collected depends on the application. E.g. for the creation of official identity card or passport, biometrics elements are requested. For KYC and other banking obligation, additional elements like good standing may be requested.

ACollection.NP 2: There are commonly requested attributes: i.e. family name(s), first name(s) and date of birth.

ACollection.NP 3: Independently of the expected outputs, and on top of the commonly requested attributes (i.e. family name(s), first name(s) and date of birth), a unique identifier is generally requested. This may also be derived from the set of document that define the set of attributes, in a more functional or generic way, in the sense that they commonly require a "unique" identification of the applicant.

ACollection.NP 4: Whatever the way to define (list of attributes or functional description) most of the documents aim at collecting identity attributes that allow to **uniquely identify** the subject in a context.

ACollection.NP 5: There are two leading international benchmarks for core identity attributes: ICAO 9303 for Machine Readable Travel Documents and, in the Europe region, CIR2015/1501 [i.2] for electronic identification schemes, both setting forth a list of required and optional attributes.

Table 2

ICAO 9303 Machine Readable Travel Documents (part 5) (Visual Inspection Zone) (also applicable to EU national identity cards pursuant to EU Regulation 2019/1157 [i.41])	**CIR 2015/1501 [i.2] eIDAS electronic identification schemes**
Required attributes	
• full name of the holder (primary identifier and secondary identifier) • nationality • date of birth • passport number • sex • BIOMETRIC - Holders' signature • BIOMETRIC - Holder's facial image	• current family name(s) • current first name(s) • date of birth • a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time
Optional attributes	
• place of birth • additional data elements at the discretion of the issuing State • BIOMETRIC - Fingerprint	• first name(s) and family name(s) at birth • place of birth • current address • gender

One finds variations around this minimal set; some documents requesting less information and other requesting more.

Documents requesting less than CIR (EU) 2015/1501 [i.2]:

- ETSI EN 319 411-1 [i.10];
- CA/Browser forum [i.56];
- Romania: Communication for Qualified Trust Service Providers [i.65];
- EC Report on Existing Remote On-Boarding Solutions in the Banking Sector [i.72];
- National Bank of Belgium [i.75];
- eKYC Project [i.85];
- Germany. BNtA 126/2017 [i.67];

- Italy: IVASS (the Institute for the Supervision of Insurance) act no. 44/2019 [i.79].

Documents requesting more CIR (EU) 2015/1501 [i.2]:

- Regulation 2019/1157 [i.41];
- ICAO 9303 [i.87];
- UK. Guidance on Identity proofing [i.57];
- EU commission eID/KYC expert group [i.73].

Other documents do not list a minimal set of identity attribute but define it in a functional way:

- ISO/IEC 29003 [i.16]: as one or more attributes that, when combined, uniquely identifies the subject in a context;
- UK: Draft BSI 8626 identifying information from the applicant to make the identity uniquely identifiable given, family names and dates of birth appear to be required in all cases [i.63];
- NIST Special Publication 800-63 (multipart [i.43], [i.44], [i.45]): collect and record a biometric sample at the time of proofing (e.g. facial image, fingerprints) for the purposes of non-repudiation and re-proofing;
- TR-03147 on Assurance Level Assessment of Procedures: the set of ID attributes has to allow a unique identification [i.64].

ACollection.NP #6 : The address is occasionally found as a required identity attribute and plays an important role, especially in that it is a prime determinant of the residency status of the person, with key tax and other implications, but is only partially related to identity-proofing - it tends to be more related to the status or position of the identified person. In addition, it is inherently unstable and difficult to verify and therefore often based upon a simple confirmation of the applicant.

6.3.2.1.2 Legal person

ACollection.LP 1: there is some convergence around the current legal name and a unique identifier.

As for natural persons, one considers as benchmark the CIR (EU) 2015/1501 [i.2] (obviously relevant in the framework of the STF) and defining the minimum data set for a legal person as including all of the following mandatory attributes:

a) current legal name;

b) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

May contain one or more of the following additional attributes:

- current address;
- VAT registration number;
- tax reference number;
- the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council [i.21];
- Legal Entity Identifier referred to in Commission Implementing Regulation (EU) No 1247/2012 [i.46];
- Economic Operator Registration and Identification referred to in Commission Implementing Regulation (EU) No 1352/2013 [i.47];
- excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012 [i.48].

One finds variations around this minimal set; some documents requesting less information and other requesting more, but generally there is more convergence for legal persons than for natural persons.

Documents similar to CIR (EU) 2015/1501 [i.2]:

- Romania: Communication for Qualified Trust Service Providers [i.65].
- Italy. IVASS (the Institute for the Supervision of Insurance) act no. 44/201 [i.79].

Documents requesting less than CIR (EU) 2015/1501 [i.2]:

- ETSI EN 319 411-1 [i.10]

Document requesting more CIR (EU) 2015/1501 [i.2]

- CA/Browser forum [i.56]
- EU commission eID/KYC expert group [i.73]

6.3.2.1.3 Individuals acting on behalf of legal entities

Legal entities are usually represented by natural persons claiming authority to act on their behalf. A proper identity-proofing process therefore should, in addition to verifying the identities of the natural person and of the legal person involved, separately evaluate the link between the natural person and the legal entity so as to confirm that the individual is indeed in a position to act on behalf of the legal entity.

The ability and legal capacity to act on behalf of the legal entity therefore needs to be assessed separately. It should not, in our view be seen as a core identity attribute (it is of limited assistance when it comes to identifying the person) but should rather be seen as a 'status attribute', i.e. an attribute giving indications as to what the position of the person is and/or what it is allowed to do in social or professional interactions.

This status attribute for natural persons acting on behalf of legal entities is relatively easy to assess for individuals who are authorized by law to act on behalf of legal entities (for example, chief executives and board members of companies) as their names will usually appear in the registration documents of the legal entity and can therefore be independently verified. However, even in those situations, there is no guarantee that the person will be fully authorized to act on behalf of the legal entity for the act or transaction that is contemplated once the identity-proofing process has taken place, therefore leaving a question mark over the scope of the confirmed authority in the contemplated context.

The difficulty is compounded when the individual's name does not appear in the registration document of the legal entity - a very common situation for larger legal entities. Very few of the documents address that situation or prefer to deal with it entirely manually, without providing any specific guidelines.

ACollection.LE1: Few documents request a specific set of attributes to identify an individual acting on behalf of legal entities. When this is the case, the evidence to be submitted tends to be defined in very broad and unspecific terms, especially for situations where the individual is not directly authorized by law to act on behalf of the legal entity but needs.

- French ANSSI Référentiel [i.66]
- ETSI EN 319 411-1 [i.10]

6.3.2.2 Type of evidence to be/that can be presented

6.3.2.2.0 General

The identity attributes required to be collected originates from what is generally defined as a 'trusted' or 'authoritative' sources and backed up by the production of evidence, which may be documentary or electronic (or a combination of both).

6.3.2.2.1 Customary trusted/authoritative sources for the ID attributes (Presentation of eligible issuers or trusted data sources of ID attributes)

ACollection.TE1: Most of the documents require the collection of the attribute or evidence on these attributes from "authoritative" or "authorized" sources without further defining them. However, those sources can be implicitly identified using a list of identity documents generally accepted (i.e. passports, national IDs.):

- **ETSI EN 319 411-1 [i.10]:** appropriate and authorized source
- **Regulation 2019/1157 [**i.41**]:** in its recital, the Regulation mentions that authentic and secure identity cards requires secure 'breeder' documents to support the application process. Member States retain full responsibility for this.
- **CA/Browser forum (EV):** most of the element to be proved with regard to organization are verified directly with official source [i.56].
- **UK: Guidance on Identity proofing:** (highest level) the organization that issued the evidence proved the person's identity by comparing and matching the person to an image of the claimed identity from an authoritative source [i.57].
- **UK: Draft BS 8626 [**i.63**]:** issued by recognized independent/authoritative sources.
- **BITS: Norway [**i.70**]:** a check against the population register is expected. This check also yields physical address, (not provided by ID document).
- **EC Report on Existing Remote On-Boarding Solutions in the Banking Sector:** reliable data sources such as the company registration office database.
- **CA/Browser forum:** (for organization identity verification) using documentation provided by, or through communication with, at least one of the following [i.56]:
  a) A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
  b) A third-party database that is periodically updated and considered a Reliable Data Source;
  c) A site visit by the CA or a third party who is acting as an agent for the CA; or
  d) An Attestation Letter.
- **Germany. BaFin Circular 03/2017 on Video Identification [**i.80**]:** documentation from an appropriate and authorized source. Only identity documents with security features that are sufficiently forgery-proof, clearly identifiable.

ACollection.TE 2: Guidance for the application of the levels of assurance which support the eIDAS Regulation [i.1] defines 'Authoritative sources' as an authoritative source is any source that is nationally trusted to provide valid data. An authoritative source may be a register, or any other information provided by a responsible entity. A source can only be authoritative for the information provided by it.

This guidance provides example of such source. This is an important reference as almost no other document does detail what they mean by "authoritative" or "authorized" sources (see **ACollection.TE1**).

6.3.2.2.2 Type of document or evidence

The 2018 *Study on eID and digital on-boarding : mapping and analysis of existing on-boarding bank practices across the EU* contains a useful classification of ID documents worth presenting here. [i.52]

Type 1 - A physical document that is not machine readable *(i.e. does not have a Machine Readable Zone, MRZ), nor electronically readable (i.e. does not have a chip). This type represents physical only documents that can be digitalised through scanning or photographing. Since it is not possible to interact in an electronic way with such a document, it is considered outside the scope of eIDAS. However, it can be used in KYC and AML procedures. Within the EU, at the time of performing the present study, such documents were the exception rather than the rule.*

Type 2 - A physical document that is machine readable*. This MRZ can be read using Optical Character recognition (OCR) technology. The document contains a picture of the holder. Such documents are in use today in Member States. Strictly speaking they do not fall within the scope of eIDAS since they are not electronically readable. However, similar to type 1 documents, they are in use in current KYC and AML procedures.*

Type 3 - A physical document which is both machine-readable and electronically readable. *This includes the most recent passports and eID cards which have both a MRZ and a chip. The chip can be interacted with either contact-based or contactless. Such documents fall within the scope of eIDAS, and it is up to the issuing Member State to notify (or not). For usage in KYC and AML procedures, the decision to take reliance on such a document is a discretionary decision of the financial institution performing the on-boarding. The general expectation is that in this case, the document is qualified by an eIDAS LoA of Substantial or High.*

Type 4 - A 'logical document', implemented in digital media only*. Such an electronic identification means consists of personal identification data attributes stored within a secured enclave implemented in digital media (e.g. an app on a mobile device). These electronic identification means have no physical representation and are only electronically readable (i.e. digital only). They may rely on technology which is not yet commonplace for eID means inthe public sector today, such as mobile applications. It can be assumed such means might increasingly be used. From an eIDAS and KYC/AML perspective, they are treated on equal footage as a Type 3 document. This means it is up to the issuing Member State to notify it as an official eID means, with a specific LoA.*

It should be noted that the trend towards 'open data' environments, where credentials are directly accessible from trusted or authoritative source, mitigates the need for documentary or other evidence presented by the claimant. Indeed, when a credential is directly accessible in a secure way from a third party trusted or authoritative source, there is only limited need to further verify the credential, but confirmation that the claimant is indeed the person he/she pretends to be remains a requirement, a matter discussed in the 'attribute binding' clause below. However, the trend is more noticeable for status attributes (such as professional qualifications) than for core identity attributes.

ACollection.TE3: the evidence to be provided to support the identity attribute collection is probably one of the topic where one finds the most detailed and extensive information, whatever the origin of the documentation (be it governmental, financial sector or even requirements for TSPs).

ACollection.TE4: the requirement on evidencing vary from very generic requirements (like **Regulation 2019/1157** [i.41] recommending in its recital (10) secure 'breeder' documents), to very detailed requirements (like **CA/B forum** that details the exact list of accepted documents for legal and natural persons, respectively).

ACollection.TE5: a quasi-generally common point is the request for 'authoritative source' documents, meaning in practice, for natural persons, identity cards, residence cards or passports (see also information about "trusted sources" below). A possible reason for that situation is that these documents are very widely available, benefit from common specifications (e.g. ICAO 9303 for passports [i.87]) and include biometric attributes that facilitate a secure remote attribute binding process.

ACollection.TE6: few information refers to electronic identification means (including eIDAS electronic identification means) as acceptable identity evidence.

The following sources provide a detailed list of documents/elements to be collected, or consulted, to provide evidence of the verified identity:

- CA/B forum [i.56];
- UK. Guidance on Identity proofing [i.57];
- National Bank of Belgium [i.75];
- Spain. SEPBLAC Video Identification procedures [i.76] and [i.77];
- eKYC Project [i.85].

The following sources provide a functional description on the evidence to be provided, be it the kind of document (e.g. from an authoritative source), and/or the quality of the evidence (e.g. in terms of security features):

- NIST Special Publication 800-63 (multipart [i.43], [i.44], [i.45]): different types of evidence are allowed, and according to the IAL, some strength is required.

NOTE 1: Tthe document specifies the criteria to reach a certain strength. This depends amongst other on the trust and issuing process of the issuing source.

- TR-03147 on Assurance Level Assessment of Procedures [i.64].

NOTE 2: The overall assurance level are determined based on ID document providing the lowest assurance level for a specific ID check.

- ANSSI: verification des titres d'identité a distance [i.66].
- BITS: Norway [i.70].
- EC Report on Existing Remote On-Boarding Solutions in the Banking Sector [i.72].
- National Bank of Belgium [i.75].
- Spain: SEPBLAC Video Identification procedures [i.76] and [i.77].
- eKYC Project [i.85].
- Germany. BaFin Circular 03/2017 on Video Identification [i.80].

6.3.2.3 Type of presentation (of the attributes)

6.3.2.3.0 General

The clauses below are independent of the type of presentation (face 2 face or remote). Quite obviously, face 2 face is the simplest case, where the credential evidence is physically presented for identity-proofing purposes. There is then no specific issue with the presentation of the evidence, with the understanding that whether the evidence is genuine and whether it relates to the natural person claiming to be the identity information are topics discussed further in the related clauses later in the present document.

6.3.2.3.1 Collected as digital representation of an ID document (e.g. scan or photo of ID or video passport)

ACollection.TP1: quasi all documents analysed allow to collect a digital representation of the identity attributes or related evidence.

NOTE: This does not mean that the collection process can be done remotely (e.g. for Regulation 2019/1157 [i.41] the applicant should appear in person).

ACollection.TP 2: there are requirement for digital representation (whether provided on-site or remotely, e.g. through a video):

- **CA/B forum (EV):** only if authenticity verified, i.e. not improperly modified when compared with the underlying original AND recognized as legal substitutes for originals under the laws of the CA's jurisdiction [i.56].
- **UK: Guidance on Identity proofing:** if a physical document, it should be protected by physical security features [i.57].
- **ANSSI: verification des titres d'identité a distance:** Remote verification of authenticity of an identity document, when this identity document is never physically present at any step of the verification process, can be considered as sufficient only if it is demonstrated that technical and organizational measures are in place and reduce the risk of fraud with an efficiency at least equal to physical presentation of an identity document. The identity document contains security characteristics that can be verified through picture or video (e.g. in color) or contains machine readable information, containing all the necessary information for the identification of the applicant, and authenticity of these information can be proven through the use of automated means performing cryptographic verifications (for example, a QR Code) [i.66].
- **BITS: Norway:** Documents are read by an application. This application also provides a "selfie" picture [i.70].
- **Spain: SEPBLAC Video Identification procedures [i.76] and [i.77]:** photograph or snapshot of the front and back of the identification document used. The photograph or snapshot obtained should meet the quality and clarity conditions that allow its use in research or analysis. The mere capture of frames of the video-identification process is not considered valid for these purposes.

- **Germany. BaFin Circular 03/2017 on Video Identification [i.80]:** Only identity documents with security features that are sufficiently forgery-proof, clearly identifiable and therefore verifiable both visually in white light and using the available image transmission technology as well as having a machine-readable zone may be used during the video identification process.

6.3.2.3.2 Digitally extracted from an ID electronic ID document

ACollection.TP 3: It is possible to reliably extract attributes from an electronic identity document either on premise or remotely.

ACollection.TP4: there are few requirements on **how** to extract attribute from an identity document:

- **UK. Guidance on Identity proofing:** if the evidence includes digital information, it should either be protected by: cryptographic security features that correctly identify the person or organization that issued [i.57]. Also (for highest level):
  - all digital information (including biometric information) is protected by cryptographic security features;
  - the cryptographic security features can prove which organization issued the evidence.
- **ANSSI: verification des titres d'identité a distance** : authenticity of these information can be proven through the use of cryptographic means (e.g. ICAO PKD registry for passports) [i.87].

6.3.2.3.3 Transmitted in purely digital form as an eID (or SSI)

ACollection.TP5: there is no prevention to acquire identity attributes through identity providers and/or SSI. However there are very few, if not no requirement on how to do it.

6.3.2.3.4 Communication channels

6.3.2.3.4.1 In the event of remote collection

This sub-clause looks at the different aspects of protection ; presentation of the leading IT protocol and APIs used for the transfer of ID attributes (e.g. SAML or OpenID Connect), description of customary security measures deployed to protect the communication channels, such as integrity of the attribute transmission (e.g. end-to-end encryption), presentation of customary workflow/parties; e.g. are ID attributes remotely presented by the applicant or obtained from a third party independent of the applicant?

ACollection.COM1: there are very few specifications on how to do protect the communication channel(s). Some documents limit their requirements to "have secure channel" without further prescription.

However, that secure channel(s) need to be put in place for other steps of the identity proofing process, such as the identity attributes and evidence validation and/or the mapping with the applicant. In this case, the collection if the identity attributes and related evidence is de facto covered.

The analysed documents that provide specifications are:

- BITS: Norway [i.70]:
  - Requirements for optical scanning of documents are posed, with validation requirements.
  - Requirements to NFC reading of documents are posed, with validation requirements.
  - Requirements for subject biometrics capture with liveness detection are posed.
  - Resistance against biometric attacks is described, referring to ISO/IEC 30107 ([i.32], [i.31], [i.118] and [i.28]) series of standards on biometric presentation attack detection.
  - Requirements for (security of) the client-side application (usually mobile app) are posed.
  - Requirements for (security of) the server-side application are posed.
  - Requirements for verification of identity by the server-side application are posed.

- National bank of Belgium [i.75]: Controls in place to ensure that identity documents produced during the transmission have not been altered:
  - built-in features which enable them to detect fraudulent documents, features that compare the security features ingrained in the identity document presented during the transmission with a template;
- EC Report on Existing Remote On-Boarding Solutions in the Banking Sector: Screen to be adequately illuminated [i.72].

6.3.2.3.4.2 In the event of physical presence

ACollection.COM2: there are few information on how to do secure the collection of attribute and evidence, but it is likely covered as a general features (e.g. as it is the case for ETSI EN 319 401 [i.9] that requires secure & trained personnel for the whole process). Otherwise, general requirements are requested, like:

- **Regulation 2019/1157 [i.41]:** biometric identifiers should be collected solely by qualified and duly authorized staff.

There is nevertheless one remarkable reference that addresses specifically the security of the collection of biometric data at the collection point:

- ISO/IEC 30107 ([i.32], [i.31], [i.118] and [i.28]) on biometric presentation attack detection.

6.3.2.4 Final remarks

The above analyse focused on the collection of attributes and evidence for legal and natural persons, or natural persons acting for a legal person. Some documents address more cases, e.g.:

- **ETSI EN 319 411-1 [i.10]**: it is also possible to collect attributes for system or device.

In Spain SEPBLAC Video Identification procedures [i.76**] and [**i.77**]:** evidence for Entities without legal personality or Investment funds are also covered.

National Bank of Belgium: evidence for trust or a similar legal arrangement are also covered: corporate name, the information referred to in 1° or in 2° regarding its trustee(s), its founder(s) and, where appropriate, its protector(s), as well as the provisions governing the power to make binding agreements on behalf of the trust or similar legal arrangement.

6.3.3 Attribute validation

6.3.3.1 Introduction

An official ID document should meet specific technical requirements to be considered functional and secure. Security features are an integral part of identity verification. The identity document should withstand attacks or manipulation to the document including but not limited to changing personal details, separating and reusing individual security elements or designing a forged or counterfeit document. This clause provides an overview of the customary security checks and a collection of elements that are implemented for a compliant identity verification process.

As a foundation for document security, specific elements or security features that are embedded within the ID document are verified. These security features both protect the document structure and personal data located therein. It is important to distinguish this analysis pertains to the attribute validation as in the security feature check implemented through a remote/online process (digitally extracted from ID documents or obtained via an eID or SSI). The goal is to determine that the evidence collected is genuine (issued by a recognized, independent/authoritative source) and is valid, meaning the document is not expired or revoked.

6.3.3.2 Findings

6.3.3.2.0 General

AValidation.1: Identity documents such as passports, cards such as national ID cards or driving license, eIDs, as well as alternative digital identification through cloud-based solutions, or mobile documents that are being developed, are/will remain vital for identity verification and authentication purposes.

AValidation.2: Electronic identity documents such as the national eID card or ePassports that are equipped with secure applications and a microprocessor provide additional layers of security to the physical features embedded on the document.

AValidation.3: Whether a technical specification or a national regulation, security features can be either visible and or invisible, or secret.

AValidation.4: The attribute validation relies on the strength of the proofing process to obtain the identity evidence. The elements of attribute validation vary depending on type of process (i.e. digital), legislation, specifications, and is not limited to other criteria.

The findings consider:

- Customary security checks implemented, and security features verified in relation to attributes collected as a digital representation of an ID document;
- Customary security checks implemented in relation to 'purely digital' attributes (digitally extracted from ID documents or obtained via an eID or SSI);
- Description of other checks implemented if any (e.g. matching with other data, verification of expiry date, etc.);
- Description of external (governmental) sources queries if any;
- Applicable technical standards if any.

The findings can distinguish between the following variations:

Optical (Use of Camera):

- Evidence is genuine: Dynamic security feature verification, checksum.
- ID attributes are valid: Official government ID, not expired, not invalidated.
- Authentication: Possession (ID card) + Biometrics.
- External sources required: no.
- Standards: for example - BaFin circular 3/2017 [i.80].

Federated (e.g. BankID):

- Evidence is genuine: Provided by source of the evidence (e.g. a bank) + federation protocol.
- ID attributes are valid: Provided by source of the evidence.
- Authentication: Provided by source of the evidence (e.g. SCA/PSD2 for banks).
- External sources required: Yes.
- Standards: not listed.

eID:

- Evidence is genuine: Mutual authentication against chip, validation of certificates.
- ID attributes are valid: Official government ID, validation against revocation list, digital signature of attributes.

- Authentication: Possession (ID card) + knowledge (PIN).
- External sources required: Yes, access to government infrastructure for validation/access.
- Standards: eIDAS + implementation acts.

SSI:

- Evidence is genuine: Validation of certificates, possibly Secure Enclave on mobile phone.
- ID attributes are valid: Depends on source of the attributes (e.g. could be from government ID card), validation against revocation list, digital signature of attributes.
- Authentication: Depends. Typically, method of mobile phone (e.g. possession of phone + fingerprint sensor of phone or PIN).
- External sources required: Depends. Some do require external validation, some are decentralized (e.g. based on DLT/Blockchain).
- Standards: W3C DID, otherwise very few.

6.3.3.2.1 Customary security features embedded and collected

Customary security features that are embedded to an ID document for collection should have security features implemented that are difficult to reproduce and be produced with materials that are not for commercial resale. These include both optically variable features, and secure printing elements:

- Security paper.
- Special high security ink.
- Holograms.
- Other surface structures.

Optical security features embedded in the document and common to an attribute validation includes:

- Hologram.
- Identigram.
- Kinematic structures.
- Tilted laser images.
- Typography.
- Window (e.g. personalized).
- Security thread (personalized);
- Optically variable ink.
- Microlettering.
- Guilloche structures.

6.3.3.2.2 Features

An official ID document shouldafford various elements and levels of security as part of its defensive measures against potential attacks. Elements common to the ID document include:

- Materials.
- Product structure.

- Technologies (an electronic level of security such as embedded software in electronic passports or national eIDS that have chip activated technology features to enhance its security).
- Security features.
- Graphical design.

Various components are then combined to reinforce the comprehensive verification process and that security features provide enhanced validation required in a remote process.

6.3.3.2.3 Document protections

To make forgery or counterfeiting very difficult for an attacker, an official ID document should offer the highest level of features that enhance the security of the document itself.

Experts selected in the design and printing of official government issued documents classify production and verification methods. Examples include:

- Printing process: With regard to "printable" security features on the document, there are first, second, and third level optical and non-optical also known as magnetic features, pigments, or printed ink that is either visible of invisible in daylight, or only visible in white light.
- First Level Security features can be categorized as Surface data. The basic security requirement is often referred to as overt security printing and includes the use of ultraviolet light, watermarks, or holograms and other features that are complimented by applying heat sensitive ink, optical variable ink or other application technologies.
- Second Level Security Features is more advanced than the physical security mechanisms from a level one feature by embedding encoded and confidential information inside or on the chip, which is itself embedded into the ID document. This includes magnetic strips, Radio Frequency Identification (RFID) or smart chips, with embedded identity and biometric data such as fingerprint scan.
- Third Level security features or Forensic Data provides security and integrity of information that can be accessed by forensic tools and authorized access to do so. The third level of security feature qualifies as the highest security level technology to secure an identity and the identity document.
- In the Lamination process: The lamination process brings together the individual layers or foils without reducing the integrity of print quality and protects the ID document from mechanical visible damage. If a "graphically structured lamination plate" is used for example, state-of-the-art surface elements such as MLI/CLI lenses, guilloche patterns with micro-lettering are used. Other innovative lamination technologies combine the graphical background printing design to form special 3D shapes, 3D photographs, and optical diffractive elements known as holograms on the surface of the ID document.
- Personalization: The final step is the integration of personal data and a photo of the identity document owner. There are several security features that ensure the integrity of the document such as micro letters, angle dependent information, 3D and ghost images.

6.3.3.2.4 Security Feature Check for a Natural Person

6.3.3.2.4.0 General

National regulations establish a minimum set of security feature checks on an ID document during a remote identification process to provide a higher degree of certainty that the ID attributes are not expired or revoked and that the evidence is genuine meaning it has been issued by a recognized independent/authoritative source.

6.3.3.2.4.1 Technical sources

The minimal requirements for the attribute validation depend on various outputs and as such does not always include detailed requirements in comparison to national regulatory requirements. For the following standards and sources, determination that ID attributes are valid and authentic fall simply to the Electronic Registered Delivery Service Provider (ERDSP) with no other specifications listed. Other sources simply map the identity of enrolled subjects with their certificate information (i.e. a certificate that support their signature and to ensure the signature is in the control of the subject).

Sources:

- ETSI EN 319 411-1 [i.10].
- ETSI EN 319 521 [i.15].
- EN 419 241-1 [i.40]/ETSI TS 119 431-1 [i.19].
- ISO/IEC 29115 [i.30] on entity authentication assurance framework.
- ISO/IEC 29003 [i.16] on Identity proofing.
- ISO/IEC 30107 ([i.32], [i.31], [i.118] and [i.28]) on biometric presentation attack detection.

6.3.3.2.4.2 Authentication Assurance Frameworks

The authentication assurance framework sources, as outlined by other standards, framework for managing authentication assurance within a given context and specify up to four (4) levels of authentication assurance (e.g. ISO/IEC 29115 [i.30]). These sources in whole or in part normatively prescribe the criteria and guidelines for achieving levels of entity assurance as well as the controls that mitigate authentication threats. The scope of these sources does not prescribe requirements for attribute validation as such. Noteworthy to this clause, however, is the reference of processes necessary to checking identity information and credentials -i.e. against data sources, issuers, and other resources. These processes relate to the authenticity, validation, correctness, and ability to bind the identity information to the entity.

For this reason, these sources are relevant to connecting the identity process and migitging authentication threats. A threat assessment should include relevant attacks and the applicable resistance to such attacks. It should consider risks that can result from verification to validation through remote or electronic identification means. In ISO/IEC 29115 [i.30] for example, it mentions attack scenarios including online guessing, credential duplication, phishing, replay attack, session hijacking, man-in-the-middle, credential theft, or spoofing scenarios.

Sources:

- Regulation 2019/1157 [i.41] on strengthening the security of identity cards.
- Guidance for the application of the levels of assurance which support the eIDAS Regulation [i.22].
- CIR EU 1501 [i.2].
- FIDO Alliance White Paper: Using FIDO with eIDAS Services [i.88].
- EC Report on Existing Remote On-Boarding Solutions in the Banking Sector [i.72].
- EU commission eID/KYC expert group 'assessing portable kyc/cdd solutions in the banking sector' report ('report2') [i.72].
- FATF digital identity guidance [i.74].

6.3.3.2.4.3 Blockchain technology and other alternative frameworks sources.

Blockchain Technology utilizes signature and encryption methods that are tamper proof to ensure secure information integrity and authentication. Since the concept of expiration or revocation is not handled by default in blockchains, it can be done through classical data crypto validation. Its governance is built on a related trust model that is issued from an authoritative source that is issued and supported by a source external to the blockchain.

The alternative sources listed below do not explicitly detail attribute validation in their scope. As such, these sources make reference to validation for example with CIR 1502 [i.3] or referencing Peer Review feedback that highlights the complexity of verification and validation of identity documents, especially in the case of foreign identity documents that are used for an eID (as it is the case for some of the already notified eID schemes). It recommends:

- International databases such as the Schengen Information System (SIS) or Interpol databases, PRADO database for verification of optical/physical security features of identity documents, iFADO (Intranet False and Authentic Documents Online) should be used to confirm the documents' validity.
- If the verification is performed physically or if the identification is performed solely based on the picture of a document, a professional and trained agent should assess the validity of the document.

Sources:

- NISTIR 8202. Blockchain Technology Overview [i.82].
- ILNAS White Paper on Blockchain and distributed ledgers technology, economic impact and technical standardization [i.83].
- Decentralized Identifiers (DIDs) [i.84].
- PRADO [i.86].
- NISTIR Draft Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification [i.125]
- NISTIR Draft Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification [i.126]

6.3.3.2.4.4 Certification Authority Browser Requirements

A framework for certification authorities establishes the evaluation of any document for alteration or falsification, and the document's validity by checking the age of the information provided, frequency of updates on information sources, the purpose of the data collection, the public accessibility of the data available and how difficult it would be to falsify or alter the data.

An Extended Validation (EV) attests to the signing of a personal statement and the identity of the signer, the EV should identify the original vetting documents used to perform the identification and verify reliable methods of communication.

Source: CA/Browser forum requirements

6.3.3.3 National Regulation

6.3.3.3.0 General

National guidelines can vary by score, the required number of randomly selected security features that are to be checked, or by different market use cases (i.e. from AML compliance, electronic identifications, to considerations such as the customer's risk profile, relationship or transaction) and can include a cross reference check to other sources (e.g. PRADO [i.86], including but not limited to a credit reference check, a check against the population register, or against a combination of multiple reliable sources that can be supplemented with data analysis, IP address analysis, and location or device analysis as well).

In each, the attribute validation verifies that a document has not been falsified or manipulated and is official. The process checks whether the document:

- is genuine (not forged or counterfeit);
- is issued by an authoritative source;
- has not expired;
- has not been cancelled or reported as lost or stolen;
- has visible security features that are genuine;

- queries validate that information matches official sources;
- affords reliable checks against the legitimate owner (matching of the automated calculation of the check digits in the machine-readable zone and the cross-check of information provided there with the information visible on the identity document; examination of the orthography of the digits, the authority code and the typefaces to ensure that they are correct); and
- has security features that are visually recognized in white light.

6.3.3.3.1 Framework for electronic validation

When financial institutions verify the customer's identity by electronically reading the data registered on the microprocessor of his identity card, there should also be a simultaneous electronic verification to ensure that the data included on the chip was signed electronically by the National Register (i.e. this is feasible for all ICAO 9303 MRTD SoD's signature provided the CSCA cert. and CRLs are available). This implies CRL check.

Sources:

- France: ANSSI: vérification des titres d'identité à distance [i.66].
- Germany: BNtA 126/2017 [i.67].
- Germany: BNtAg 208/2018 on eIDAS [i.68].
- Germany: BaFin Circular 03/2017 on Video Identification [i.80].
- Germany: TR-03147 on Assurance Level Assessment of Procedures for Identity Verification of Natural Persons [i.64].
- Spain: SEPBLAC Video Identification procedures [i.76] and [i.77].
- Italy: Provision of Bank of Italy on arrangements for appropriate customer verification to combat money laundering and terrorist financing [i.79].
- Romania: Communication for Qualified Trust Service Providers [i.65].
- BITS: Norway, Requirements for secure digital verification of identity [i.70].
- National Bank of Belgium: Object of the identification and identity verification: Comments and recommendations [i.75].
- UK: Guidance on Identity proofing and authentication [i.57].
- UK: Draft BSI 8626 Design and operation of online user identification systems [i.63].
- US: NIST Special Publication 800-63 Digital Identity (multipart [i.43], [i.44], [i.45]).

6.4 Attribute binding

6.4.1 Introduction

Mapping ID attributes with applicant - also known as the 'attribute binding' can be defined as the steps taken to confirm, with a given degree of confidence, that the claimed identity credentials (for example those shown in a passport or ID card) which have been obtained and confirmed as valid are indeed those of the applicant and not of someone else.

In face to face interactions, this process typically implies comparing the physical characteristics of the purported holder with the credentials information - most notably the age, sex as well as photo shown in an ID or travel document, but may include additional steps as required, such as collecting biometric data. The same principles can apply, mutatis mutandis, to 'Supervised remote' interactions where the applicant is not in the same location as the live operator performing the identity-proofing process.

In other remote interactions, this process is performed in a variety of manners which can involve the confirmation of a password or code or the remote implementation of an automated biometric confirmation process, with differing LoA outcomes. This implies that knowledge-based, possession-based or inherent (biometric) authentication factors are used for identity-proofing processes which can be implemented in a 'full-remote' automated way, without involving any operator for the identity-proofing service provider.

6.4.2 Findings

Binding.1: As remote identity-proofing tends to become 'the new normal', a trend reinforced by the Covid-19 pandemic, ensuring that the presented identity credentials correspond to the person whose identity is claimed takes a new significance and is now a process at the forefront of recent technology developments, especially with increasing availability of biometric-enabled devices and the wider deployment of NFC functionalities for smartphones.

Binding.2: Identity-proofing technology solutions are now available both for Android and IOS- based mobile devices offering improved customer experience as well as deployment scalability. These increasingly make use of NFC reading functionalities allowing the secure remote retrieval of ID data, including passport or ID photo, request the applicant to take a selfie and compare it with the official ID photo as well as perform a number of liveliness detection tests to combat spoofing and other online fraud. These are generally viewed as offering better reliability and expected to gain prominence in the coming years as well as become standard practice in the not-too-distant future.

Binding.3: There is significant uncertainty as to what 'equivalence to physical presence' means in practice. This illustrates a clear need of clarification and standardization. 'Physical presence' is often defined as a benchmark but remains a loose notion that but not meaningfully specified, especially for the attribute binding dimension (to give one example, not all personnel implementing identity-proofing processes are as trained as custom officers).

Binding.4: The *Collection Documents* rarely consider the Attribute binding process in isolation or assume that its takes place 'in person', without further analysis. As a result, there is little literature specifically dealing with this dimension, especially when taking place on a remote basis.

List of the most relevant *Collection Documents*

- NIST 800 63 3 [i.36].
- EU implementing Regulation 2015/1502 [i.3] and related ECN LoA guidance.
- BSI TR 03147 [i.64].

Binding.4.1: 'In-person/physical appearance' attribute-binding - i.e. the process of ensuring, with a sufficient degree of assurance, that the person physically present is indeed the one whose credentials have been obtained and confirmed as valid is largely undocumented and seem to primarily rely on the visual skills of the operator, without further requirements or applicable metrics.

Part of the problem stems from the fact that the reliability of physical presence identity-proofing is highly contextual and dependent upon the skills and training of the operator performing it - an experienced custom officer will likely achieve better false-acceptance results than say a bank employee performing KYC processes for a new client. In addition, no metrics are generally available for physical presence identity proofing processes, further affecting the practicality of benchmarking exercises.

Binding.4.2: As a result, there is significant uncertainty as to what constitutes 'equivalence to in-person/physical appearance'.

Article 24.1 (d) of eIDAS refers to "other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence". The wording is also to be found in ETSI EN 319 411-2 [i.11] (clause 6.2.2)

Binding.5 The 'Supervised remote' Attribute binding process has been recognized for regulatory purposes in a number of situations and countries but has not achieved universal recognition.

The 'Supervised remote' Attribute binding process implies human interactions at both ends, i.e. with an operator conducting a video interview of the applicant, with minimum technical specifications and requiring the applicant to perform certain actions live.

List of the most relevant [Collection Documents] addressing 'Supervised remote' Attribute binding processes:

- NIST 800 63A [i.43]
- BaFin Circular 3/2017 (GW) - video identification procedures [i.80]
- Spain: SEPBLAC Video Identification procedures [i.76] and [i.77]

Binding.5.1: There is no generally recognized framework for the 'Supervised remote' attribute binding process or more generally video identification.

Binding.6: The 'full remote' (automated) attribute binding process makes use of authentication factors, with low and Substantial LoA requirements typically relying on 'knowledge-based' and/or 'possession-based' factors. The use of 'inherence-based' factor - in practice biometric validation - appears eligible for higher LoA requirements.

Binding.6.1: The 'full remote' (automated) attribute binding process is a recent development which has not, as of today, yet been fully specified and recognized by regulatory authorities for the purpose of achieving a high LoA.

A number of drafts and proposals are being prepared:

- Norway: BITS Requirements for Solutions for Secure digital verification of identity [i.70].
- UK: BSI BS 8626 Design and operation of online user identification systems [i.63].

A possible reason appears to be that 'full remote' automated Attribute binding processes aiming at a high LoA make use of biometric technologies that, as of today, cannot be easily reconciled with the existing LoA framework.

Binding.6.2: As for the Attribute Collection and Attribute Verification phases, the fact that the Attribute binding phase is performed remotely brings new opportunities as well as new risks that are increasingly investigated and considered, but in relation to which a consensus is only gradually emerging.

Binding.6.3: The deployment of automated biometric processes for Attribute binding purposes is viewed as offering false match rate improvements compared to in-person processes;

Binding.6.4: A number of key metrics are gaining prominence for the assessment of attribute binding processes, especially when using inherence-based factors.

In Europe, eIDAS refers to 'physical presence', 'possession of the [credential] evidence' and 'comparison of one or more physical characteristics of the person with an authoritative source'.

Clause 2.1.2 of the Annex of EU Comission Implementation Regulation 2015/1502 [i.3] addresses remote identity proofing by referring to:

- A presumption that the Attribute binding process is valid for the Low LoA;
- A requirement that the applicant is 'verified to be in possession of the *credentia*l evidence' for the Substantial LoA;
- A requirement that 'the applicant is identified as the claimed identity through comparison of one or more physical characteristics of the person with an authoritative source'.

The revised eIDAS Cooperation Network LoA Guidance draft in relation to Regulation 2015/1502 [i.3] identifies two useful criteria for the evaluation of the reliability of the Attribute binding process: low false-match rate and ability to defeat high potential attacks. However, these are not further defined or discussed.

A number of key criteria are increasingly considered for such purpose:

- The Personal Attack Detection (PAD) rate;
- The Attack Presentation Classification Error Rate (APCER);
- The Bonafide Presentation Classification Error Rate (BPCER).

(See ISO/IEC 19989-3 [i.23] for details on their definition and related terminology.)

Assuming satisfactory PAD results, there is an increasing linkage between the APCER and the required Identity-proofing LoA, meaning that a High LoA needs to show the ability to defeat 'High' potential attacks whereas a Substantial LoA needs to show the same with respect to Moderate potential attacks. Illustration can be found in TR-03147 [i.64].

Binding.7: Identity-proofing use cases deployed by the financial sector subject to AML-CFT requirements customarily achieve a Substantial LoA level which can be performed on a full-remote basis without the use of biometric solutions.

The AML-CFT regulatory framework of most countries tend not to require a High LoA identity proofing, a trend likely to be increased with the FATF digital identity guidance of March 2020 [i.74] offering significant risk-based flexibility to regulated entities.

6.5 Security requirements

6.5.1 Introduction

Security requirements for identity proofing in the context of ETSI/ESI has two different aspects:

1) Security of the operation of an identity proofing service, including its environment, equipment, procedures, personnel, etc.

2) Security related to specific identity proofing mechanisms, their operation, their ability to protect against specific attacks, and additional policy and security requirements on operation of the specific identity proofing mechanisms.

The technologies used for the identity proofing means, e.g. characteristics and security of biometric algorithms, are out of scope, as is security of physical identity documents.

For item 1, a trust service component is subject to the same basic set of requirements and be able to provide equivalent security as the trust services of which it is a component.

For item 2, at least the following means can be envisaged:

- Physical appearance with verification against physical identity document and possibly use of biometrics.
- Use of an existing eID that authenticates the person.
- Use of an electronic signature/seal authenticating supported by a certificate that identifies the person.
- Remote video interview session with verification against physical identity document and possibly biometrics.
- Remote reading of chip in identity document with face photo and biometric comparison.
- Remote session with photo and possibly optical reading of identity document, and photo of face with either automated (biometric) recognition or manual check.
- Proof of possession, e.g. of a mobile phone or email address.
- Other means and combination of several means.

ETSI DTS/ESI-0019461 [i.50] should describe best practice for secure provisioning of those means that are considered relevant, which may not be the complete list above.

6.5.2 Findings

6.5.2.1 Security of an identity proofing service

6.5.2.1.1 Identity proofing component and relationship to trust services

In the context of the work in ETSI/ESI, this is defined as a trust service component, meaning the following:

- It is a defined component of the operation of a trust service.

- This component can be an integral part of the trust service operation, but it can also be outsourced to a subcontractor specializing in identity proofing.
- A specialized identity proofing service can undergo independent conformity assessment to obtain a conformity assessment report that can be used as a component in the conformity assessment and supervision of the trust service providers to which it delivers identity proofing services.
- Explicit supervision of an identity proofing provider may be foreseen at least at national level.

An identity proofing service that is used for trust services can also fulfil other purposes such as identity proofing for electronic ID issuing and for enrolment in services such as banking. Security requirements for other use cases may be aligned with security requirements for trust services but may also differ.

As a component of a trust service, the identity proofing service should comply with the trust service regarding security and policy requirements. A clear conclusion is that security and policy of an identity proofing service is expected to be based on ETSI EN 319 401 [i.9], which is the common basis for all trust services. Further policy and security requirements can be derived from specific standards for specific services. ETSI EN 319 401 [i.9] is considered to cover the relevant requirements for the ISMS (Information Security Management System) of the service provider and use of the applicable parts of the ISO/IEC 27000 family of standards [i.123].

6.5.2.1.2 Requirements from ETSI standards for trust service security and policy

ETSI EN 319 411-1 [i.10] poses policy and security requirements for certification authorities. The standard defines several policies, where the LCP, NCP, and NCP+ policies are relevant for natural and legal person and natural person representing a legal person. NCP requirements for identity validation for a natural person generally refer to physical presence or means that are considered equivalent to physical presence. LCP is explicitly intended for certificates where a lower level of identity proofing is sufficient. Note that identity proofing generally is the task of the RA (Registration Authority) component of a certification authority.

The policies IVCP, DVCP, OVCP, and EVCP defined by ETSI EN 319 411-1 [i.10] apply to web-site certificates. The first three build on the LCP policy, while EVCP builds on the NCP policy. All web-site certificate policies are enhanced to refer to requirements from CA/Browser Forum guidelines.

ETSI EN 319 411-2 [i.11] defines the specific policies QCP-l/QCP-l-qscd for legal persons, QCP-n/QCP-n-qscd for natural persons, and QCP-w for web-site certificates. Initial identity validation for these policies should be done either by physical presence or by "methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence". In addition, the requirements of the eIDAS Regulation Article 24.1 apply to issuing of EU qualified certificates [i.22].

ETSI TS 119 431-1 [i.19] specifies policy and security requirements for TSP service components operating a remote QSCD/SCDev. The standard has no specific requirements for identity proofing, except noting that this should be done according to the policy and practices of the certification authority that issues the certificate for the public key of the subject's signing key pair. Thus, for remote signing, the requirements of ETSI EN 319 411-1 [i.10] and ETSI EN 319 411-2 [i.11] generally applies regarding identity proofing. In the same application area, the standard EN 419 241-1 [i.40] refers to eIDAS assurance levels for eID and eIDAS implementing regulation (EU) 2015/1502 [i.3].

ETSI EN 319 521 [i.15] specifies requirements for ERDS (Electronic Registered Delivery Service). The standard only poses explicit requirements for identity proofing for qualified ERDS, where the identity of senders should be verified by physical presence or means that are considered equivalent to physical presence, by an electronic identity means at assurance levels substantial or high as defined for eIDAS, or by a certificate of an advanced electronic signature or seal.

The ETSI security and policy requirements for the trust services signature validation, signature preservation, and timestamping do not contain requirements for identity proofing as these services do not have the need to prove identity of natural or legal persons as trust service subjects, only as customers of the service. The same applies to the standard ETSI TS 119 431-1 [i.19] and ETSI TS 119 431-2 [i.134] on security and policy requirements for TSP service components supporting AdES digital signature creation.

6.5.2.1.3 Requirements from other documents

Several other documents provide input on security and policy requirements. The standard ISO/IEC 29003 [i.16] is specifically on identity proofing and provides definitions and concepts that may be reused by ETSI/ESI. From a security viewpoint, Annex B on contra-indications and fraud detection is noticeable.

The eIDAS implementing regulation (EU) 2015/1502 [i.3] and its accompanying guidance document pose requirements for identity proofing relatively to the identity assurance levels defined by eIDAS. The eIDAS assurance levels are increasingly adopted not only where mandated, for cross-border use for government services, but also nationally. They may become de facto the European standard levels not only for cross-border use. Policy requirements for trust services in Europe may be linked to eID assurance levels.

Internationally, the standard ISO/IEC 29115 [i.30] defines identity assurance levels and is a foundation for the eIDAS levels. The standard lists threats and required controls but is not updated, e.g. mobile equipment was not in scope at the time of writing.

The CA/Browser Forum requirements for issuing of EV certificates are of relevance but are in general covered by ETSI EN 319 411-1 [i.10] and ETSI EN 319 411-2 [i.11].

National documents provide useful input on policy and security requirements, such as UK guidance [i.57] on identity proofing and authentication with Good Practice Guides, NIST Special Publication 800-63 (multipart [i.43], [i.44] and [i.45]), German TR-03147 [i.64], specification from BITS in Norway [i.70], and Italian guidelines for KYC for AML purposes. The UK guidance documents are particular in that they include identity proofing for legal persons.

Germany and Spain have national specifications that outline a video interview process as described in clause 6.2.2.2.

Draft specifications from UK and France are evaluated to include useful input on policy and security requirements. Draft documents cannot be directly referenced by ETSI/ESI, but the content may still be used as basis for recommendations.

The study on existing remote on-boarding solutions in the banking sector, published by the European Commission eKYC expert group, contains useful state-of-the-art information on different user identification journeys with security checks.

6.5.2.2 Security of identity proofing means

6.5.2.2.1 Introduction

Above, several identity proofing means were identified:

- Physical appearance with verification against physical identity document and possibly use of biometrics.
- Use of an existing eID that authenticates the person.
- Use of an electronic signature/seal authenticating supported by a certificate that identifies the person.
- Remote video interview session with verification against physical identity document and possibly biometrics.
- Remote reading of chip in identity document with face photo and biometric comparison.
- Remote session with photo and possibly optical reading of identity document, and photo of face with either automated (biometric) recognition or manual check.
- Proof of possession, e.g. of a mobile phone or email address.
- Other means and combination of several means.

In this clause, some analysis is done regarding security requirements based on the documents studied and the answers received for the questionnaires. The analysis separates certain sub-means that are used by several procedures, use of physical identity documents, provision of photo for biometric or manual comparison, biometrics, and use of auxiliary sources for identity information.

In addition to the overall information provided below, input from vendors of identity proofing services and products is important for more detailed requirements.

6.5.2.2.2 Use of identity documents

The unquestionably most secure way to use an identity document is to read the contents of the chip embedded in the document, for documents that have such a chip according to ICAO 9303 specifications on eMRTD. This applies to most passports and many national ID cards. The chip contains the same information that is printed on the passport or ID card, including a high-quality face photo. Fingerprints may also be stored in the chip, but these are generally not available except for border control. The chip's content is signed by the issuer and can be verified by use of the appropriate certificate.

The chip interface is NFC (Near Field Communication). Reading the content implies photo of the MRTD print on the passport or ID card necessary to obtain access to the chip, then an NFC enabled device is needed to read the chip content. In practice, this today requires use of an app on a mobile phone, alternatively specialized equipment of similar type as used in border control. Use of a PC or similar with a connected NFC card reader may be possible. All communication channels should be secured, and app security is important. Information read from the chip should be transferred through the app and mobile phone to be processed server-side.

For documents that do not contain an NFC chip, or when reading of the NFC chip is impractical, physical examination of the identity document is necessary. This can be manual, upon physical appearance or to examine the result of a remote capture of the identity document's appearance. The examination can also be automated by optical scanning of the document with automated verification against expected appearance.

Physical examination of an identity document should verify that it is a document type that exists, and that the document has the expected visual appearance for the document type. This includes checks against specified security elements of the document to the extent possible. From optical scanning one can obtain a face photo of the document holder, but the photo resulting from a document scanning will have considerably poorer quality than a picture read from the chip of a document.

Whenever possible, verification of an identity document should include a check that the document is not revoked or otherwise declared invalid by the issuer. Note that for passports and national ID cards, such checks may not be available at all or be restricted to access by government organizations or for border control.

6.5.2.2.3 Provision of photo by applicant

Many of the processes listed above include use of a face photo of the applicant for either manual or automated comparison to the face photo of an identity document. Comparison may be manual or based on face biometrics. Comparison may also be based on a combination where manual and biometric comparison are used together, or where manual comparison is used as a fall-back when biometric comparison does not yield a clear result.

Where manual processes are used for the identity proofing, a face photo may be required as documentation of the appearance of the person present, even though the photo is not actively used in the identity proofing.

For reliable results, it is recommended that the face photo is obtained in real time during the identity proofing process and not simple upload of a photo. This requires a device with camera on the user's side. Furthermore, the process of obtaining the face photo should include protection against defined biometric attack vectors. E.g. the process should ensure that a live person is present in front of the camera, and that the photo is of this real person. Use of a secure app installed on the user's mobile device is today a good option.

The photo should be transferred to the server side for use, e.g. for biometric comparison.

6.5.2.2.4 Face biometrics and other biometrics

Increasingly, identity proofing will use biometric technology for comparison of an applicant against an identity document. This is relevant for remote identity proofing but can also be applied when physical appearance is used for identity proofing. Today, face biometrics is the only generally available technology. Reference photo may be obtained from the chip of the identity document, from optical scanning of the identity document, or in some cases from an identity register that includes photos (e.g. a passport register).

Other biometric information is currently not readily available from identity documents or registers, e.g. use of fingerprints is restricted. This does not rule out future use of fingerprint or other biometric mechanisms, e.g. iris. But in today's situation face biometrics is regarded as the only relevant mechanism.

Biometric algorithms and their quality and security are out of scope of the work in ETSI/ESI. Security of the biometric process is however relevant and may include issues such as false acceptance versus false rejection rate, conditions for an uncertain answer, resistance against biometric attack vectors (see in particular ISO/IEC 30107 ([i.32], [i.31], [i.118] and [i.28]). Several of the documents referred in the present document provide input on security of biometrics, e.g. the "requirements for secure verification of identity" from BITS in Norway [i.70].

6.5.2.2.5 Auxiliary sources of identity information

Initially, identity information will be obtained from the identity document presented in presence or remotely, or from an eID or e-signature/seal if such mechanism is used. There may be a need to obtain or verify further attributes from/against trusted sources. One example is to verify that a natural person has the required authorization to act on behalf of a legal person.

Only general policy and security requirements can be posed for use of such auxiliary sources of information. A source should offer information that can be trusted at the same level of assurance as required for the rest of the identity proofing process, but it is noted that attribute level of assurance as a measure is not widespread. This means that one may need to rely on subjective judgement regarding the reliability of information from such sources.

6.5.2.2.6 Physical appearance

Physical appearance is referred to in many contexts, including the standards mentioned in clause 6.6.2.1.2, as a benchmark for identity proofing, stated typically as physical appearance or means that provide equivalent assurance as physical appearance. However, in most cases there is no specification of what "physical appearance" means in terms of security and reliability of the process, e.g.:

- Which identity documents are accepted?
- What checks should be done on the validity of documents, e.g. security elements and revocation status?
- What is the process for verifying the person's identity against the identity document?
- What are the competence requirements for the personnel carrying out the process?
- What are the requirements for equipment and security of equipment, e.g. for manual or automated entering of the collected information into an RA (registration authority) application?
- What are requirements for records keeping (some general requirements exist in some standards)?

To exemplify, personal appearance can be at a passport office with highly skilled personnel in a secure environment. In other cases, physical appearance may be at a bank office, post office, or some other site that the trust service provider sees fit for the purpose.

For physical appearance to be useful as a benchmark for other identity proofing means, there is likely a need to specify at least two policy levels for the process, checks to be performed, and security.

6.5.2.2.7 Use of existing eID

Use of an existing electronic ID (eID) for authentication may be a major track for identity proofing of trust service subjects. In this case, the requirement should be on the assurance level of the eID and possibly on the attributes conveyed by the eID. Further attributes may be obtained from other sources such as registers, based on the identity from the eID.

6.5.2.2.8 Use of electronic signature or seal

Requiring a digital signature from an applicant to confirm identity is a highly relevant means. In this case, requirements are needed on the quality level of the certificate, e.g. by referral to the policies defined in ETSI EN 319 411-1 [i.10] ETSI EN 319 411-2 [i.11]. One may also pose requirements on the quality of the signature, e.g. requiring a qualified electronic signature can be a policy requirement.

The identity attributes available are initially those included in the certificate used for signing/sealing. As for use of eID, further attributes may be obtained from auxiliary sources.

6.5.2.2.9 Remote video interview with control against ID document

In a remote video identity proofing process, a video session is run, and usually recorded, leading the user through a defined procedure. The user has a device equipped with a camera; a mobile device will usually yield a better result than a PC. On a mobile device, an app may be used for the procedure, but the procedure can also be carried out in a web interface on both a mobile device and a PC. The video session can be real time with a human operator steering the procedure and evaluating the result of the identity proofing. This can be likened to physical appearance but at a distance.

A remote video session may also be automated, where the user receives online instructions. The recorded video is typically examined at a later stage by a human operator.

In both cases, a human operator can be assisted by machine processing, e.g. for face biometrics, biometric attack detection, and analysis of the identity document.

A typical sequence of a remote video interview consists of the following steps:

1) The user shows an identity document that is moved to show that it is not a photo and to reveal as many security elements of the document as possible. A photo of the document is captured.

2) A video of the user's face is recorded, where the user may receive instructions on movements to show that it is a live person and the user's real face. A face picture is captured.

3) The picture on the identity document is compared to the face picture, either manually or by face biometrics, or using a combination of biometrics and human judgement.

4) Identity information is captured from the identity document.

5) Other steps may be used in the process, e.g. questionnaire to gather more information.

The main security issues of the process are verification that the document is not fake and protection against biometric attacks like "deep fake" face fraud. Policy is defined regarding e.g. documents accepted, the process steps, competence of human personnel, recording and storage of evidence, and degree of automation of the process.

6.5.2.2.10 Remote reading of chip in identity document with control against ID document

This process is mostly useful when the user has a mobile device with NFC reader and camera, and with a suitable app installed. The app should be secure and communicate in a secure way with a designated server that carries out the identity proofing procedure. Although in theory possible, carrying out the entire process in the app on the phone is not recommended.

A typical process has the following steps:

1) Use camera to take a photo of the MRTD field of the identity document. A video sequence may be used to verify that it is a real document and not a photo.

2) Hold the identity document against the phone for a few seconds while the interface to the eMRTD application on the chips is called and the information read out and transferred to the server.

3) On the server verify the issuer's signature on the information and extract information and face photo.

4) Use the device camera to obtain a new face photo of the user. Usually, a video sequence will be run to ensure that a real person is in front of the camera. Instructions on movements and other mechanisms may be used. The photo is transferred to the server.

5) Face biometrics is used to compare the two face photos. Since good quality photos are used, the biometrics comparison can be very reliable if a state-of-the-art algorithm and reasonable parameters for false acceptance and false rejection rates are used.

6) Other steps may be used in the process, e.g. questionnaire to gather more information.

This process is usually fully automated. Manual verification may be used for quality assurance and for judgment in case the process yields a negative or non-conclusive result. State-of-the-art face biometrics using good quality photos can be considered on par with physical appearance judged by skilled personnel.

Specific security issues for this identity proofing means are related to security of the app used, to ensure that it is not possible to insert an information package copied from the chip of another document (assuming that forging an information package or changing its content is practically impossible) and/or a photo different from the one captured in the process. Biometric attack vectors should be considered as for all other processes that use biometrics. Security and reliability of the server-based processing is important.

6.5.2.2.11 Remote optical reading of identity document with control against ID document

For identity documents without an NFC chip, or when reading the NFC chip is impractical, the identity document may be optically scanned, deriving the face photo, and reading identity information by OCR (optical character recognition). Then, the camera on the user's device is used to obtain a face photo, preferably using liveness detection procedures as for the video interview and NFC reading cases. This process can use an app on a mobile device or be done in a web interface.

NOTE: A process that consists merely of upload of a photo of the identity document and of the user will yield weak security against manipulation of the identity document and/or the photo.

The photo scanned from the identity document and the fresh face photo can be compared automatically in real time by face biometrics. Since the photo quality obtained from the optical scanning is low, a relatively large number of the biometric comparisons are expected to yield a non-conclusive result. These cases may be resolved either by repeating the process or by manual verification as a fallback mechanism.

Due to the risk of a non-conclusive result from face biometrics in this case, the identity proofing provider may decide to always use manual verification, possibly enhanced by face biometrics. Manual verification may be done in real time or later depending on the identity proofing provider's policy.

Security issues for this identity proofing means are similar to the NFC reading process. Protection against insertion of photos, of document and the user's face, is important. Biometric attack vectors should be considered as for all other processes that use biometrics. Security and reliability of the server-based processing is important. Security of manual processes is expected to be ensured similarly to the remote video procedure.

7 Conclusions

The present survey demonstrates the general applicability of the general method of decomposing identity proofing process into 3 steps, i.e. the attributes and evidence collection, the attributes and evidence validation and the biding with the applicant (see clause 4.2.3). It also confirms the classification of identity proofing process into three main categories; those requiring on-site physical presence, the remote and attended, and the fully automatic processes (in some cases, they can still be later overseen by a registration officer).

The Technical Specification proposed to follow the present document (ETSI DTS/ESI-0019461 [i.50]) is to focus on providing "best practices" for identity proofing. The present survey provides good basis to build such best practices. In particular, the best practices should:

- Offer consistent guidelines for both face to face and remote identification scenarios in terms of reliability and risk management;
- Support identity proofing requirements for trust services including trust services qualified under eIDAS regulation 910/2014. They should be applicable to normalized and qualified trust service policies;
- Aim to serve other contexts such as KYC (know your customer) and anti-money laundering (AML);
- Be applicable to any of the three electronic identification scenarios being considered in the eIDAS Regulation review (baseline, introducing new trust services for identification and a European identity scheme);
- Be applicable to both substantial and high levels of electronic identification as identified in Regulation 2015/1502 [i.3];
- Support identity proofing provided as a component of a wider (trust) service, or subcontracted to a specialized (trust) service component provider (identity proofing provider), possibly supporting several service providers, whether operating as a trust service or providing other types of identity related service; and, finally,
- Aim to provide a common reference for policies and standards using identity proofing.

Annex A:
CEN and ISO standards of relevance to Identity proofing

A.1 Introduction

This Annex identifies existing standards and to some extent standards in progress in ISO/IEC JTC1 and the European standards organization CEN and assesses their relevance to identity proofing. While many standards have relevance, only a few are of core importance to the work in ETSI/ESI. Three sub committees of ISO/IEC JTC1 have published relevant standards. In CEN, the relevant specifications are developed by CEN/TC224.

A.2 ISO/IEC JTC1/SC17 Cards and security devices for personal identification

This committee publishes standards related to physical identity cards and devices, which are relevant to identity proofing of trust service subjects in that such identity proofing may rely on both physical documents and digital information embedded in chips in such documents. Notably, the committee has standards on physical characteristics of ID cards, on machine-readable travel documents, communication towards contact-based and contact-less chip in ID cards.

The ISO/IEC 7501 [i.89] series of standards is ISO/IEC's issuing of the ICAO 9303 documents on machine-readable travel documents. See review of the ICAO document.

The ISO/IEC 7816 [i.90] series of standards specifies the interface to communicate with cards that contain a contact-based chip, meaning physical and electrical contact is necessary to communicate with the chip. This standard is referred to for contact-based smart cards.

For contactless cards, three standards exist. ISO/IEC 14443-1 [i.91] on proximity cards is the most relevant, being the basis for the NFC (Near Field Communication) standards in ISO/IEC 18092 [i.92] (also ECMA-340) and ISO/IEC 15693-2 [i.93] (also ECMA-352) and thus also for the NFC interfaces of most passports and identity cards and for standards by GSMA and ETSI and more. The standards for close-coupled cards (ISO/IEC 10536 [i.129]) and vicinity cards (ISO/IEC 15693-2 [i.93]) are less relevant.

The ISO/IEC 18013 [i.140] series of standards specifies ISO-compliant driving licence and is relevant to identity proofing when a driving license is used as an identity document. The specification covers both visual and machine-readable features, which may include contact-based and contact-less chip in a driving licence document. Also note ISO/IEC TR 19446 [i.94]describes differences between ISO-compliant driving licences and the European Union driving licence specifications.

A.3 ISO/IEC JTC1/SC27 Information security, cybersecurity, and privacy protection

This committee publishes some standards that are very important to identity proofing. Notably, the ISO/IEC 27000 [i.123] series of documents are important to security and policy requirements, with the standards ISO/IEC 27001 [i.24], ISO/IEC 27002 [i.35], and ISO/IEC 27005 [i.127] as the most important ones. Use of these standards for trust services and trust service components is covered by reference to ETSI EN 319 401 [i.9] as a common basis for policy and security requirements.

The ISO/IEC 24760 series [i.122] specifies a framework for identity management. This is relevant as identity proofing is part of identity management, however, the ISO/IEC 29003 [i.16] that covers specifically identity proofing is the most important input document to ETSI/ESI from SC27. This standard is separately reviewed in the present document.

In privacy, ISO/IEC 27701 [i.95] is a new standard that extends ISO/IEC 27001 [i.24] and ISO/IEC 27002 [i.35] for privacy information management, and that can be relevant in the context of identity proofing. The same applies to ISO/IEC 29100 [i.136] on privacy framework, ISO/IEC 29101 [i.96] on privacy architecture framework, ISO/IEC 29134 [i.97] on guidelines for privacy impact assessment, ISO/IEC 29151 [i.137] on code of practice for protection of personal information, ISO/IEC 29184 [i.98] for online privacy notices and consent, and ISO/IEC 29190 [i.138] on privacy capability assessment model.

ISO/IEC 19792 [i.99] on security evaluation of biometrics and ISO/IEC 24745 [i.100] on biometric information protection can be relevant to specification of security for use of biometrics in identity proofing, also refer to the standards from SC37 below. However, the standards are old, from 2009 and 2011 respectively, should be used with care. They are currently undergoing revision in SC27.

Work is ongoing in SC27 on a new ISO/IEC 19989-3 [i.23] series of standards for criteria and methodology for security evaluation of biometric systems, including presentation attack detection is also a topic in SC37 (see below), but extends this by testing. This work is potentially important to identity proofing.

The ISO/IEC 24761 [i.101] standard specifies authentication context for biometrics, meaning means to convey and check the validity of results of a biometric enrolment and verification process executed at a remote site. The standard may be relevant to providers of identity proofing services and products but is considered out of scope for the present work in ETSI/ESI.

Further work of SC27 includes cryptography and security services that use cryptography, evaluation criteria for IT security (the ISO/IEC 15408 [i.25] series), conformance testing and security evaluation, network security, application security, cloud security, incident management, digital evidence and investigation, timestamping, and more. Many of these standards can be relevant for providers of identity proofing services or products but they are either out of scope for the current work in ETSI/ESI or covered by reference to ETSI EN 319 401 [i.9] and/or ETSI EN 319 403-1 [i.139].

A.4 ISO/IEC JTC1/SC37 Biometrics

Since identity proofing in many cases will use biometric mechanisms, the standards of this committee become relevant. Most of the standards are relevant only for technical implementation of identity proofing with biometrics, but there are also standards that are useful for policy and security requirements for identity proofing, which is the scope of the work in ETSI/ESI. Note also that ISO/IEC JTC1/SC27 works on security of biometrics, see above.

Notably, the ISO/IEC 30107 ([i.32], [i.31], [i.118] and [i.28]) series specifies biometric presentation attack detection. This covers characterization of attacks that take place at the sensor during presentation and collection of the biometric characteristics. An identity proofing solution that uses biometrics should utilize protection against such attacks. This standard is separately reviewed in the present document.

The ISO/IEC 24779 [i.102] series of standards define pictograms, icons, and symbols for use with biometric systems. This standard should be referred to for the user experience of biometric systems.

The ISO/IEC 19784 [i.103] series of standards specifies a Biometric API (Application Programming Interface). The topic is not directly relevant to the scope of the work in ETSI/ESI, but the API may be useful to providers of identity proofing products or services. The ISO/IEC 30106 series [i.130] specifies an object oriented BioAPI with specific parts for implementations in Java™, C#, and C++.

The ISO/IEC 19785 [i.104] series of standards defines a Common Biometric Exchange Formats Framework (CBEFF) to define and register format specifications for biometric information. A CBEFF data structure is called a Biometric Information Record (BIR) and describes a Standard Biometric Header (SBH) with metadata to describe the characteristics of the biometric data contained in the data structure. The BIR and SBH can also support security of the biometric data. CBEFF requires a Biometric Registration Authority (RA) to register identifiers of biometric organizations, who may publish specifications (standards or proprietary formats) for Biometric Data Blocks (BDB) and how these are referenced from a BIR with SBH. The full specification of a BIR is called a patron format.

The ISO/IEC 19794 [i.105] series of standards describes biometric data interchange formats in terms of general common content, meaning, and representation of biometric data formats in part 1, and other parts of the standard describing formats for specific biometric means. These formats are registered under CBEFF with ISO/IEC JTC1 SC37 as RA, meaning they define BDBs. The new ISO/IEC 39794 [i.106] series defines extensible biometric data interchange formats based on ISO/IEC 19794 [i.105].

The CBEFF system is additionally used by industry standards bodies, governments (e.g. USA and India), commercial providers, and notably by ICAO for biometrics related to MRTD (Machine Readable Travel Document).

Biometric data formats are not directly relevant to the scope of the work in ETSI/ESI, but the topic may be very important to providers of identity proofing products or services.

The ISO/IEC 30108 [i.107] series, of which only part 1 is published as far back as 2015, builds on previous work by INCITS (the USA InterNational Committee for Information Technology Standards) and OASIS and specifies Biometric Identity Assurance Services (BIAS). A BIAS identity comprises a subject, biographic data, and biometric data. Further parts of the standard should specify specific BIAS implementations but have not been published. It seems like this standard has not gained any momentum, meaning ETSI/ESI may investigate it for relevant content, but it should probably not be referred to in any way.

Further standards from ISO/IEC JTC1/SC37 include biometric performance testing and reporting, conformance testing, quantification of biometric sample quality, and specific use cases for biometrics.

In addition, ISO/IEC JTC1/SC37 has published several technical reports that can be referred to for information on biometrics in identity proofing. Examples include:

- ISO/IEC TR 29196: Guidance for biometric enrolment [i.108].
- ISO/IEC TR 29194: Guide on designing accessible and inclusive biometric systems [i.109].
- ISO/IEC TR 29156: Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics [i.110].
- ISO/IEC TR 30125: Biometrics used with mobile devices [i.111].
- ISO/IEC TR 29144: The use of biometric technology in commercial identity management applications and processes [i.112].
- TRs on cross jurisdictional and societal aspects with implementation of biometric technologies, e.g. biometrics and children and biometrics and elderly people.

A.5 CEN/TC224 Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment

CEN/TC224 co-operates with ETSI/ESI on standards for trust services and digital signatures. The committee in CEN additionally has several standards that are relevant to identity proofing.

The CEN TS 15480 series of standards [i.135] specify European citizen card. The standard is important to identity proofing to the extent that it is used by European countries in their issuing of identity cards. Primarily, this will apply to physical characteristics of identity cards and identity proofing using manual control or optical scanning. For cards that include a contactless chip, the ICAO 9303 specifications and communication according to ISO/IEC 14443-1 [i.91] are the relevant specifications.

Work is ongoing for the CEN TS 17489 series of standards [i.113] that will cover secure and interoperable European breeder documents. Given the current draft status of these standards, they cannot formally be referred by ETSI/ESI but their relevance to identity proofing is clear. The types of breeder documents that are in scope are birth certificates, marriage and partnership certificates, and death certificates. The breeder documents management processes include first-time application, later-in-life registration of an identity, and content update (e.g. name-changing), meaning registration, issuance, renewal, inspection/verification, and revocation. Representations of a breeder document can be physical and logical/digital, including paper-based, hardware-based, or server-based. The document should be linked to its legitimate holder. A specific purpose of the standards is to specify how citizens retain the control of breeder document data and how they can use them to support identity proofing and verification.

An important standard is ETSI EN 301 549 [i.114], "Accessibility requirements for ICT products and services", which is aimed to support the EU accessibility Directive (EU) 2016/2102 on accessibility of the websites and mobile applications of public sector bodies. The standard is based on the W3C Web Content Accessibility Guidelines (WCAG) 2.1. Identity proofing should be available to people with disabilities, meaning this standard is relevant.

The biometrics standards developed by CEN/TC224 are primarily related to automated border control. They are as such not directly relevant to identity proofing, but they may contain useful information to an identity proofing product/service provider on best practices in biometrics.

Annex B:
Vendors Questionnaire

B.1 Contributors

ESI/ETSI STF 588 received feedback from the following companies:

- SK ID Solutions AS, Estonia www.skidsolutions.eu
- Yubico, Sweden https://www.yubico.com
- iProov, United Kingdom https://www.iproov.com/
- Signicat AS, Norway https://signicat.com
- InnoValor, Netherlands www.readid.com and www.innovalor.nl
- Onfido, United Kingdom https://onfido.com
- IDnow GmbH, Germany https://www.idnow.io/
- Digidentity B.V.Netherlands https://www.digidentity.eu/en

B.2 Q&A

Questions	***KEY MESSAGES OF RESPONDENTS***	***Comments***
What identity proofing technologies are provided or used by your organization's products? (Please select one or more and provide a brief explanation)?	• *3 out of 8: Physical appearance with document verification* • *7 out of 8: Remote document reading by reading NFC chip in documents* • *4 out of 8: Use of existing eIDs* • *7 out of 8: Use of electronic signatures and/or PKI certificates* • *6 out of 8: Biometrics* • *2 out of 8: Remote WebAuthn registration* • *4 out of 8: Remote document reading by optical scanning* • *2 out of 8: Video interview*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
How are identity attributes typically collected and/or verified? (Please select one or more and provide a brief explanation)?	• *8 out of 8: From identity documents* • *6 out of 8: From the user:* – *Onfido verifies users' identities online with a 2-factor approach: legal identity, face biometrics* • *6 out of 8: From existing customer records of service providers (e.g. banks)* • *5 out of 8: From government or other registers* • *6 out of 8: From eIDs or PKI certificates* • *3 out of 8: From other trusted data sources (please specify):* – *By the WebAuthn Relying Party during the registration process* – *WebAuthn credentials are enrolled from a Relying Party* – *We ask user to enter data which we verify using ID, Chamber of Commerce, PKI certificates*	
What challenges do your organization believe are most important in the identity proofing area? (Please select one or more and provide a brief explanation)?	• *1 out of 8: State of standardization* • *7 out of 8: Regulations* • *1 out of 8: Cultural differences for traditional identity management in Member States* • *2 out of 8: Technical* • *5 out of 8: Scaling to volume of users* • *8 out of 8: Trust/Security* • *6 out of 8: State of standardization* • *1 out of 8: Reduce travelling by providing secure remote identification processes* • *8 out of 8: User Friendliness* • *3 out of 8: Conversion Rate* • *2 out of 8: Price* • *1 out of 8: No identity proofing performance minimum threshold* • *1 out of 8: No identity proofing standards across verticals and use cases* • *1 out of 8: Accurate data extraction* • *1 out of 8: Low False Acceptance Rate and False Rejection Rate*	
Which application areas are you targeting with your product? (Please select one or more and provide a brief explanation)?	• *8 out of 8: Financial Services* • *8 out of 8: Trust Services* • *6 out of 8: Health* • *4 out of 8: eCommerce* • *5 out of 8: Insurance Products; ecommerce* • *3 out of 8: Travel/Hospitality* • *1 out of 8: Issuing of eID, especially mobile app-based eID* • *3 out of 8: Age Verification;* • *3 out of 8: Mobility/Drivers Licenses* • *2 out of 8: Gaming/Gambling* • *1 out of 8: Government*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
In which countries are your offering your services? Do you have official permission for each country?	• *2 out of 8: Estonia* • *Latvia* • *Lithuania* • *3 out of 8: USA* • *2 out of 8: Sweden* • *3 out of 8: UK* • *3 out of 8: Netherlands* • *Poland* • *South Africa* • *Singapore* • *Norwa* • *Denmark* • *Finland* • *Germany* • *Belgium*	
Do you have any opinions on applicability of various technologies for certain application areas, e.g. which identity proofing technologies that could be sufficient to achieve a certain level of assurance of an identity? What pre-requisites should be stated for a technology to be applicable, e.g. security, competence of personnel, documents accepted etc.? Please describe for each application area and/or country from above.	• *This should not be technology question - these assurance levels must be well described to state the not acceptable and acceptable risks for each level. It would be then up to each service provider to prove their service conformance to the expected levels and it is normally a set of technologies and organizational measures that make up a secure enough system. The worst thing at the moment is security level of "physical presence" that is referred but nowhere explained or described to make comparison - such "cultural heritage" points should be eliminated to allow technical innovation without losing trustworthiness.* • *Yubico does not offer identification services per se, but rely upon third-party identification services. In the US, we work with identity proofing companies that comply with NIST 800-63-3 [i.36] aligned identity proofing. In Sweden and the rest of the EU we rely upon QTSPs that comply with the ETSI standard ETSI EN 319 411-1 [i.10].* • *In the USA, the identity proofing system should adhere to the NIST 800-63-3 [i.36] guidelines. In Sweden and the rest of the EU, the identity proofing for issuing certificates should follow the ETSI standard ETSI EN 319 411-1 [i.10].* • *For identity proofing using biometrics, it is imperative to use technologies that can detect human presence and real-time authentication. If this is condition is not met, the assurance level in authentication is low, as there is little protection against a range of digital attacks. When using documents for identity proofing, documents with NFC chips are the most secure and tamper resistant, therefore provide high assurance level.* • *Reading of information from NFC chip combined with face biometrics should be applicable for anything (except issuing of passports and national ID cards). Video interview seems to be generally accepted as a substitute for personal appearance. Optical reading of identity card plus plus biometrics is less reliable but perhaps can fulfil "substantial"? Then, all depends on "doing it properly", according to best practice policy and security. This applies to physical appearance as well, which can be anything from a passport office with highly skilled personnel to a visit to a post office with a newly employed clerk and showing only a driving license.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
	• *Remote identity proofing is the way to go, particularly given Covid19 challenges. Identity document verification and identity document holder verification are key. Using NFC, this will be far more reliable than current physical or video-based identity proofing solutions. Assurance level eIDAS high is realistic for NFC-based identity document verification. Holder verification based on biometrics is more challenging in terms of assurance levels due to lack of standards/guidelines/certifications. Application areas are mainly eID solutions and (Q)TSP.* • *With our two-factor verification method, and applying machine learning algorithms, is possible to achieve great robustness, corresponding to a substantial/high-level of assurance. The minimum bar/threshold should be higher than identity record, as it is currently used in some Member States.* • *"Maintaining high security standards is important and must be a prerequisite for any identity application. While certain IDV procedures pose less risk than others (i.e. car rental or age verification vs. an IDV/KYC for bank account opening), the security, competence of personnel, and type of documents accepted ought to have regulations and measures to support each IDV purpose. A one-shoe-fits-all product that is effective for lower risk applications should not be accepted for IDV where security requirements are high. This is not feasible and leaves the market open to attack and major security breaches. There are significant differences between a system that accepts static imagery for face comparison or security feature checks vs. a system with dynamic security feature checks and dynamic face comparison/liveness checks.* • *A solution that relies on the best competences of both an agent and the efficiency of machine learning and AI to its system, can offer a higher quality of trust to meet robust security requirements. Our hybrid product, AutoIdent Level 4, utilizes facial recognition technology that is supported by key features. These include AI for biometric checks, liveness detections, and security feature checks by using dynamic streaming for these processes and it is followed with an agent or what we refer to as a manual review. These features have made us a technology leader for the last 6 years, and experts in fraud detection. Our technology is based on facial recognition comparison technology, which scans the characteristics in the user's face to compare it to a picture on the ID-card or passport. Our facial recognition matching is able to determine whether two images actually are the same person. It has an accuracy rate over 99,7 %.* • *Liveness detection provides a significant advantage in preventing spoofing attacks, identifying whether the user in front of the camera is a real person, and detecting manipulations to the images and video stream. The hybrid solution is based on dynamic image processing rather than static images. This provides an enormous security advantage compared to traditional photo technology that has thus far been the staple of the market. With "video" technology, the security checks are based not on a single image, but on several hundred images for each identification.* • *Furthermore, if the algorithms of our AutoIdent product deliver values that fall short of or exceed the defined threshold values for a positive or negative identification result, a manual check of the data collected in the identification process is performed. Other identity solution providers who rely on a selfie or biometric test without added security features run the risk of missing more sophisticated system manipulations."* • *NFC for ID verification only option for High/Level 4 (but also used for lower levels), video identification only for Substantial/L3 but has risk for manipulation and my opinion is that video is not user friendly, not secure. Only governmental ID with nationality should be accepted (will rule out drivers' license) but not all countries have trusted issuing process for passports, so more evidence of identity is required.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
How are your products offered? Please select one or more:	• *2 out of 8: Software for on-premises installation* • *3 out of 8: Software for in-device installation* • *8 out of 8: Cloud services* • *IDaaS (identity as a service) for our customers but also sell and distribute related service components* • *In many cases in combination with mobile apps* • *SDKs for input capture and a single API for processing/results* • *Digidentity App on mobile phone with virtual smart card with identity* • *3 out of 8: Hardware components* • *1 out of 8: Manual processes (e.g. for document inspection)* • *Some methods require (video interview) or may use (remote document reading/biometrics where the result is not clear yes/no from automated processing)* • *1 out of 8: Mobile app for NFC* • *scanning and cloud server for processing of scanned data. Similar for the biometrics part*	
What standards are used or referred to for your products (international, national, industry standards)? Please specify application area and/or country, if necessary.	• *ETSI EN 319 401 [i.9], and direct eiDAS together with secondary acts and local implementation acts. Nothing exists for identity proofing* • *FIDO2 (WebAuthn)* • *FIDO U2F* • *PIV* • *NIST Special Publication 800-73 [i.14]* • *OpenPGP* • *OATH-HOTP (IETF RFC 4226 [i.115])* • *OATH-TOTP (IETF RFC 6238 [i.121])* • *NIST FIPS 140-2 [i.7]* • *NIST 800-63 (US, global) (multipart [i.43], [i.44], [i.45])* • *ISO/IEC 17025 [i.116] standard* • *Apple's MFi certification [i.128]* • *ISO/IEC 27001 [i.24]:* • *ISO/IEC 19795-1 [i.117]:2006 for testing biometric verification performance* • *ISO/IEC 30107-3 [i.118]:2017 for testing presentation attack detection* • *NFC reading: ICAO 9303 [i.87] specifications for eMRTD* • *Optical reading: Checks against document standards, e.g. ICAO for passport, European identity card specs, etc. and national specifications for document content, layout and security elements;* • *Biometrics: ISO standard for attack vectors, etc.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
What procedures or mechanisms are most important to cover by standardization in identity proofing? Please select one or more and provide a brief explanation:	• *8 out of 8: Required level of assurance/security* • *2 out of 8: Security requirements for services or products and their environments* • *5 out of 8: Procedures for document validation* • *5 out of 8: Technologies for document validation* • *4 out of 8: Procedures for capture of biometric sample (e.g. process for selfie picture)* • *3 out of 8: Technologies for capture of biometric sample (e.g. selfie picture)* • *5 out of 8: Security requirements for services or products and their environments* • *3 out of 8: User interaction and interfacing* • *3 out of 8: Biometric technologies* • *liveness detection or Presentation Attack Detection* • *1 out of 8: User interaction and interfacing* • *1 out of 8: Competence requirements for document validation;Security requirements for services or products and their environments* • *1 out of 8: Communications security and cryptography*	*An identity proofing standard should set the bar, that is, define the levels of performance plus security requirements. That's it. It shouldn't define anything else and leave to the market to come up with best technologies, best user experience, best processes, best competences.*
In your opinion, what are the most pressing needs for further standardization?	• *Allow cross-sectoral (telco, financial, gambling, trust services etc) and cross-country conformity of identity proofs with single conformity claim per service.* • *Remote identification proofing for QTSP CAs that issue Qualified Certificates to individual QSCDs. The remote identification process should provide the equivalent security as physical identification.* • *Most important is to improve and clarify the requirements and processes for remote identity proofing. In particular, it should be clarified how the passport information can be matched to a national ID-register and how the ID photo can be matched against a photo taken by a web camera.* • *Testing of biometric authentication technologies to cover a range of attacks is yet to be standardized. There are very few testing labs, who test only for presentation attacks. This leads to products which are supposedly tested, but are actually vulnerable to digital attacks, flooding the market. Testing requirements and processes need to be standardized and stringent. The buyers can then make an informed choice about the best product for their need.* • *With referral to previous answer, the "how to do it right" best practices. Technology standardization is important but can be done in other contexts (e.g. biometrics). Best practices - policy and security - should to a large extent be applicable across technologies, referring to use of state-of-the-art technology that protects against identified threats to a sufficient level.* • *Assurance levels for biometric solutions.* • *Build up a standard that:* – *it's independent from eIDAS (that is, the eID layer becomes a separate layer to which eIDAS refer to)* – *it is output/performance/level of assurances centred, like, largely, the NIST 800-63 (multipart [i.43], [i.44] and [i.45])* – *it does not limit the market/players by any other means (approaches, technologies, processes, competences, etc.), that is, that fully foster a healthy competitive market* – *it sets the minimum bar high in terms of security and Fraud (max acceptable False Acceptance Rate is very low)* – *it's a must for all regulators in all verticals/use cases to be adopted, in all EU 27 countries* – *that's business and users friendly*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
	• *Standards establish universally reliable quality measures, and best practices in the identity proofing process and establish the format, credentials, and authentication protocols that are needed for interoperability. Standards are critical at all stages of identity verification and authentication.* • *Presently, standards used for identification systems lack uniformity; in particular for levels of assurance, how products ought to be tested, or how to meet these requirements. There are vendors that claim their products are secure enough to be trusted for various IDV requirements, but they are not able to meet higher security standards. The effectiveness of an interconnected and interoperable identity process cannot be trusted without standards.* • *Technologies used for specific levels of assurance*	
Do you provide products that are approved for identity proofing according to national regulations in any country and for any purpose (e.g. for KYC, for issuing of eID at a defined assurance level, or for issuing of (qualified) certificates)? If affirmative, can you provide examples?	• *We use national eID's with qualified signing capability to onboard customers to other eID schemes. The problem is that we need to read through their CP and CPS to understand if the have the issuance against "physical presence" for all these certificates and that makes no sense. Please create a qc statement finally that would indicate this as it is important feature based on eIDAS!* • *One contributor does not offer identity proofing products or any identity proofing products.* • *iProov powered solutions conform to ETSI EN 319 401 [i.9], which has been certified by independent auditors including TÜV Informationstechnik GmbH for conformance to eIDAS Clause 24 1(d), and confirmed by the Government of Estonia. These solutions are used to renew national digital ids in Estonia. We are used to complete KYC processes by banks in Netherlands.* • *Yes, various eIDAS approved qualified TSP's make use of our identity proofing services, various eIDAS notified eID providers make use of our services (at level substantial and high), financial institutions make use of our product for KYC purposes, governments use our product for re-identification of residents. Examples: https://readid.com/blog/NFC-replace-physical (eIDAS QTSP); https://readid.com/blog/NFC-based-identity-verification-empowers-worlds-most-successful-Remote-Identity-Verification-Immigration-Programme (UK Home Office 'brexit' app); https://readid.com/cases/Digidentity (eIDAS eID provider for UK).* • *We support clients across multiple geos (EU27, UK, US, India, SE Asia, etc.) to comply with their respective vertical regulations, namely in financial, gaming, healthcare, etc.* • *Our products are approved for identity proofing according to natinal regulations throughout EU and the EMEA region for KYC, issuing identifications with the eID in Germany, and for issuing QES with a TSP partner. The defined assurance level for issuing certified certificates is at substantial.* • *Yes, we deliver eID Substantial/High in Netherland, eID Substantial in UK, issue qualified certificates for digital signatures.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
Which application areas are most important for use of your products (e.g. KYC in various industries, eID issuing, trust services)?	• *Our service is used for KYC, AML, health records access, age verification and many more.* • *Enterprise authentication solutions, banking and finance, remote authentication (VPN type solutions), and federal eID systems in the US and the EU.* • *Enterprise authentication, remote authentication VPN solutions, eID issuing, and trust services.* • *Any area that requires the authenticating or relying party to ensure that the person authenticating for the service is genuine human and is present at the time of authentication, iProov services are most important to use. This includes KYC, eID issuing, trust services, onboarding and authentication.* • *Signicat's main customer base is the financial sector (banking, insurance, debt collection and more) where KYC is the primary purpose. We have customers that use our identity proofing services to issue eIDs, targeting "substantial", although none are yet formally audited/notified to a specific LoA. No use for trust services at present but in scope in conjunction with going directly from identity proofing to a (qualified or advanced) signature by the proved identity or in conjunction with eID.* • *eID issuing, trust services, KYC, onboarding of customers in finance, police enforcement, attestation de vita for insurance companies.* • *The key use cases we support are: eKYC, right to access your healthcare records, right to drive, age verification, etc.* • *KYC and QES with trust services* • *eID issuing, remote signing*	
How do you handle privacy regulations (e.g. GDPR) and privacy concerns related to identity proofing?	• *That is listed in the personal data protection claim and terms and conditions for the service, but as a rule although we collect a lot of personal data we avoid any kind of customer profiling and therefore we are not also useful as KYC claim generator, but only enable users to securely sign their own claims.* • *Yubico does not offer identity proofing products per se, but the identity proofing companies we cooperate with comply with GDPR. Yubico does not offer any identity proofing products, so GDPR is not an issue.* • *iProov complies with GDPR (regulation (EU) 2016/679 [i.6]), and as such, all biometric images can only be used under agreed and specific terms:* – *User authentication* – *Fraud detection* – *Maintenance of these methods* • *Signicat always operates "on behalf of" the customer (e.g. a bank) according to a data processing agreement. The customer is always the data controller. We do some verification that the customer is within regulations but overall the customer is responsible while we ensure that our processing is within GDPR and national rules. Means also that all personal information is per customer and never shared across different customers.* • *ReadID InnoValor is a data processor under GDPR, we process the data for our customers that are responsible (banks, governments, TSPs, eID providers, etc.). So privacy is their responsibility.* • We are GDPR compliant. We have a public privacy policy. We are in constant engagement with the *Information Commissioner's Office* in the UK. We are developing unbiased machine learning algorithms. • *We adhere to national and international privacy regulations as well as EU level regulations like GDPR.* • *We only store and use verified personal data which are required to provide the service requested. We also applied for GDPR certification which is currently being assessed.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
Vendors must adhere to variations in national laws, centralized directives, and market acceptance. What obstacles influence your marketability and the opportunity to introduce new solutions in the market?	• *Mostly that financial and trust services are regulated differently from ground up (directive vs regulation). No common responsible body in member states and no mechanism to enforce any of the good intentions of EU against local protectionism* • *As regards to identity proofing, clear standards and regulations on remote identity vertification is of importance for online enrollment of X.509 certificates and FIDO credentials. (Footnote: FIDO2 should be recognized by ENISA as eIDAS eID scheme with level of assurance high. We in FIDO Alliance have a discussion with ENISA about this.)* • *The eIDAS regulation should be streamlined and clarified so all EU member states can implement remote identity proofing solutions with the same level of requirements. At the moment, there are different interpretations and requirements in various countries. The corresponding ETSI standards need to reflect the legal requirements in the eIDAS regulation.* • *Negative perceptions around use of facial verification, because it has been confused with facial recognition, which is primarily used in surveillance.* • *Regulatory requirements, which mandate the use of video calls for secure authentication. iProov products are designed to reduce effort, increase adoption and leverage cutting edge technology. Video calls with trusted agents are insecure, insert effort and lower adoption rates."* • *National rules do seldom exist, meaning there may be a cumbersome and uncertain process to have a new solution accepted as being within national regulation (e.g. approval by a supervisory body). Authorities tend to be far too conservative and rely far too much on exaggerated belief in physical appearance as the most secure way. Authoritative sources for personal information are available only in a few countries (e.g. population registers).* • *Not so long ago Apple mobile phones did not support NFC; now that has changed and opened the market for us. We scan ID-documents; sometimes we need to consult databases of stolen/lost ID-documents. On a national level this is doable; on a EU level this is less trivial as databases such as Interpol are not accessible for private companies like InnoValor. We would appreciate it if such databases will offer their services to ID proofing organizations. The lack of such open interfaces undermines the whole international QTSP/eID market.* • *"Restrictive requirements in some Member States require businesses to do identification via a synchronous video call. This method is outdated and prone to fraud.* • *Secondly, regulations currently mainly apply to eKYC standards and largely leave out other sectors. Regulators in all sectors should be made aware of the benefits of digital identity verification and ensure that standards are implemented appropriately to facilitate the uptake of digital identity solutions in all verticals."* • *A lack of regulatory harmonisation does influence a vendor's marketability. The greater issue here is the lack of harmonisation when it comes to establishing higher security standards for a product to meet. To establish a more level playing field establishing a minimum security threshold i.e the eIDAS LoA should be harmonised across borders. It would be important to provide a level playing field as vendors with lower security standards offer lower prices, distorting the market and threaten overall trust in the market.* • *Different interpretations of eIDAS within European Supervisory bodies. Different supervisory policy between eID and Trust Services*	
Do you provide identity proofing of a natural person representing a	• *5 No, but we use local business registries for that purpose a lot* • *1 N/A* • *2 Yes*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
legal person? If affirmative, how is this done - sources for verified authorizations etc.?	– *by verifying identity of natural person and then verifying against the appropriate business register that the person has a designated role (e.g. signing rights). Business registers are mainly national, often requiring a national ID number for the role lookup, e.g. in the Nordics. Roles apart from those defined in the specific business register are not currently supported but in some countries other authoritative sources may exist.* – *By verify legal representation using Chamber of Commerce or required authorization from legal representative (as defined in ETSI EN 319 411-1 [i.10] and ETSI EN 319 411-2 [i.11]). Legal representative or authorized representative is identified as natural person.*	
Do you provide identity proofing or verification for legal persons? In case, how is this done - sources for verified information etc.?	• *2 Yes* – *By verifying legal representation using Chamber of Commerce or required authorization from legal representative (as defined in ETSI EN 319 411-1 [i.10] and ETSI EN 319 411-2 [i.11])* – *Through issuance of e-seals* • *5 No* – *Verification for AML purposes (beneficial owners, sanction lists etc.) is under development. Identity proofing would be of a natural person representing the legal person authorized to carry out the action leading to a check/verification for the legal person as such.* • *1 N/A*	
In your opinion, to what extent is unique and persistent identification of a person (natural or legal) a requirement? What information should be provided as a minimum for identification?	• *The bare minimum required is information based on what you are able to find someone in a physical world and take legal action against them if it becomes necessary. This information differs from member state to another and one person may have several of such identities, but within EU we should aim for the chance that we are able to turn to a specific law enforcement in a specific MS to get our rights enforced."* • *The minimum requirement for identification is a valid ID-document (such as a passport) and a comparison of the ID photo with the person's face. The identification does not necessarily have to persistent, since a person may change name, sex or physical attributes.* • *Minimum information for identification is an ID document (e.g. a passport) and face recognition. Persistent identification of a person might be difficult to sustain, since the person may change name, physical attributes or even gender.* • *This depends on context. In some cases, identification does not have to be unique, e.g. proving name and date of birth is enough. But in general all persons should be uniquely identified both within their nation(s) and linked across nations where needed (e.g. to verify that the person with a given Norwegian national ID number is the same as a person with a Polish national ID number). In theory, the minimum for unique identification should be a unique number coupled to stored biometrics; all other attributes are additional information. But no nation defines identity that way.* • *Unique and persistent identification is of utmost importance; particularly on eIDAS level high. A persistent identifier in combination with some minimum set of attributes (based on eIDAS) is required. The attributes are needed for identity linking/matching as not all relying parties will (be able) to make use of the persistent identifier or will use another persistent identifier.* • *The digital identity should be linked to an individual legal identity as a minimum bar for a robust online identity verification.* • *A valid and official ID* • *Security Feature Check* • *Real time identification* • *Ability to verify Live Person (Liveness detection)*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
	• *Biometric face comparison* • *System that is able to produce a face to face equivalent IDV* • *If we want the eID to replace phyical ID than we must verify the identity the person uniquely. Full name, DoB, place of birth, nationality, social security number.*	
How do you see use of self-sovereign identity affecting the identity proofing area - identity proofing for SSI and use of SSI for identity proofing?	• *Hype of enthusiasts and nowhere on a horizon is there a viable business case (specially now when UK is out of EU). SSI is a replacement for eID and public data services where there is none available for whatever reason - if there is a proven eID and public data services that can be accessed by individuals and services without a hassle then for meaningful interactions SSI will not be used. That said if someone in EU continues to spend tax money for creating SSI's then please negotiate Twitter® and Facebook® and Google® and Apple® access with them - this is on the right level of assurance then.* • *Self-sovereign identity solutions can be beneficial for systems with lower requirements on authentication (eID AoL low/substantial) or Advanced Electronic Signatures. For eID AoL high or Qualified Electronic Signatures, self-sovereign identity solutions will typically not meet the requirements.* • *Self-sovereign identity solutions have the benefit of being simple and user-friendly, although the identity proofing for SSI does not provide the sufficient level of identification. Typically, SSI solutions meet eID assurance level low or substantial. SSI could be used for enterprise solutions or simple eCommerce applications.* • *Advanced decentralized identity technology platforms enable organizations and governments to issue, accept, and verify credentials with individuals that serve as digital proofs of one's identity. This technology gives people total control over their identity and personal data, while providing the freedom of being able to take and use these credentials anywhere, and allowing organizations to deliver more seamless and secure experiences for their users.* • *On-boarding onto a SSI platform and subsequently binding users to their devices on which the credentials are stored, are key vulnerability points, which require high level of assurance in the identity and genuine presence of the remote user. Server based biometric authentication is the key to make this secure and successful.* • *Use of SSI for identity proofing is in principle the same as using a "normal" eID and other authoritative sources of identity information; you have to determine the level of trust in the SSI and the information it provides. Identity proofing for SSI is in principle the same as identity proofing for other purposes; the identity and associated information must be proven to a required assurance level, and the information must be associated with the SSI at the same level.* • *Not for identity proofing in the context of eID's or QTSP's. SSI will useful for secondary services offered by e.g. banks or ecommerce parties that need personal information of the user.* • *We believe that the next evolution in the identity proofing space is a self-sovereign, decentralised, user-owned, reusable identity. While this is a newer area of discussion, the idea of a decentralized system where users control their own identity is valuable. A secure and relaiable IDV must be ensured at the beginning of such ID ownership. We do see high potential in this area. All approaches thus far have not shown user adoption or traction.* • *SSI is the future but to be able to trust SSI, the identity must be verified by a trusted party.*	
From your point of view: What has so far prevented SSI from	• *Self-sovereign identity solutions lack the trustworthiness that is needed for governmental or banking security IT-systems. One way to increase the reliability of self-sovereign identity could be to rely upon eID AoL high credentials for issuance of the SSI credentials.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
becoming successful? How could this be changed? Why should it be changed? Not every technically interesting solution is meant to be successful.	• *SSI does not provide the trustworthiness that is needed for high-end systems such as governmental or banking services with high security requirements. One way to improve the use of SSI could be to rely upon authentication with an eID scheme at assurance level high, which is used for issuing the secondary SSI credentials.* • *Lack of user friendliness and complexity. People cannot manage passwords, they cannot be expected to manage their own identity information the way current SSI solutions require. A part of this is that the risk of loss of information is too big, e.g. losing the "identity wallet" or the access to it. We are working on a concept called "identity custodian" meaning a trusted actor that can provide "SSI with a recovery possibility".* • *No real use cases. Not trivial to give user control over his/her personal data.* • *The lack of standards and the lack of support from governments and regulators has greatly prevented a self-sovereign identity scheme to emerge.* • *"It is still relatively new and in practice still requires further development with regard to security and confidentiality of personal information. Existing identity systems rely on a centralized system to ensure that each unique identifier is linked to a singal identity. A good start would be further clarification on inclusion and access, as well as measures to ensure its use for both public and private industry services and applications.* • *Lack of trust. Difficult to set up SSI.*	
How do you see the future role of the GAFAs (Google®, Apple®, Facebook®, Amazon®) in identity proofing?	• *They are going to be there, but not as proofs of identity but proofs of matching to the expected profile. In the context of these companies the real physical parameters of the person do not matter much.* • *Since GAFA provide authentication services as well as federated web-SSO solutions such as OpenID-Connect and SAML v2, and they have billions of end-users, their contribution to the standardization and development of (remote) identity proofing will be extremely important. (Microsoft should be added to the list of tech giants as well.)* • *GAFA play a very important role in the identification and authentication sphere, and they also provide web-SSO protocols such as OpenID-Connect and SAML v2. It is therefor important that GAFA adhere to and implement the (upcoming) standard on identity proofing. (Microsoft should also be part of this group of tech giants.)* • *"Single digital identity will be become increasingly common. Serious industry players will start to emerge with credible, scaled offerings that allow consumers to create one digital identity for use in many different contexts and situations, from healthcare to car hire. The result for the consumer will be infinitely enhanced convenience, coupled with greater control of their own identity security.* • *Suppliers in this new market will likely come from different sources. Some will be national governments, others will be major commercial organizations.* • *They will have at least one thing in common; a compelling reason for consumers to sign up and create a single identity in the first place. GAFAs have a strong incentive to play in this sector."* • *One role is as sources of auxiliary information that can add evidence to identity proofing (e.g. information from a Facebook® profile). Another role is that the actors may develop identity proofing solutions/services that they use for their own purposes, while also selling/providing verified identities to other actors. The main limitation to them is the fact that official, national identity is often needed, where they have to adhere to national regulations like any other actor.* • *Not. Too US-based, continuity of id-proofing unclear (they may decided e to stop with it), big-brother aspects, not enough identity assurance.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
	• *Weak versions of digital identity have been already adopted on a wide-spread basis by citizens across the globe, including through GAFA platforms with well known examples of abuse. The standard of identity verification used by these platforms is insufficient and prone to fraud. Rather than giving away digital identity to non-EU players, the EU should provide a strong alternative to European consumers. This underlines why there is a strong need for an EU-wide framework supported by all EU27 governments, adopted across all verticals and all use cases.* • *Any company must be willing to uphold privacy and standards that ensure high quality and secure identification procedures. As a European company, it is important that the EU maintains control over its citizens' identities and does not hand it over to foreign companies. The principles of the GDPR must be upheld.* • *No, their business model does not provide trust.*	
If you are working with physical documents: How do you ensure that the document has not been forged? What is the highest quality level of a forged document that you are able to detect? *If you are working with face comparison: How do you compare the face? How do you prevent presentation attacks (e.g. using liveness detection)?*	• *I cannot see the relevance of the answer - we have seen a lot of them and with good quality, but what does it help. Now with NFC reading capability hopefully we will make a step further in that area. We do use external partners who handle the technical part of that, but as a requirement we of course need that and check that it is actually well done* • *I do not have a strong opinion since I am not an expert on physical documents. I do not have a strong opinion since I am not an expert on face comparison.* • *I do not have a strong opinion, since I am not an expert in this field. I do not have a strong opinion, since I am not an expert in this field.* • *iProov product uses face-matching as the basis for a biometric verification, and protects it with unique methods of forgery detection including presentation attacks and replay attacks. Together, these methods create a "one-time biometric".* • *At the time of authentication, the iProov servers send to the user's device a unique code which is used by iProov software on the device to create the 'Flashmark': a colour sequence of flashes determined by the code. The coloured light from the screen reflects from the user's face. A video streaming application in the iProov software streams a short video back to iProov's servers, which is analysed in realtime to assure genuine presence."* • *For NFC reading, checking that the information is really read out from a document (using a trusted app that has not been tampered with) and checking signature on the information. For optical reading, best effort using both configuration and machine learning to recognize security elements and other characteristics of a genuine document. Reliability for optical reading depends on the number of documents treated (for learning), meaning reliability is higher for frequently used documents than for documents that are rarely seen.* • *A video sequence is required with analysis of liveness. Real time commands (turn head right/left etc.) can be used. Presentation attacks, e.g. according to ISO standard, must be considered. Deep fake animation may cause problems today but is also still a very unlikely threat.* • *We read digitally signed personal data from the chip on official identity documents. We challenge the chip to check if it is not cloned.* • *Compare face from chip of identity document with selfie. Liveness is important and can be realized in various manners (challenge response mechanisms, movement detection or light flashes).*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
	• *Onfido has developed a wide set of machine learning algorithms that check both the extracted data and the visual authenticity of a document image. We also developed additional techniques related to the input capture phase that helps identify fraudulent behaviours. FInally, we are planning to integrate with government-run source-of-truth services wherever they will be offered. We use biometric analysis to match the face on the ID to the face in the photo, as well as running passive liveness checks to detect fake webcams, photo-editing software, photos of photos, photos of print-outs etc. We also offer a variant that collects a video of a user going through specific challenges proposed by our platform/machine (liveness tests).* • *Our products serve remote identification platforms. We have an extensive fraud department that continually montiors and analyses various attacks to the system from simple forgery, counterfeit, to sophisticated communication manipulation attempts on the back end system. We have counter measures for all of these attack scenarios. With these years of experience, we have incorporated what we have learned into our new generation of machine learning products that not only meet face-to-face requirements, but now can exceed traditional identification methods to tackle the rapid rise in and sophistication of cybercrime. Unlike static selfie image solutions, which are based on capturing and analysing static images, our hybrid solution is based on video technology, which provides an enormous security advantage compared to traditional photo technology that has thus far been the staple of the market. With video technology, the security checks are based not on a single image, but on several hundred images for each identification. Only by doing dynamic security feature verification, it is possible to reliably verify ID documents in a remote setting. The highest quality level of a forged document that we have been able to detect is anything below a state forged document.* • *"The biometric check uses face recognition comparison technology to scan the characteristics in a user's face to compare it to a picture on the ID card or passport.* • *To detect stolen or modified IDs, the system's 3D face recognition protects against fraud attempts, and presentation attacks. With integrated live video streaming detection works far better at capturing hundreds of images vs. a few static images."* • *We have third parties that verify ID using photo analysis or read NFC data. We should be able to detect all kinda of forged documents.* • *Yes, we use liveness detection, and a combination of face recognition and periocular recognition (area around the eyes).*	
If you are working with optical approaches: How do you see the threat of deep fakes? How do you prevent attacks using deep fakes?	• *iProov has systems to monitor and analyse attacks on our online face verification systems, which are used to set up accounts and to authenticate their use. We have seen attacks using deepfakes being attempted. They were not successful. Countering the deepfake threat is going to be a ceaseless challenge, requiring active monitoring and technical innovation. iProov has developed one method that works, but it is focused on protecting real-time communication like facial authentications, including for video calls, and continuously evolves to stay effective. Other forms of content will be difficult to protect; and there will always be the conundrum that if you tell people how a detection system works, it helps them to spoof it, and if instead you keep it secret then no one knows how to evaluate the protection and whether it even works. Protect the chain of trust that underwrites the integrity of a piece of content. That's hard, but depfake-resistant authentication is a key tool to do so.* • *Capturing the picture of the document is at least a video process where it is clear that a physical document (and not only a picture) is present. Then, configuration and machine learning is used to detect security elements and to verify that the document is (more or less likely) real. Using a trusted app instead of a web interface is strongly preferred.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
	• *At Onfido, we are exposed to a wide variety of fraud attack vectors. Deep fakes is one of them and very relevant. Our liveness test challenges are randomly generated, so this protects against pre-recorded video. On top of it, we always detect fake webcams to prevent a man-in-the-middle attack.* • *The threat of Deep fakes is evolving and increasing in sophistication and believability. To date, we have not experienced a deep fake attack to our system. We have developed our own counter measures against a potential deep fake attack. In our research lab we have successfully developed a working prototype of an actual deep fake. We see its relevance becoming mainstream in the future and are constantly refining, researching, and establishing counter measures against such attacks.*	
Are your products subject to third-party audit, conformity assessment, or certification? If affirmative, is this at national level or internationally recognized?	• *1 out of 8: Service conformity assessment* • *2 out of 8: product conformity assessment (FIPS 140-2 and NIST FIPS 140-2 certification [i.7].* • *3 out of 8: ISO/IEC 27001 [i.24]* • *1 out of 8: ETSI/eIDAS audited.* • *1 out of 8: SOC for Service Organizations: Trust Services Criteria Type II Compliant* • *2 out of 8: Yes with no details*	*We use subcontractors, many different, for all of optical reading, NFC reading, and video interview - and for face picture capture and biometrics. Many of these have national approvals that may require audits and conformity assessment. This is one reason for having many different actors, in addition to the fact that some actors are better at certain documents than others (e.g. optical reading of the home country's documents). So we aim at putting together solutions using the best suited actor(s) as subcontractors, also for compliance with national requirements. International recognition is rare or non-existing but some actors refer to audit against eIDAS requirements for eID LoA, e.g. substantial or high.*
For service providers: do you publish the security and policy requirements you adhere to and the practices you follow? What are the most important security measures in your opinion? Would you be willing to share your requirements?	• *We have a full repository of documentation https://www.skidsolutions.eu/en/repository/ but more detailed internal requirements my be shared if we do see the value in it.* • *iProov is fully audited* – *Certified to ISO/IEC 27001 [i.24]: Information Security Management System* – *Conforms with ISO/IEC 19795-1 [i.117] for testing biometric verification performance, audited by the UK National Physical Laboratory* – *Conforms with ISO/IEC 30107-3 [i.118] for testing presentation attack detection, audited by UK National Physical Laboratory* • *iProov powered solutions conform to ETSI EN 319 401 [i.9], which has been certified by independent auditors including TÜV Informationstechnik GmbH for conformance to eIDAS Clause 24 1(d), and confirmed by the Government of Estonia"*	

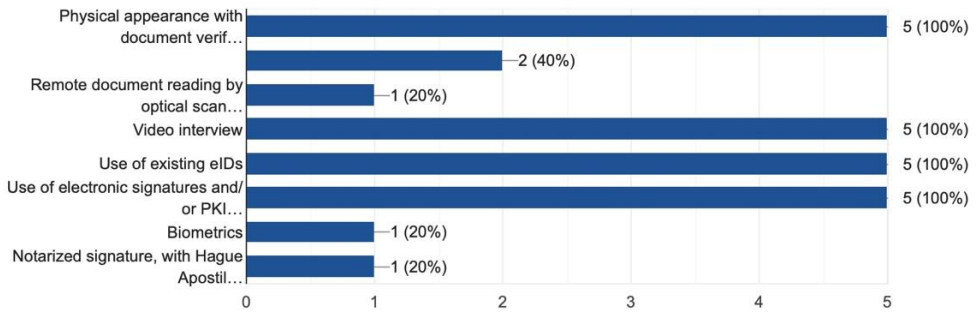
Questions	KEY MESSAGES OF RESPONDENTS	Comments
	• *Privacy statement is published. Same for overview of security and compliance. But we do not have a published policy and security requirements document for identity proofing. Practices are partly covered at the developer site but not in a comprehensive way. We are willing to share requirements.* • *In terms of security and compliance, here our public webpage. In terms of privacy, here our public privacy policy. We can also share more info re: our security practices.* • *Yes, we do publish security and policy requirements. IDnow follows best practice and uses only hardened systems - be it for OS and service configuration or supporting infrastructure like firewalls. Only necessary services and ports are allowed. The systems are patched regularly. Regular penetration tests and vulnerability scans are conducted to check effectiveness of control implementations.* • *Yes, everything documented in Certificate Practice Statement (CPS)*	
For hardware and software providers: Do you publish recommendations for secure use of your products? What are the most important security measures in your opinion?	• *Yes, Yubico provides guidelines for how to deploy and operate the YubiKey in FIPS 140-2 mode [i.7].* • *Yes, Yubico has published instructions how to deploy and operate the YubiKey in FIPS 140-2 mode [i.7]. The most important security measure is to protect the credentials in cryptographic hardware.* • *Documentation on how to use our products can be found online at https://www.idnow.io/developers/* • *Our product is secured by design. There are additional measures that can be taken like certificate pinning, mutuals TLS, custom PKIs and IPsec VPN.* • *IDnow Developer Hub - Documentation, APIs, SDKs - IDnow* • *Our APIs, SDKs and documentation help developers to get started with identity verification within minutes. Contact us to get your API key and free support from our developer support team. (7 kB)"*	
Do you follow any general security management standards in your operation? Please check all that may apply:	• *7 out of 8: ETSI EN 319 401 [i.9];* • *5 out of 8: ETSI EN 319 411-1 [i.10] and ETSI EN 319 411-2 [i.11]* • *1 out of 8: ETSI EN 319 421 [i.13] for qualified timestamp service.* • *8 out of 8: ISO/IEC 27001 [i.24]* • *1 out of 8:ISO/IEC 27002 [i.35]* • *2 out of 8:ISO/IEC 27005 [i.127]* • *2 out of 8:ISO 22301 [i.119]* • *1 out of 8: ISO/IEC 17025 [i.116]* • *3 out of 8: ITIL (ITIL (Information Technology Infrastructure Library) is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business)* • *3 out of 8: Common Criteria [i.42];* • *3 out of 8: SOC for Service Organizations: Trust Services Criteria reporting* • *1 out of 8: ISACA's Control Objectives for Information Systems and related Technology -COBIT* • *1 out of 8: NIST FIPS 140-2 [i.7],* • *1 out of 8: NIST SP 800-63C AAL 3 [i.36]* • *1 out of 8: FedRAMP High, DFARS/NIST SP 800-171 [i.12]* • *1 out of 8: Apple's MFi certification [i.128]* • *1 out of 8: FIDO2 and FIDO U2F certifications.*	
Identity verification solutions are driven by compliance requirements and existing standards in	• *Yubico is one of the contributors to the W3C WebAuthn standard, which contains a section on security considerations (https://www.w3.org/TR/webauthn/#security-considerations). We recommend our customers to adhere to these security considerations.In this standard, there is a section on security*	

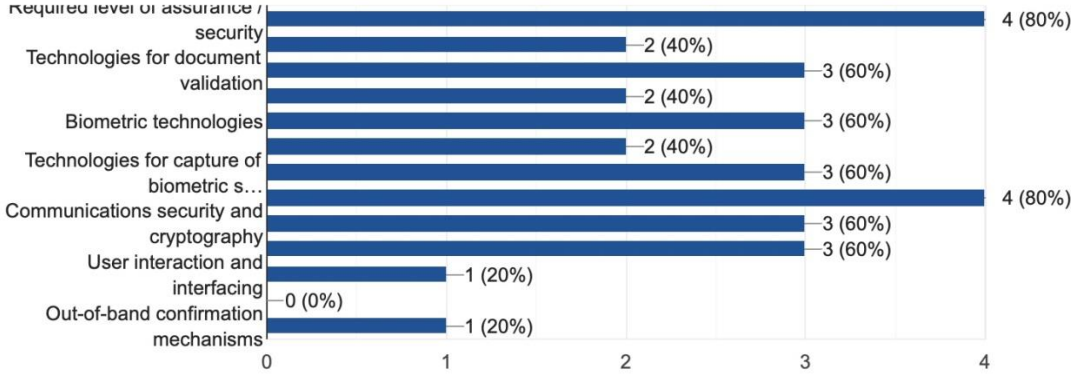
Questions	KEY MESSAGES OF RESPONDENTS	Comments
security. How does your firm ensure customers are using secure and trusted platforms?	*(https://www.w3.org/TR/webauthn/#security-considerations) that we refer to for WebAuthn Relying Party implementations.* • *Private cloud solution run according to strict requirements and ISMS certified to ISO/IEC 27001 [i.24] are the foundations. Then, other security measures and procedures up to the standard of a QTSP (ETSI EN 319 401 [i.9] and more). Several compliance audits and external checks including penetration testing. Supervision in Norway. Etc.* • *We do not trust the mobile phone and work server side.* • *We are ISO/IEC 27001 [i.24] and SOC for Service Organizations: Trust Services Criteria 2 certified. We apply state-of-the-art security best practices, as detailed in answer 32* • *We operate under universally recognized standards and regulations to provide solutions that meet some of the highest security requirements. We are able to fulfil compliance requirements for remote KYC requirements within AML regulations at national and international levels.* • *The security of our solution is not dependent on security of customers platforms.*	
What measures are in place to safeguard against potential cyber threats?	• *Service specific measures for authentication, sign, preserve, timestamp, identity proofing.* • *Certifications, pentests, screening of personnel, redundancy, logging and monitorring.* • *"At Onfido, we have established the following Roles & Responsibilities for Information Security:* • *The CTO is ultimately responsible for security.* • *The Director of Security and the security team will oversee the implementation and management of security controls.* • *The Head of Compliance is responsible for the implementation and management of the ISMS, including reporting upon its effectiveness.* • *Information Asset/ Risk Owners are responsible for identifying and classifying their information and addressing risks.* • *Managers at all levels are directly responsible for complying with our information security controls and ensuring adherence by their staff.* • *All staff including temporary workers, contractors, and where appropriate, 3rd parties are responsible for complying with our information security policies.* • *In terms of processes, we have a number of automated tools to catalog all Onfido assets such as domains, applications, software packages and other developer-related resources. The tools collect data daily and monitor for changes. The results are evaluated on a daily basis and actions taken in the event of upcoming risks.* • *We also have a framework around cybersecurity risks and incidents. It starts with a notification of the incident, followed by categorization and execution. There are a number of playbooks (checklist) which are used to ensure that all incidents are followed through consistently.* • *Cybersecurity risks are included within the corporate Risk Assessment and Risk Management process, which is owned by the Risk & Compliance team. Open risks are reported to the Executive team on a quarterly basis.* • *The process is based mostly on monitoring, awareness and education. Some of the critical software components such as machine learning models are developed in isolated environments."* • *IDnow follows best practice and uses only hardened systems - be it for OS and service configuration or supporting infrastructure like firewalls. Only necessary services and ports are allowed. The systems are patched regularly. Regular penetration tests and vulnerability scans are conducted to check effectiveness of control implementations.*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
The concept of identity proofing typically implies factors that work together to raise the level of security against fraud. What factors play the largest role in security for your organization?	• *For identity proofing, the most important factors are face recognition, comparison with an ID-document (passport), and biometric checks of fingerprints or iris.* • *To identify employees, an ID card in conjunction with an employment agreement are required. The employee will also be granted access to the IT-systems he is authorized to access. Hardware multifactor authentication is also required for access to the IT-systems.* • *For identity proofing, probably combining measures to achieve increased assurance of the result. A result from one mechanism (e.g. reading an identity document) may be enhanced by consulting another source (e.g. verifying the information against the relevant national population register).* • *The availability of international databases for lost/stolen identity documents. They are not available and therefor undermine the assurance of identity proofing. Fraud detection across multiple customers (eID providers and QTSPs).* • *Onfido verifies users' identities online with a 2-factor approach: legal identity, face biometrics. These two factors together are very robust, especially because we ask our clients and their users to capture them live on their smartphones. Doing so, we can collect multiple signals related to both the user device and the way the user connects to our SDKs that help us prevent many sophisticated fraud vector attacks.* • *The ability to produce products that are able to meet higher levels of security.* • *Keeping up to date with latest development in fraud and cybercrime to be able to update the security in our organization and products.*	
How would a strategy focusing on providing 'trust and safety-first' products and services look like?	• *First and foremost, the applicable regulations (eIDAS and GDPR) must be adhered to, in conjunction with implementations according to the corresponding ETSI and CEN standards. When necessary, additional protocols for authorization, such as OpenID-Connect or SAML v2, can be implemented as well. The cloud services must be deployed according to the ENISA, ETSI and CEN guidelines, in conjunction with cybersecurity protection measures.* • *First and foremost, the eIDAS regulation and the related ETSI, CEN and ENISA publications must be adhered to. Based on this legal and standard framework, the identification proofing system can be implemented. With the identity proofing system, and related CAs or other issuance systems in place, the credentials can be issued to preferably hardware tokens. The cloud services need to be protected against cybersecurity attacks with firewalls and IDS systems. Role based models, designed for specific apps or devices, can be implemented according to the zero trust principles.* • *All measures that document trust, e.g. compliance, conformity assessment and such, plus having real top-level security in place, plus being a trustworthy company and actor. Two aspects: Both really be trustworthy, but also appear as trustworthy to convince the market. These aspects are actually to some extent independent.* • *Enforce it with legislation. ID-infrastructures should be recognized as a vital/critical infrastructure like energy and telecom.* • *At Onfido, we put at the center of our trust and safety first strategy the following elements:* – *Smooth user experience* – *Full GDPR compliance (consent collection a must)* – *Robust machine-learning powered fraud detection features* – *Manual escalation to specialized agents in case the machine points to anomalies"*	

Questions	KEY MESSAGES OF RESPONDENTS	Comments
	• *We consistently design, build, and operate products that are based on maintaining some of the highest security standards and regulations. We began building our first product to meet the German Federal Information Security Office, BSI and BaFin requirements and regulations for video identification procedures.*	
Is there any other input you would like to provide to ETSI/ESI for standardization in identity proofing?	• *Connected with eIDAS:* – *in the ENISA report [i.53] on eIDAS compliant eID solutions (https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions) does list FIDO authenticators at eID AoL low. This could be adjusted such that specific FIDO authenticators can be listed as eID AoL high. We in the FIDO Alliance have an ongoing discussion with ENISA about this.* • *Independent from Eidas. Please, build up a standard that:* – *it's independent from eIDAS (that is, the eID layer becomes a separate layer to which eIDAS refer to)* – *it is output/performance/level of assurances centered, like, largely, the NIST 800-63 (multipart [i.43], [i.44], [i.45])* – *it doesn't limit the market/players by any other means (approaches, technologies, processes, competences etc.), that is, that fully foster a healthy competitive market* – *it sets the minimum bar high in terms of security and Fraud (max acceptable False Acceptance Rate is very low)* – *it's a must for all regulators in all verticals/use cases to be adopted, in all EU 27 countries* – *that's business and users friendly"* • *Cross border interoperability is a key result we welcome. We support harmonisation in standard setting as in policy making. We believe that higher security standards will ensure the trust and confidence both the market and public require to operate efficiently and securely. We support conitual collaboration between public and private sectors.* • *In developing a Remote Identification solution, what are the risks that a physical identification would mitigate and how would remote identification impact those risks*	

Annex C:
TSP Questionnaire

Question	KEY MESSAGES OF RESPONDENTS (emphasis added)	Comments
What identity proofing technologies are provided or used by your organization's products?		*Remote document reading by video interview, eID, esigning, and physical presentation lead as top 4 identification approaches.*
Do you have any opinions on applicability of various technologies for certain application areas, e.g. which identity proofing technologies that could be sufficient to achieve a certain level of assurance of an identity? What pre-requisites should be stated for a technology to be applicable, e.g. security, competence of personnel, documents accepted etc.?	• *Following strict requirements on personnel, checks, interview script, physical security artifacts of national IDs, etc. (Reliable)* ***Liveness detection could help to scale out the process.*** • *Yes, there are several identity proofing technologies that can help to achieve the level of assurance required for trust services (qualified and not qualified****). The issue is that technology is much faster than regulation****. Therefore, we believe that the prerequisites that can be stated for a technology should concern the security requirements: these requirements should be clear and applicable for each technology that aspires to be used in identity proofing activity for trust services. Security requirements shall be prescribed by respecting the technology neutrality principle.* • *Some principles regarding the management of the personnel in such activities already provided for by ETSI standards and don't need to be extended.* • *Other prerequisites - like the list of documents accepted - shouldn't be prescribed as mandatory requirements to achieve a certain level of trust, considering that the level of trust is attributable to the process designed to achieve it and not the technology used.*	*Security requirements ought to be clearer - important to maintain technology neutrality* *NFC reading + biometric (face) verification generally viewed as eligible for higher LoA* *Liveliness detection viewed as a key robustness-enhancing factor*

Question	KEY MESSAGES OF RESPONDENTS (emphasis added)	Comments
What procedures or mechanisms are most important to cover by standardization in identity proofing?	*Top Value = "Required Level of Assurance".* 	*Biometric related processes and maintaining required level of assurance are viewed as most relevant areas for standardization efforts*
What are the most pressing needs for further standardization?	• *It is fundamental to provide common rules regarding security requirements to be fulfilled, avoiding depressing the creativity of the market players that are constantly developing new enhanced methods to carry out identity proofing. By providing these common rules, the technology neutrality principle (that is one of the most important pillars of eIDAS Regulation [i.1]) must be respected and protected. Indeed, this set of rules should be written in such a way as to be applicable to any technology without limiting the use of future and not yes developed technologies. In this context the choice of techniques that the task force will choose to draft these rules will be crucial (in such a context the GDPR accountability principle could be source of inspiration)* • *A common standard API* • *Leveling requirements across EU* • *Public EIDs*	*Harmonization of security requiremnts, technology neutrality, common standard API are all areas in need of standardization*
Vendors must adhere to variations in national laws, centralized directives, and market acceptance. What obstacles influence your marketability and the opportunity to introduce new solutions in the market?	• *The regulation concerning identification is very fragmented, in particular considering the different purposes for which the activity can be requested (e.g. for issuing of an eID, for KYC, for trust services). This fragmentation results in an obstacle, as to enter new markets it is required to be compliant with industries specific regulations that are often similar but not identical (examples: Italian regulation on SPID-issuance regarding video identification is similar but not identical to the one issued by the Italian Banking authority for AML identification, the German Regulation issued by Bundesnetzagentur concerning video identification aimed at the issuance of qualified certificates is similar but not identical to BAFIN circular 3/2017 [i.80]). In this context we would welcome a standardization concerning the security requirements (i.e. requirements that apply to all the application areas) that could certainly foster a market growth.*	*Call for greater harmonization on an EU level- eIDAS* *Fragmentation an issue for market entry* *Looking for standardization on security requirements.*
How do you see the identity proofing area in 5-10 years?	• *A lack of security and regulation standardization* • *Market Acceptance*	

Question	KEY MESSAGES OF RESPONDENTS (emphasis added)	Comments
If you are working with physical documents: How do you ensure that the document has not been forged? What is the highest quality level of a forged document that you are able to detect?	*NOTE: Most answers not directly relevant to 'binding with applicant' dimension, except for the following:* • *It depends on the process and technology used. The documents checks can be performed by a properly trained human operator or by a software using different techniques to complete the needed checks.* • *Physical document analysis is complemented with in person video call, following national regulatory requirements. Otherwise, only notarized (+ Hague Apostille) copies are accepted* • *We are "not able to guarantee 100% of document integrity"*	*Process and technology dependent* *Validity through person or software are applicable* *Agent review complements remote processes.*
If you are working with face comparison: How do you compare the face? How do you prevent presentation attacks (e.g. using liveness detection)?	• *It depends on the process and technology used. The face comparison can be performed by a human operator or by a software using a dynamic approach.* • *Live in-person interview is required. Order of questions is random, some questions are random.* • *The face is compared by a human verification:* – *1. by comparing the face with the image store into an ID document;* – *2. by using liveness detection.*	*Biometric analysis and verification based on an ID document coupled with liveliness detection generally seen as the key requirements*
The concept of identity proofing typically implies factors that work together to raise the level of security against fraud. What factors play the largest role in security for your organization?	• *Interview script with random questions, risk profiling* • *The risk analysis*	*Randomized interview script, risk profiling and analysis*

History

Document history		
V1.1.1	February 2021	Publication