ETSI TR 119 520-1 V1.1.1 (2024-04)

Electronic Signatures and Trust Infrastructures (ESI); Framework of ERDS/REM standards; Part 1: New (Q)ERDS/(Q)ERDSP standardization rationalized framework as a result of the new components brought by eIDAS2.0

Reference

DTR/ESI-0019520-1

Keywords

ERDS, QERDS, QREM, REM,
standards framework

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

The present document is part 1 of a multi-part deliverable covering the framework of ERDS/REM standards, as identified below:

Part 1: "New (Q)ERDS/(Q)ERDSP standardization rationalized framework as a result of the new components brought by eIDAS2.0";

Part 2: "Impact of emerging technologies on ERDS/REM Models".

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.

Introduction

The Regulation (EU) No 910/2014 [i.1] ("eIDAS Regulation" henceforth) entered into force in 2014 aiming to "enhance trust in electronic transactions in the internal market" (recital 2) and "creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic registered delivery services, and for interoperable e-government services across the European Union" (Recital 6). In fact the Commission "identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy" (Recital 4).

The eIDAS Regulation [i.1] relies on standardization as it provides for trust services, and in particular for Electronic Registered Delivery Services (ERDS), the option for the Commission to issue implementing acts establishing reference of standards providing presumption of conformity with the relevant requirements of the Regulation in case of compliance with referenced standards.

On June 3, 2021 the Commission adopted a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity ("eIDAS 2.0" henceforth) [i.2]. According to this proposal, publication of delegated acts by the Commission referencing standards would become mandatory for (among the others) ERDS, in line with the text in the recital 24 of eIDAS 2.0 [i.2]: "It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services". It is then needed to provide a new (Q)ERDS/(Q)ERDSP standardization rationalized framework identifying the changes to be performed in the currently existing standard framework and the new components brought by eIDAS 2.0 [i.2].

ETSI has already held a Plugtests™ event addressing REM Baseline on May 2021, service providers implemented the first REM Baseline prototypes and this provided an important feedback on REM Baseline, before the ENAP. The Plugtests™ event also confirmed the validity of the approach to ensure trust compliance and interoperability, as per eIDAS Regulation [i.1] principles.

The REM Baseline has been implemented to meet the time to market requirements and ETSI TC ESI agreed on the opportunity to extend the Baseline concept to all (Q)ERDS/(Q)ERDSP standardization rationalized framework.

The extension of the Baseline concept to the entire ERDS standard requires a harmonization and reorganization of the (Q)ERDS/(Q)ERDSP standardization rationalized framework, in an evolutionary and forward-looking perspective.

To support these requirements, considered essential to fully achieve the interoperability ambitions of eIDAS 2.0 [i.2], further reorganization work will be needed in particular with regard to (Q)ERDS/(Q)ERDSP standardization rationalized framework that can exploit all the material already produced for the REM baseline.

Additional requirements from the market can be considered during this reorganization and accommodation work.

1 Scope

The present document defines the new (Q)ERDS/(Q)ERDSP standardization rationalized framework, identifying the most relevant changes to be performed in the framework currently existing, among which: the incorporation of an ERDS HTTP-based baseline, offering similar features than REM baseline but on HTTP-based protocols; those due to the changes brought by eIDAS 2.0 [i.2] (including new components such as the EU eWallet, and the Electronic Attestations of Attributes); and those ones due to emerging technologies that might have an impact in this field.

It also contains recommendations for updating ETSI TR 119 000 [i.4] and ETSI TR 119 001 [i.5].

Finally, the present document identifies the issues that may impact in the policy and security requirements standards.

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) No 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] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

[i.3] ETSI TR 119 520-2: "Electronic Signatures and Trust Infrastructures (ESI); Framework of ERDS/REM standards; Part 2: Impact of emerging technologies on ERDS/REM Models".

[i.4] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of digital signatures and trust services; Overview".

[i.5] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.6] ETSI SR 019 050: "Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures".

[i.7] ETSI TR 119 500: "Business Driven Guidance for Trust Application Service Providers".

[i.8] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.9] ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".

[i.10] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents".

[i.11] ETSI EN 319 522-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats".

[i.12] ETSI EN 319 522-4-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings".

[i.13] ETSI EN 319 522-4-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings".

[i.14] ETSI EN 319 522-4-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings".

[i.15] ETSI TS 119 524-1: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 1: Testing conformance".

[i.16] ETSI TS 119 524-2: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 2: Test suites for interoperability testing of Electronic Registered Delivery Service Providers".

[i.17] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.18] ETSI EN 319 532-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and architecture".

[i.19] ETSI EN 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic contents".

[i.20] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats".

[i.21] ETSI EN 319 532-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles".

[i.22] ETSI TS 119 534-1: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 1: Testing conformance".

[i.23] ETSI TS 119 534-2: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 2: Test suites for interoperability testing of providers using same format and transport protocols".

[i.24] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.25] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.26] 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.27] 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.28] ISO 19626: "Processes, data elements and documents in commerce, industry and administration. Trusted communication platforms for electronic documents".

[i.29] ETSI TS 119 182-1: "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

[i.30] IETF RFC 7159: "The JavaScript Object Notation (JSON) Data Interchange Format".

[i.31] IETF RFC 7515: "JSON Web Signature (JWS)".

[i.32] ETSI EN 319 411 (all parts): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates".

[i.33] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.34] ETSI TS 119 461: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[i.35] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

Electronic Registered Delivery Service (ERDS): electronic service that makes it possible to transmit data between the sender and recipients by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations

Electronic Registered Delivery Service (ERDS) evidence: data generated within the electronic registered delivery service, which aims to prove that a certain event has occurred at a certain time

Electronic Registered Delivery Service Provider (ERDSP): trust service provider which provides electronic registered delivery service

Qualified Electronic Registered Delivery Service (QERDS): As specified in Regulation (EU) No 910/2014 [i.1].

Qualified Electronic Registered Delivery Service Provider (QERDSP): trust service provider which provides qualified electronic registered delivery services

recipient: natural or legal person to which the user content is addressed

sender: natural or legal person that submits the user content

trust service component: one part of the overall service of a TSP

3.2 Symbols

Void.

3.3 Abbreviations

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

API	Advanced Programming Interface
BDX	Business Document Exchange
CAB	Conformity Assessment Body
CSI	Common Service Interface
DNS	Directory Name Server
DNSSEC	Domain Name System Security Extensions
EAA	Electronic Attestation of Attributes
EBSI	European Blockchain Services Infrastructure
EDICG	European Digital Identity Cooperation Group

eIDAS	electronic IDentification and trust services for electronic transactions in the internal market Regulation
ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
EUDIW	European Union Digital Identity Wallet
GDPR	General Data Protection Regulation
ICT	Information & Communication Technology
JAdES	JSON Advanced Electronic Signatures
JSON	Java Script Notation Object
PDL	Permissioned Distributed Ledger
QC	Qualified Certificate
QEAA	Qualified Electronic Attestation of Attribute
QERDS	Qualified Electronic Registered Delivery Service
QERDSP	Qualified Electronic Registered Delivery Service Provider
QES	Qualified Electronic Signature
QTSP	Qualified Trust Service Provider
REM	Registered Electronic Email
SMP	Service Metadata Publishing
SSASC	Server Signing Application Service Component
TL	Trust List
TLS	Transport Layer Security
TSP	Trust Service Provider
TTP	Trusted Third Party
URI	Uniform Resource Identifier

4 (Q)ERDS/(Q)ERDSP inputs for a new rationalized standardization framework

4.1 General

The present document sets out a proposal for a new (Q)ERDS/(Q)ERDSP standardization rationalized framework harmonizing and reorganizing the existing family of Electronic Registered Delivery Services (ERDS) standards. The present document takes into account the new requirements and components defined in eIDAS 2.0 [i.2], as well as extend the REM Baseline concept to HTTP-based ERDS, aiming at reorganizing the entire framework for better accommodating the content produced for the REM Baseline.

The present document will propose a set of standards required for fully specifying the provision of Electronic Registered Delivery Services (ERDS) and Electronic Registered Mail (REM) as a result of the analysis made of:

- The new legal context brought by eIDAS 2.0 [i.2] to the European Union;
- The new components defined within eIDAS 2.0 [i.2] (like the electronic wallet, Electronic Attestations of Attributes, etc.);
- The emerging technologies and models which could impact in one way or the other the provision of ERDS and REM services (as the management of ERDS Evidence, for instance) including the work on close fields like hybrid mail systems.

In accordance with the taxonomy of specifications defined in ETSI TR 119 000 [i.4], ETSI SR 019 050 [i.6] proposed in fact the production of three types of deliverables: ETSI ENs for policy and security requirements (ETSI ENs 319 5x1), ETSI ENs for technical specifications (ETSI EN 319 5x2), and ETSI TSs for testing conformance and interoperability (ETSI TS 119 5x4). The following standards for Electronic Registered Delivery are to be reviewed and rationalized (see Table 1).

Table 1

Document	Title
ETSI TR 119 000 (V1.2.1) [i.4]	The framework for standardization of signatures: overview
ETSI TR 119 001 (V1.2.1) [i.5]	The framework for standardization of signatures; Definitions and abbreviations
ETSI SR 019 050 (V1.1.1) [i.6]	Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures
ETSI TR 119 500 (V1.1.1) [i.7]	Business Driven Guidance for Trust Application Service Providers
ETSI EN 319 521 (V1.1.1) [i.8]	Policy and security requirements for Electronic Registered Delivery Service Providers
ETSI EN 319 522-1 (V1.2.1) [i.9]	Electronic Registered Delivery Services; Part 1: Framework and Architecture
ETSI EN 319 522-2 (V1.2.1) [i.10]	Electronic Registered Delivery Services; Part 2: Semantic Contents
ETSI EN 319 522-3 (V1.2.1) [i.11]	Electronic Registered Delivery Services; Part 3:Formats
ETSI EN 319 522-4-1 (V1.2.1) [i.12]	Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings
ETSI EN 319 522-4-2 (V1.1.1) [i.13]	Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings
ETSI EN 319 522-4-3 (V1.1.1) [i.14]	Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings
ETSI TS 119 524-1 (V1.2.1) [i.15]	Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 1: Testing conformance
ETSI TS 119 524-2 (V1.2.1) [i.16]	Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 2: Test suites for interoperability testing of Electronic Registered Delivery Service Providers
ETSI EN 319 531 (V1.1.1) [i.17]	Policy and security requirements for Registered Electronic Mail Service Providers
ETSI EN 319 532-1 (V1.1.1) [i.18]	Registered Electronic Mail (REM) Services; Part 1: Framework and Architecture
ETSI EN 319 532-2 (V1.1.1) [i.19]	Registered Electronic Mail (REM) Services; Part 2: Semantic Contents
ETSI EN 319 532-3 (V1.3.1) [i.20]	Registered Electronic Mail (REM) Services; Part 3: Formats
ETSI EN 319 532-4 (V1.3.1) [i.21]	Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles
ETSI TS 119 534-1 (V1.2.1) [i.22]	Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 1: Testing conformance
ETSI TS 119 534-2 (V1.2.1) [i.23]	Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 2: Test suites for interoperability testing of providers using same format and transport protocols

4.2 Cross-border interoperability

4.2.1 Introduction

To address the need for cross-border interoperability in qualified ERDS services, as outlined in the eIDAS Regulation [i.1], it is essential to establish a concise set of technical requirements. These requirements should be minimal to facilitate adoption by various Qualified Trust Service Providers, yet comprehensive and adaptable enough to meet immediate needs and be capable of encompassing future developments.

Achieving this balance involves adopting a "baseline" approach, a term commonly used in the industry, which includes a cost-effective mode of extension. This baseline's potential for inclusivity and extensibility can be realized through the implementation of the classic "modular" method in conjunction with an innovative "non-orthogonality" principle.

The objective of the Electronic Registered Delivery Services (ERDS) baseline is to efficiently address specific questions while minimizing resource needs:

- To what extent, and with what level of effort, can the ETSI ERDS baseline accommodate additional ERDS implementations.
- Conversely, how feasibly and with what effort can a generic ERDS system align with the ETSI ERDS or ETSI REM standards.

4.2.2 ETSI ERDS baseline

4.2.2.1 General Requirements

The ERDS baseline aligns with the principles established in eIDAS2 Regulation [i.2] Recital 24, which emphasizes the need for a legal framework to facilitate cross-border recognition between national legal systems in the realm of electronic registered delivery services. This framework aims to create new market opportunities for Union trust service providers and ensure accurate delivery of data using qualified electronic registered delivery services, with a particular focus on the correct identification of the addressee.

This baseline extends the Registered Electronic Mail (REM) baseline concept to the entire Electronic Registered Delivery Services (ERDS) standards framework. It ensures compliance, trust, and interoperability across a broad spectrum of solutions through a new binding protocol characterized by innovative flexibility and adaptability. This approach facilitates extensive interoperability among various e-delivery paradigms, including REM.

Moreover, the modular design of this baseline allows for the integration of new technologies, thereby strengthening and enhancing the ERDS model and other supporting technologies. The main objective is to offer a decisive, effective, and efficient response to the growing demands of cybersecurity.

Key features of the ERDS baseline include:

1) Technological neutrality.

2) Modularity for easy adoption, pluggability, and extensibility, grounded in the non-orthogonality principle.

3) Ensuring service provision through Qualified Trusted Service Providers (QTSPs), in accordance with EU eIDAS Regulation [i.1] Article 44(a).

4) Full compatibility with software under as-is licenses.

4.2.2.2 Application to the entire ERDS standard

The REM baseline, as published in 2024 under ETSI EN 319 532-4 [i.21], specifies a minimal set of requirements designed to maximize interoperability in cross-REM domains, particularly for cross-border REM services. Adhering to the REM baseline simplifies the technical support provided by Member States' competent authorities for qualified registered electronic delivery services. Without a common baseline, supporting REM can be both costly and complex.

Extending the REM baseline concept across the entire ERDS standard allows for the inheritance of basic interoperability and compliance benefits from the REM baseline. Additionally, it facilitates the integration of various technologies that can also be transparently applied within REM, as REM baseline can be viewed as an instance of the ERDS baseline.

4.2.2.3 General needs identified to define ERDS baseline

Figure 1 shows a generic ERDS system with two Trust Service Providers (TSPs) utilizing a standard protocol without specific packaging.

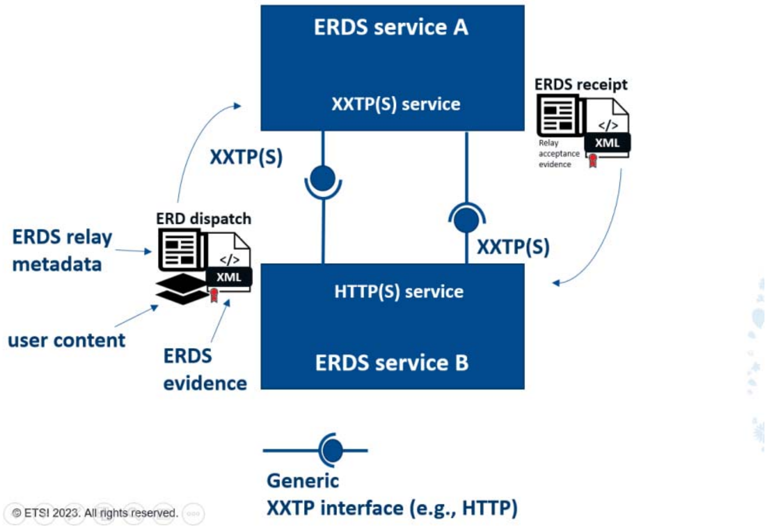


Figure 1: Generic ERDS basic flow (no baseline)

From this, the fundamental components necessary to define the ERDS baseline are identified:

- Packaging details for the data transfer:
  - User content
  - Metadata (ERDS relay metadata)
  - Evidence (ERDS evidence)
- Transport details for the packaged data:
  - Enveloping methods
  - Protocol
  - Addressing/Routing
  - Saving options
  - Security options

Figure 2 illustrates how the ERDS baseline addresses these needs with a lightweight layer comprising two modules:

- A "Smart Wrap Service" module for packaging user content, metadata, and evidence.
- An "HTTP-based Service" module for transport, supported by various technological options.

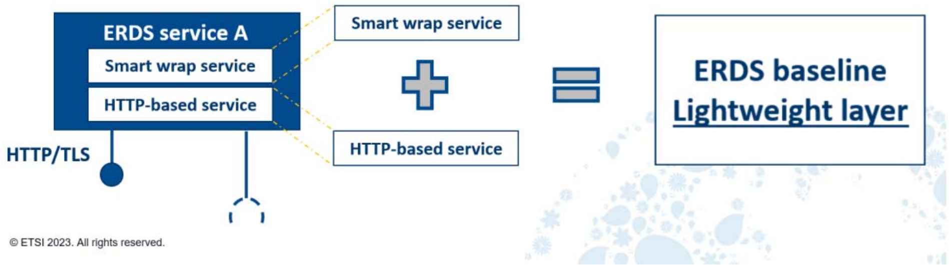


Figure 2: ERDS Baseline - A Lightweight Layer within the Existing (Q)ERDS/(Q)ERDSP standardization rationalized framework

Subsequent clauses provide more detailed information on these aspects of the ERDS baseline, contextualized within the existing model as a new, lightweight binding layer.

4.2.2.4 Packaging

The proposal for the packaging module of the ERDS baseline includes a number of classic formats options plus a general custom method (i.e. JSON, XML ZIP, MIME, CUSTOM) as illustrated in Figure 3.

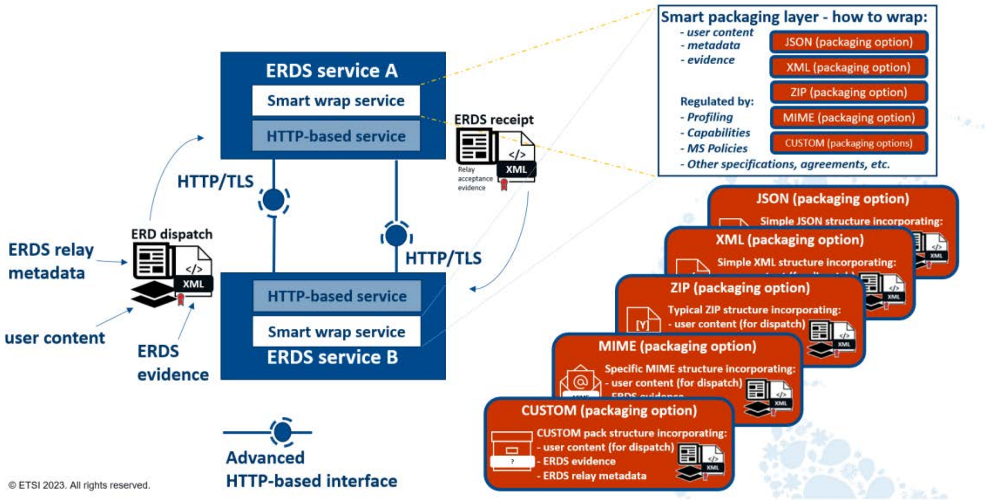


Figure 3: ERDS Baseline - Packaging Details

For example, Figure 4 demonstrates the use of the ZIP packaging option for user content, ERDS relay metadata, and ERDS evidence.

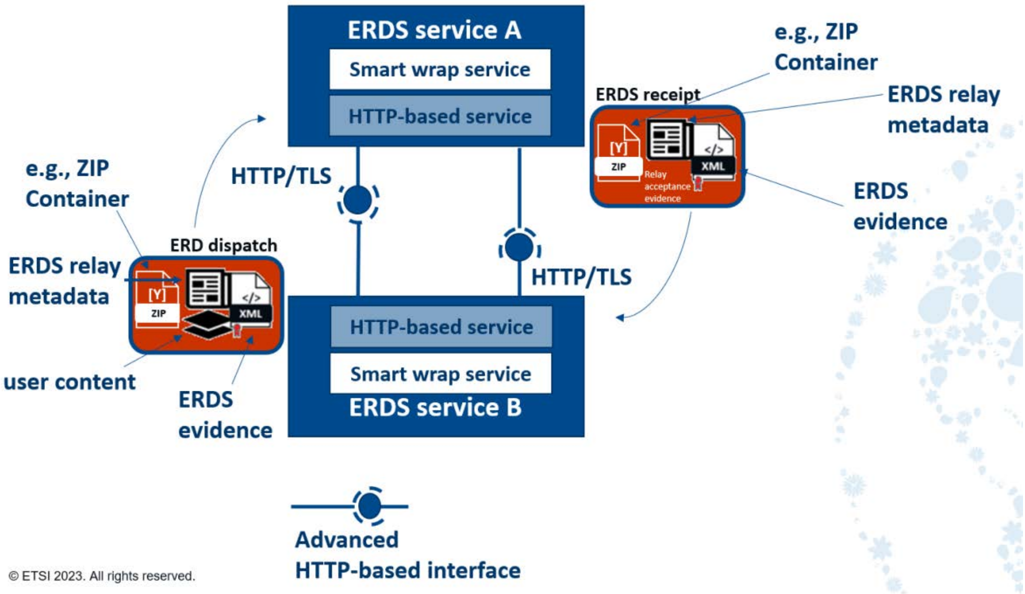


Figure 4: ERDS Baseline - ZIP Packaging Example

4.2.2.5 Transport

The transport module of the ERDS baseline consists of a set of supporting technological functions and options identified to cover the following common needs:

- Common Service Infrastructure (CSI) dealing with *addressing*, *routing* and *trusting* purposes.
- Mechanism for:
  - wrapping the ERD dispatch or the ERDS receipt together with the transport information (e.g. *relay metadata*), at protocol level, during the conveyance phase;

  - securing the relevant transport metadata information;
  - recording the transport metadata information.

- Suitable technology for:
  - a reliable transfer provided by a representational state transfer (optionally improved by an auto-resume option for recovering of issues during the transfer for potentially *huge contents*);
  - a protected transfer provided by a transport layer security (optionally improved by additional security measures for domain name system).

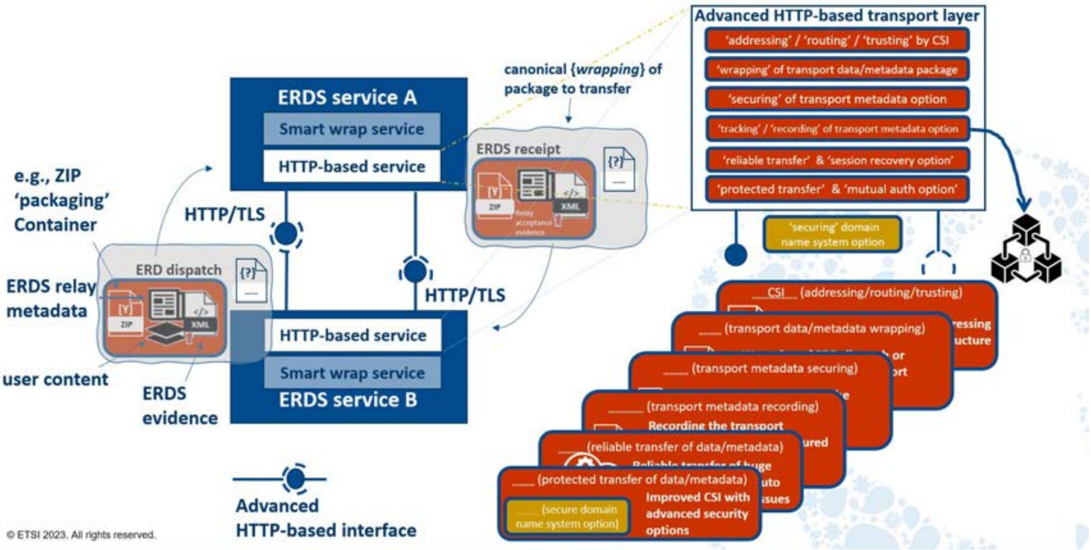

Advanced HTTP-based transport layer
'addressing' / 'routing' / 'trusting' by CSI
'wrapping' of transport data/metadata package
'securing' of transport metadata option
'tracking' / 'recording' of transport metadata option
'reliable transfer' & 'session recovery option'
'protected transfer' & 'mutual auth option'
'securing' domain name system option
canonical {wrapping} of package to transfer
ERDS service A
Smart wrap service
HTTP-based service
ERDS receipt
{?}
ZIP
XML
e.g., ZIP 'packaging' Container
HTTP/TLS
ERD dispatch
ERDS relay metadata
user content
ERDS evidence
HTTP/TLS
HTTP-based service
Smart wrap service
ERDS service B
CSI (addressing/routing/trusting)
(transport data/metadata wrapping)
(transport metadata securing)
(transport metadata recording)
Recording the transport
(reliable transfer of data/metadata)
(protected transfer of data/metadata)
(secure domain name system option)
Improved CSI with advanced security options
Advanced HTTP-based interface

Figure 5: ERDS Baseline - Transport Details

The optional technological support functions, added in a progressive and combined way, allow obtaining a *crescendo* of different levels of service.

EXAMPLE: Annex B describes **an example** of application of the present schema tailored to fit the requirements of eIDAS 2.0 [i.2] (Regulation No 910/2014 amended to establish a framework for a European Digital Identity for TSPs providing, amongst others, EU qualified ERDS).

The proposed model aims to be defined at a level of abstraction such as not to preclude the option of integration of different protocols and/or methods of transmission of contents. The ERDS-to-ERDS relay interface according to the specific transmission protocol AS4, currently defined in ETSI EN 319 522-4, sub-parts 1 [i.12], 2 [i.13] and 3 [i.14], is, for instance, one of these. This also applies for Hybrid Mail Secured electronic Postal Service (SePS) protocols, as outlined in ETSI TR 119 520-2 [i.3], clause 4.2.3.

Other options can allow the "detached" mode for ERDS evidence or being stored in a PDL by providing a standard interface for the management.

NOTE: See ETSI TR 119 520-2 [i.3], clause 5.

The new framework proposed below intends to ensure integration and maximization of interoperability, in a cost-effective way.

4.2.2.6 ERDS baseline and REM baseline: functional relationships

The proposed approach to define the ERDS baseline allows seeing the REM baseline as an "instance" of ERDS baseline. The present clause illustrates how this is configured in the current and in the future scenario.

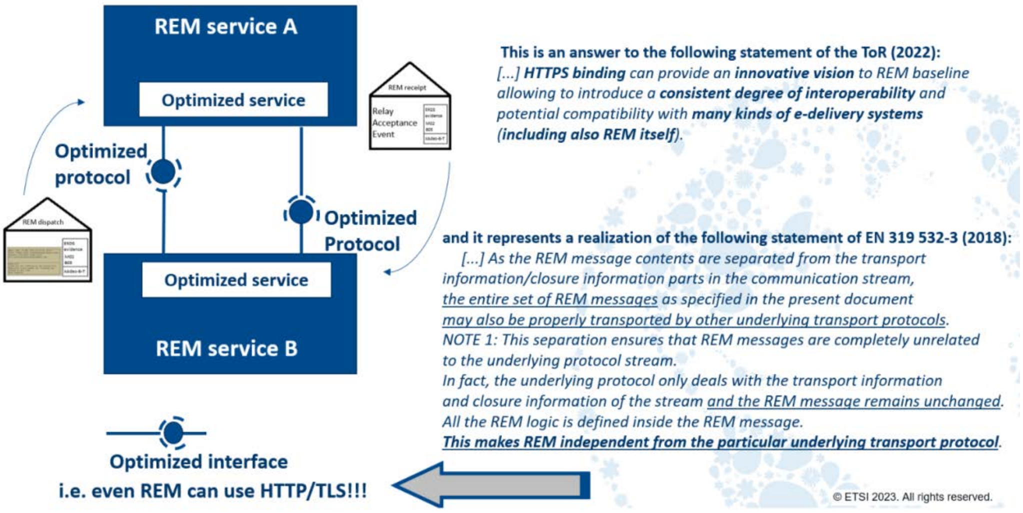
First of all, the REM logic is agnostic in respect to the transmission protocol. The optimization of the transport of the REM towards more powerful protocols represents a **realization** of what has been anticipated in the current standard of the REM. In fact, this aim appears in different places of ETSI EN 319 532-3 [i.20]:

> *"[...] As the REM message contents are separated from the transport information/closure information parts in the communication stream, <u>the entire set of REM messages</u> as specified in the present document <u>may also be properly transported by other underlying transport protocols</u>.*
>
> *NOTE 1: This separation ensures that REM messages are completely unrelated to the underlying protocol stream.*
>
> *In fact, the underlying protocol only deals with the transport information and closure information of the stream <u>and the REM message remains unchanged</u>. All the REM logic is defined inside the REM message.*
> ***<u>This makes REM independent from the particular underlying transport protocol</u>****<u>"</u>.*

See Figure 6 and also Figure A.2 of ETSI EN 319 532-3 [i.20] (for further details on the clear separation of the REM messages from the transport protocol).

The conclusion of this reasoning is that REM **can also use HTTP/TLS for transport**.

NOTE: This can be a capability-level controlled option, but for sure HTTP can be used. And this opens huge possibilities for interoperating.



This is an answer to the following statement of the ToR (2022):
*[...] **HTTPS binding** can provide an **innovative vision** to REM baseline allowing to introduce a **consistent degree of interoperability** and potential compatibility with **many kinds of e-delivery systems** (**including also REM itself**).*

and it represents a realization of the following statement of EN 319 532-3 (2018):
[...] As the REM message contents are separated from the transport information/closure information parts in the communication stream, <u>the entire set of REM messages</u> as specified in the present document <u>may also be properly transported by other underlying transport protocols</u>.
NOTE 1: This separation ensures that REM messages are completely unrelated to the underlying protocol stream.
In fact, the underlying protocol only deals with the transport information and closure information of the stream <u>and the REM message remains unchanged</u>.
All the REM logic is defined inside the REM message.
***<u>This makes REM independent from the particular underlying transport protocol</u>**.*

Figure 6: Optimization of the transfer protocol as anticipated in current REM standard

The second point is how to correlate the packaging relationship between ERDS baseline and REM baseline. In fact, the REM packaging of the *user content*, the *ERDS relay metadata* and the *ERDS evidence* can be **simply instantiated** by choosing the **MIME packaging option** of ERDS baseline, as illustrated in Figure 7.

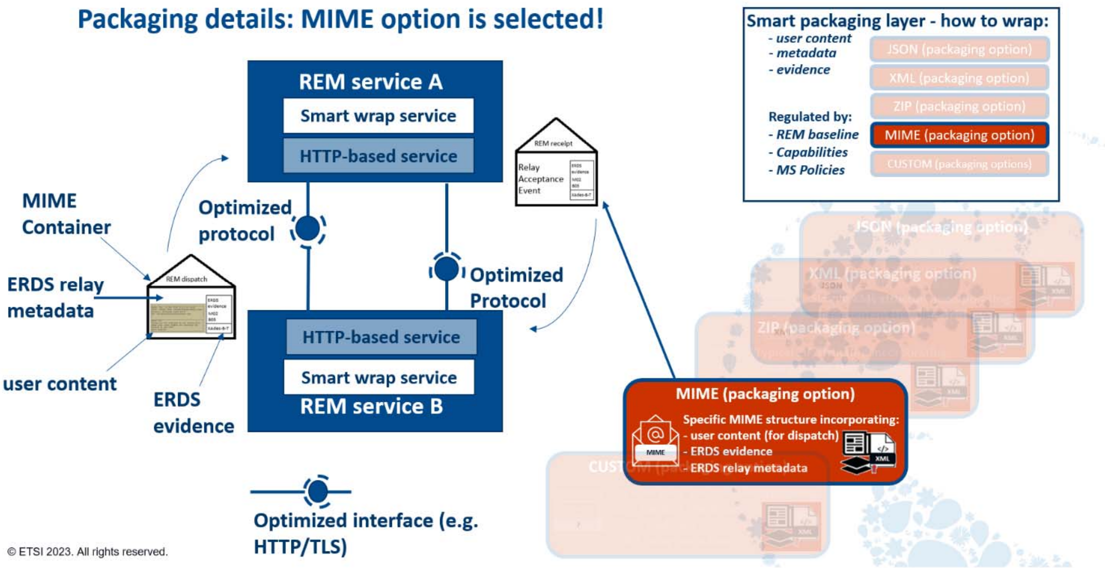


Figure 7: ERDS baseline MIME packaging option to support instantiation of REM

Finally, the transport optimized interface can be used, at QTSP-to-QTSP level as transfer protocol.

Figure 8 shows the full set of options and feature to instantiate ERDS baseline to serve a REM interaction. The selection of **MIME packaging option** for the *user content*, the *ERDS relay metadata* and the *ERDS evidence*; and the selection of **JAdES**, **Ledger**, **DNSSEC CSI** options for the *transport* of the packaged data (**CSI-TL**, **JSON**, **REST** and **TLS** are foreseen as *native functions* for ERDS baseline transport).

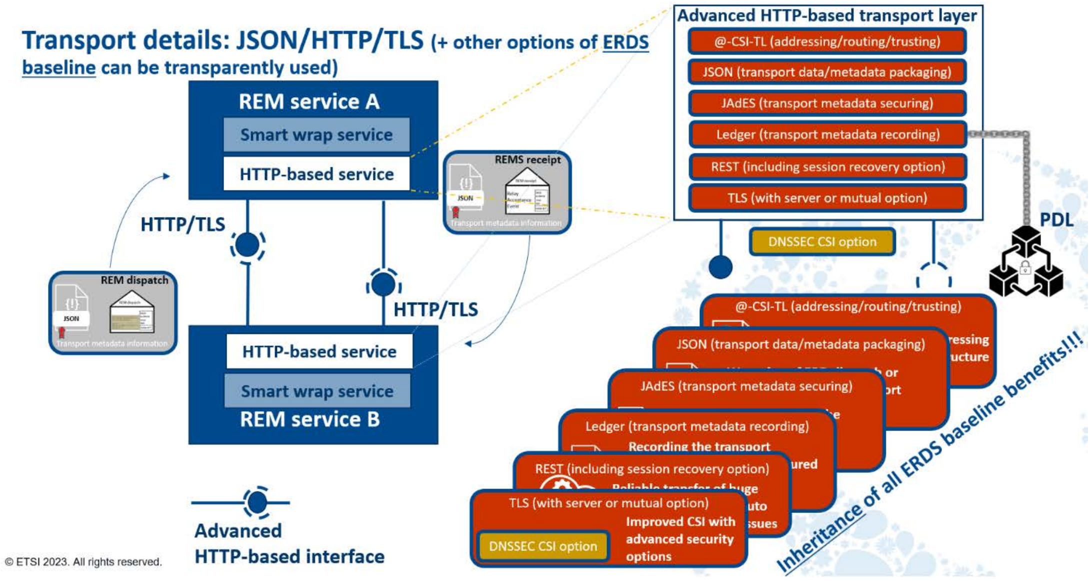

Transport details: JSON/HTTP/TLS (+ other options of ERDS baseline can be transparently used)
REM service A
Smart wrap service
HTTP-based service
REMS receipt
JSON
Transport metadata information
HTTP/TLS
REM dispatch
JSON
Transport metadata information
HTTP/TLS
HTTP-based service
Smart wrap service
REM service B
Advanced HTTP-based transport layer
@-CSI-TL (addressing/routing/trusting)
JSON (transport data/metadata packaging)
JAdES (transport metadata securing)
Ledger (transport metadata recording)
REST (including session recovery option)
TLS (with server or mutual option)
DNSSEC CSI option
PDL
@-CSI-TL (addressing/routing/trusting)
JSON (transport data/metadata packaging)
JAdES (transport metadata securing)
Ledger (transport metadata recording)
Recording the transport
REST (including session recovery option)
TLS (with server or mutual option)
Improved CSI with advanced security options
DNSSEC CSI option
Inheritance of all ERDS baseline benefits!!!
Advanced HTTP-based interface
© ETSI 2023. All rights reserved.

Figure 8: ERDS baseline HTTP transport + other options to support instantiation of REM

The example illustrated in Figure 8 represents the demonstration and practical application of how ERDS baseline through its "**new binding**" layer can be configured to instantiate REM baseline, as introduced at the beginning of the present clause.

4.2.3 ETSI ERDS baseline - inheritances from REM baseline

4.2.3.1 General considerations

Considering the technical and functional peculiarities seen in clause 4.2.2.6, further relationships, more editorial in nature, can be outlined between the ERDS baseline and REM baseline. In essence, the REM baseline can be viewed, at a functional level, as an instance of the ERDS baseline (once it is defined). Conversely, the ERDS baseline can be framed using the concept underlying the REM baseline, leveraging, mimicking, and extending some of the concepts characterizing the REM baseline.

4.2.3.2 ERDS baseline and REM baseline: editorial relationships

During the implementation of live systems according to the REM baseline, numerous feedbacks have been collected regarding the entire (Q)ERDS/(Q)ERDSP standardization rationalized framework. It is important to remember that REM heavily utilizes ERDS (e.g. ERDS evidence is commonly defined for both models, many of the generalities, schemes, URIs, etc., of REM are derived and imported from ERDS). The prevalent opinion regarding aspects that definitely need improvement in the entire (Q)ERDS/(Q)ERDSP standardization rationalized framework can be summarized as follows:

- There are too many documents: the information is fragmented and scattered across numerous sources. Readers are forced to continuously jump from one document to another, unless someone compiles another document to keep track of important points.
- There is a lack of detail on implementing many features.
- The current (Q)ERDS/(Q)ERDSP standardization rationalized framework is overly general, leading to multiple interpretations (with significant effort required to fix one, and a certain amount of risk in implementing it).

The REM baseline implemented in ETSI EN 319 532-4 [i.21] was conceived to address the latter two issues. However, during implementation, it was deemed appropriate to also anticipate a way to address the first issue. The whole set of needs has been addressed at different levels as follows:

- Compact structure of definitions in one document:
    - Annex B (informative) with the "reference map" featuring source standards and "rationales" obtained through a collection of citations from such standards.
    - Annex C (normative) with a structure similar to Annex B but with the "prescriptive" parts of the rationales cited in Annex B.
    - Annex D (informative) with suggested "best practices".
    - ZIP Attachment: with a full set of concrete "examples" (informative) and "XSDs" (normative).

NOTE: A high number of automatic cross-references have been implemented inside ETSI EN 319 532-4 [i.21] to facilitate consultation, jumping, and navigation forward/backward within the document itself.

Thus, it is considered that, during the definition of the entire (Q)ERDS/(Q)ERDSP standardization rationalized framework to implement the ERDS baseline, a more compact structure should be given to the documents, for instance, inheriting something like that implemented for the REM baseline in ETSI EN 319 532-4 [i.21]. In any case, the lesson learnt from the field is that, to facilitate the use of the documents, it is welcome to "repeat" the information in places where it is natural to have everything in a compact form, to assist the readers of the ERDS/REM framework of standards.

Therefore, it is to consider that, during the definition of entire (Q)ERDS/(Q)ERDSP standardization rationalized framework to implement the ERDS baseline, a more compact structure is given to the documents for instance on ETSI EN 319 532-4 [i.21].

In any case, the lesson learnt from the field is that, to facilitate the usage of the documents, it is welcome to "repeat" the information on places where it is natural to have everything in a compacted form, to help the readers of the ERDS/REM framework of standards as well as, to use cross-references, define all the details and finally, to provide concrete examples.

4.2.4 ETSI ERDS baseline - cross-interoperability

The ERDS baseline model, as depicted, supports the implementation of various solutions utilizing binding protocols beyond electronic mail. It establishes a universal set of requirements that enhance the trust and interoperability of systems developed under these guidelines, aligning with the Terms of Reference (ToR) requirements.

Importantly, the ERDS baseline, as proposed, enables "cross-interoperability" between diverse systems, not just among similar environments. Various methods to achieve this critical interoperability are conceivable. For example, these approaches may include:

- **Grace-Interoperability:** Direct interoperability from the sender's ERDS to the recipient's ERDS, maintaining the preferred operational mode.
- **Claim-Interoperability:** Indirect interoperability achieved through the recipient's ERDS operation.
- **Mixed Forms:** Combining the above approaches, enabling dynamic and automated interoperability.

The "Smart Wrap Service" in the packaging layer, particularly its Custom Packaging option, serves as a primary extension mechanism to integrate systems not initially anticipated. Specifically:

- The Custom Packaging option facilitates the integration of diverse ERDS systems.
- Essential elements like user content (from the sender), ERDS evidence, and ERDS relay metadata (generated by the QTSP), can be encapsulated in various container types. For instance, they could be embedded within a generic blob stream, with pointers indicating their locations within the stream for retrieval.

These concepts can be illustrated with an example of an ERDS service interoperating with a REM service. A capability query (e.g. policy or CSI) identifies the recipient's preferred packaging method (MIME, as shown in Figure 9).

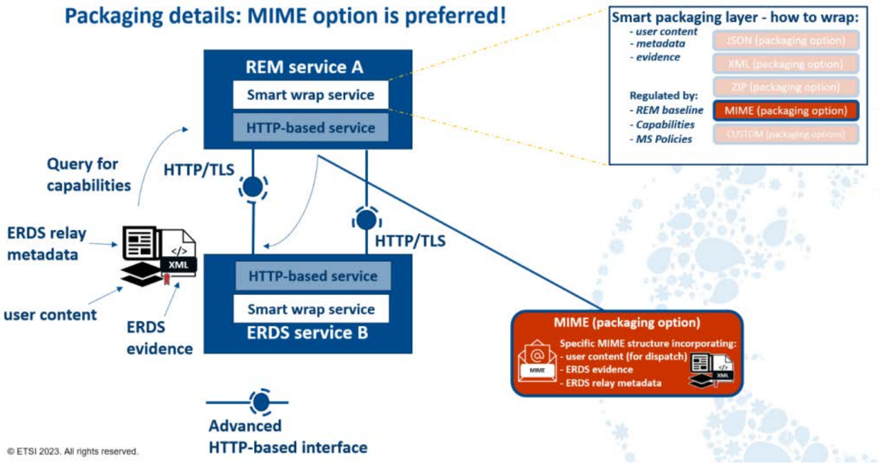


Figure 9: ERDS Baseline - Example of Interoperability ERDS/REMS (Capability Query)

In grace-interoperability, the sender's ERDS encloses individual objects using the recipient's preferred method (a REMS in this scenario), wrapped in the ERDS baseline JSON (optionally secured by JAdES), and transferred to the recipient's REMS, as shown in Figure 10.

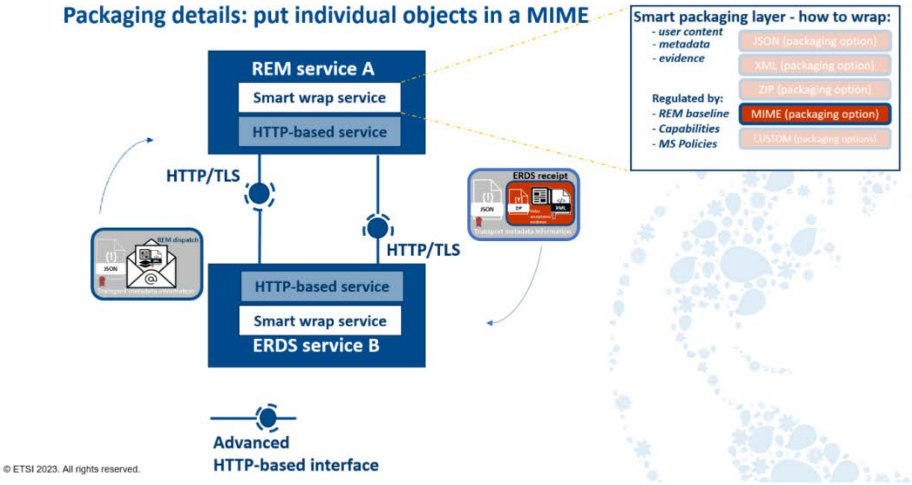


Figure 10: ERDS Baseline - Example of Interoperability ERDS/REMS (Grace-Interoperability Transfer)

The recipient's REMS, after verifying and unwrapping the content, utilizes the MIME objects as usual. The reverse flow, for receipts, follows the same mechanism: the recipient's REMS requests capabilities, wraps the ERDS RelayAcceptance in the sender's preferred method (e.g. ZIP), and sends it back enclosed in a JSON (optionally secured by JAdES).

Claim-interoperability operates similarly but leans more towards the sender's ERDS. If the recipient's ERDS allows multiple packaging methods, the sender's ERDS may choose the packaging method before sending the content.

The grace/claim forms can be combined, as the enveloping mechanism is fully automated once configured in the CSI.

The Custom Packaging option's most potent feature is its theoretical ability to integrate an extensive range of ERDS systems. By deconstructing the transfer material into essential components - user content, ERDS relay metadata, and ERDS evidence - and providing guidelines (e.g. through policy/capability) on identifying these components in any packaging form, extensive integration is feasible. This option also allows for peer-to-peer agreements for specific custom packages.

As outlined, particularly in clause 4.2.2.6, the ERDS baseline extends the concept of a baseline to a minimal set of options, ensuring a "standard" method for "open" interoperability among various ERDS systems. This approach is fully consistent with the ToR expectations and the objectives of the eIDAS Regulation [i.1].

4.3 Implications of the eIDAS2 Regulation to (Q)ERDS/(Q)ERDSP

4.3.1 Impact of the eIDAS2 in ERDS

The approval, publication and entry into force of the amendment of the eIDAS Regulation [i.1] (Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a Framework for a European Digital Identity [i.2]) known as the eIDAS2 or eIDAS2 Regulation has an impact on several areas of concern for the provision of electronic registered delivery services and REM. The establishment of new means of identity such as the European ID Wallet, new cybersecurity requirements aligned with the NIS 2 Directive [i.24], as well as the regulation of electronic attestations of attributes, among others, have to be taken into consideration in the revision of ERDS standards.

NOTE: To date two specific Articles 44(2a) and 44(2b) have been introduced to the eIDAS 2.0 [i.2] proposal, with more explicit requirements regarding interoperability in qualified electronic registered delivery services. So, the ERDS/REM baseline proposal aiming to maximize in a pragmatic way the cross-interoperability among different systems (through its XML ERDS evidence as a "standard" master cornerstone, and maintaining a high degree of neutrality potentially agnostic, in respect of many types of diverse services) assumes a higher relevance in the aiming of covering and respecting the requirements of the new version of the regulation.

Table A.1 included in Annex A identifies the most relevant changes and a tentative proposal for amendments to the ERDS standards.

As per this review, the following changes/updates should be included in the new ERDS standardization framework:

- Identity and ID proofing component: EUDIW and EAA identification.
- Impact on identification, identity matching and authentication processes: EUDIW, identity data and EAA as identity and/or authentication means, their provision, and signing/sealing.
- Impact on technical standardization and certification of EUDIW.
- Impact of EUDIW's access to a log of all transactions in interactions with ERDS.
- Relying parties' interoperation implications.
- New Interoperability framework.
- eIDAS2 [i.2] new services implication in (Q)ERDS operation (supply chain and outsourcing):
    - Validation of certificates.
    - Creation of electronic signatures.
    - Validation of electronic signatures.
    - Preservation of electronic signatures.
    - Management of remote electronic signature creation devices.
    - Issuing of electronic attestation of attributes.
    - Validation of electronic attestation of attributes.
    - Validation of data transmitted through electronic registered delivery services and related evidence.
    - The recording of electronic data into an electronic ledger.

See further details in Annex A.

4.4 Impact of emerging technologies and models on ERDS/REM models

A new set of emerging technologies and models is anticipated to have a significant impact on the provision of electronic delivery services (ERDS/REM). This necessitates a prompt assessment to ensure that ETSI standards remain at the forefront of the ERDS/REM market. The absence of standardization could result in substantial interoperability challenges among various solutions.

Numerous electronic delivery related initiatives connected to European policy measures and funded projects were introduced in the last years. It can arise the need for these services to be transformed into (Q)ERDS: for example article 24(1) of the NIS 2 Directive [i.24] states: *"Member States shall encourage essential and important entities to use qualified trust services"* and this includes QERDSs. Transforming a delivery service into a (Q)ERDS using the current framework of ETSI standard may have a strong impact on electronic delivery users and their applications and a seamless evolution is not currently fully supported by ETSI standards and could lead to non-interoperable implementations.

Novel ERDS models are emerging, wherein events are tracked within electronic ledgers, and these innovations could potentially reshape the landscape of ERDS/REM services. The absence of standardization for these novel models and technologies could result in independent implementations by various ERDS providers, precluding interoperability. The primary objective of The present document is to evaluate the influence of emerging technologies on ERDS/REM Models, not only to guarantee interoperability of implementations based on emerging technologies and models but also with those rooted in the existing set of standards.

ETSI TR 119 520-2 [i.3] puts forward concrete proposals concerning ERDS/REM service provision and models. It evaluates the impact of emerging technologies and models by closely monitoring their development. This includes:

- Emerging models implementing electronic delivery that are expected to evolve to ERDS.
- Emerging technologies that may impact ERDS/REM services, particularly those tracking events in electronic ledgers.
- Relevant standardization activities within ETSI and other organizations.
- Progress of European Commission initiatives such as the Digital Europe Program and the European Blockchain Services Infrastructure (EBSI).

The proposed framework in clause 5 takes into account the proposals from ETSI TR 119 520-2 [i.3].

4.5 New policy and security requirements for (Q)ERDS/(Q)ERDSP

(Q)ERDS Policy and security requirements are heavily impacted by eIDAS2 Regulation [i.2] and NIS 2 Directive [i.24].

The NIS 2 Directive [i.24], formally adopted by the European Parliament on 10 November 2022, and effective from January 16, 2023 (member states are required to incorporate it into their national law by fall 2024), aims to significantly enhance cybersecurity across the European Union. It is designed to build upon its predecessor, the NIS Directive, by expanding the scope of coverage from seven to eighteen critical industries and introducing a more robust framework for cybersecurity risk management, incident reporting, and information sharing among Member States. The directive categorizes entities into "essential" and "important," with each facing tailored obligations to bolster their cybersecurity resilience. Essential entities are subjected to stricter supervision and higher penalties for non-compliance.

One of the key motivations for introducing NIS 2 is to address the limitations observed with the implementation of the original NIS Directive, including its narrow scope and the lack of harmonization across EU member states which led to inconsistent levels of cybersecurity resilience. The rapid pace of digitalization and the increasing sophistication of cyber threats necessitated a more comprehensive and unified approach to secure the EU's critical infrastructure and digital environment.

NIS 2 Directive [i.24] sets out detailed requirements for entities within its scope, including the adoption of risk management measures, reporting of cybersecurity incidents, and ensuring the security of ICT supply chains. Specifically, Article 21 of the NIS 2 Directive [i.24] mandates that member states ensure both essential and important entities adopt appropriate and proportionate technical, operational, and organizational measures. These measures aim to manage the risks to the security of network and information systems used in their operations or service provision. The directive outlines specific measures including risk analysis policies, incident handling, business continuity, supply chain security, and basic cyber hygiene practices, among others. It emphasizes a holistic approach to cybersecurity, encompassing everything from policy formulation to the practical application of cybersecurity measures.

NIS 2 Directive [i.24] also places accountability on the management bodies of entities for compliance with the directive's requirements. Moreover, the directive aims to harmonize cybersecurity requirements and sanction regimes across the EU, thereby enhancing cooperation and information sharing between Member States to improve the overall cyber resilience of the EU.

Entities covered by the directive include those providing services or carrying out activities in the EU that are deemed "essential" or "important" across various sectors like energy, transport, health, digital services, and certain types of manufacturing, among others. Small and micro businesses are generally excluded, but there are specific criteria that could bring an entity into scope based on its size, significance, and the nature of its activities.

Organizations falling under the scope of NIS 2 Directive [i.24] need to assess their current cybersecurity practices against the directive's requirements and take necessary actions to ensure compliance. This includes implementing core cybersecurity policies, managing risks in their ICT supply chains, and preparing for incident response and reporting. By doing so, they contribute to strengthening the EU's collective cybersecurity posture and resilience against cyber threats.

Trust Service Providers (TSPs), critical to the EU's infrastructure, fall under the scope of the NIS 2 Directive [i.24]. This inclusion signifies recognition of the pivotal role TSPs play in the EU's digital and physical security ecosystem. In the context of the eIDAS2 Regulation [i.2], which is set to become directly applicable across the EU, trust service providers now face a dual regulatory burden. They have to comply with the stringent requirements laid out by eIDAS [i.1], which has regulated them since 2014, and now also adhere to the new directives introduced by NIS 2 Directive [i.24]. This dual regulation raises concerns about potential over-regulation and the implications for the market environment surrounding digital trust services. However, it also underscores the critical nature of trust services in ensuring the overall cyber resilience of the EU.

Under the NIS 2 Directive [i.24], TSPs are designated as essential entities, reflecting their critical role in maintaining the security and integrity of network and information systems across the European Union. Article 3 of the NIS 2 Directive [i.24] explicitly categorizes "qualified trust service providers and top-level domain name registries as well as DNS service providers" as essential entities, regardless of their size. This categorization underscores the importance of these entities in the digital infrastructure and the need for stringent security measures to safeguard against potential cyber threats. For QTSP being classified as essential entities means adhering to the highest standards of cybersecurity, reflecting their indispensable role in the EU's digital economy and the overarching goal of the NIS 2 Directive [i.24] to bolster cyber resilience across the Union.

Non QTSPs are considered important entities due to that their disruption, while still concerning, is assessed to have a less severe impact. This categorization affects the stringency of supervision and sanctions, with essential entities subject to more rigorous oversight.

The relationship between the NIS 2 Directive [i.24] and the eIDAS2 Regulation [i.2], particularly the reference to Article 21 of NIS 2 within eIDAS2, highlights the integrated approach the EU is taking towards cybersecurity and digital identity. This approach aims to enhance the security and reliability of digital services across the EU, ensuring that trust service providers, among other critical entities, operate under a robust regulatory framework designed to mitigate cyber risks effectively.

Any new proposal of (Q)ERDS policy and security requirements has to take into consideration ETSI EN 319 401 [i.25] update that includes, details and encompasses with a sector specific approach Article 21 of NIS 2 Directive [i.24] on security requirements.

See clause 4.3.1 for further details on the eIDAS2 Regulation [i.2] impact on (Q)ERDS policy and security requirements.

5 Proposal for a new (Q)ERDS/(Q)ERDSP standardization rationalized framework

5.1 Introduction

ERDS services standards could be organized around trust service components and developed through general requirements in their security policy and procedures document. Each component should focus on a specific aspect of ERDS services, and together they form a comprehensive framework for secure, reliable, and regulatory-compliant operation. Standardization in this context should, therefore, aim not only at supporting technical implementation but also at supporting regulatory compliance and effective risk management associated with the provision of ERDS services.

Trust service components are essential parts of a TSP's service, and their audits, whether conducted separately or as part of a TSP's complete audit, are crucial for ensuring the security, reliability, and compliance of the trust services provided. This approach allows for efficient auditing processes, reduces redundancy, and ensures comprehensive coverage of all service aspects.

A "trust service component" is defined in ETSI EN 319 403-1 [i.27] as one part of the overall service of a TSP. These components can vary, but they are integral to the functioning of a TSP. Examples of Trust Service Components are Server Signing Application Service Component (SSASC), components related to identity verification; components for secure communication; or time-stamping components.

The audit of "trust service component" is distinct yet related to the overall audit of a TSP. Here are some key points:

1) **Separate Conformity Assessment:** A Trust service component entirely provided by a supplier or an external organization can undergo a separate conformity assessment. This is beneficial for components used by multiple TSPs, allowing them to avoid repeated assessments.

2) **Integration in TSP Audit:** When the overall TSP is audited, the trust service components it uses, which may have been separately assessed, are also evaluated. The audit ensures that the TSP meets the requirements of each service component and that these components are effectively integrated into the TSP's service.

3) **Focus Areas in Component Audit provided by external organizations:**

   - obligations of external organizations;

   - subcontracting, outsourcing, or other third-party arrangements; or

   - termination procedures.

4) **Scope Definition:** The audit of a trust service component is focused on its specific requirements and how it integrates with the trust service. The Conformity Assessment Body (CAB) assessing the overall TSP's trust service ensures that the scope and boundaries of the trust service includes these components and that they comply with the TSP's security and policy requirements.

5) **Frequency of Audits:** The Trust Service component audit frequency should be the same as to that of the TSP although not aligned in time with the TSP audit frequency.

6) **Stage 2 Audit Considerations:** In the second stage of the TSP audit, if a trust service component has been audited separately, the audit team verifies the component's requirements and security measures, and how they fit into the TSP's service offering.

The requirements for qualified electronic registered delivery services, as outlined in Article 44 of the eIDAS2 Regulation [i.2], suggest several key "trust service components" integral to the operation of these services:

1) **Identification Component:** This component ensures the level confidence in identifying the sender (Article 44(1)(b)) and the addressee (Article 44(1)(c)). It involves identity verification processes and technologies to authenticate the identities of the parties involved in the electronic registered delivery service.

2) **Advanced Electronic Signature/Seal Component:** Per Article 44(1)(d), the sending and receiving of data are secured by an advanced electronic signature or seal. This component is critical for ensuring data integrity and authenticity, serving as a digital equivalent of a physical signature or stamp.

3) **Evidence Component:** The issuance, storage and retrieval of ERDS evidences. This is a key component to ensure eIDAS [i.1] compliance and the proposed framework includes its use with existing eDelivery service to technically evolve them to ERDS and QERDS.

4) **Time-Stamping Component:** According to Article 44(1)(f), the date and time of sending, receiving, and any change of data have to be indicated by a qualified electronic time stamp. This component provides a timestamp to every significant action or event within the service, ensuring traceability and temporal validation of the transactions.

5) **Security Component for Data Transfer:** This ensures that any change in the data necessary for the purpose of sending or receiving is clearly indicated to both the sender and addressee (Article 44(1)(e)). It involves mechanisms to detect and flag any alterations in the data, maintaining the integrity of the information throughout the delivery process. This component could involve encryption and other security measures to protect the data during transit, providing integrity, preventing unauthorized access and ensuring confidentiality.

Orthogonal to these components appears **interoperability** as a transversal technical component when two or more ERDS interoperate. Given the provision for data transfer between multiple qualified trust service providers (Article 44), standardization on this technical component ensuring interoperability is vital. Standards to be developed would include standardized protocols and formats for seamless integration and communication between different service providers.

In summary, both the ERDS and (Q)ERDS (as defined in eIDAS2 Regulation [i.2]) comprise multiple trust service components, each addressing specific requirements such as identification, evidence, time-stamping, security transfer, and interoperability.

From the previous description, the following trust service components can be provided completely by an external organization:

1) **Identification Service:** This component handles the identification of the sender and recipient with a high level of confidence. A third-party organization specialized in identification and authentication could provide this service, ensuring that the parties involved in the electronic registered delivery are authentic.

2) **Advanced Electronic Signature/Seal Service:** This component involves the generation and management of advanced electronic signatures or seals. For a QERDS, a QTSP will provide this component, ensuring the integrity and authenticity of the data sent and received.

3) **Electronic Time-Stamping Service:** The generation of qualified electronic time stamps to record the date and time of sending, receiving, and any changes to the data is a component. For a QERDS, this component will be provided by a QTSP.

These components (identification service, advanced electronic signature/seal service, electronic time-stamping) are view as complete and independent services that can be outsourced and provided by third-party organizations within the framework of QERDS and ERDS as per eIDAS2 [i.2].

From the component-based approach to ERDS, the existing standards would be organized as shown in Table 2.

Table 2: ERDS Services Component mapping table and Interoperability elements

Trust Service Component (can be provided by an outsourcer) + interoperability elements	Trust service component (Technical perspective)	eIDAS2 [i.2] requirement (as per Version for Technical Meeting on 11 October, 2023, 09-10-2023 at 16h00)	Standards
Identification Service (ID Proofing):	Identification Component	Art. 6 EUDIW EAA identification Art. 24.1 Article 44 1) b and c)	ETSI EN 319 521 [i.8] ETSI EN 319 522-1 [i.9] ETSI EN 319 531 [i.17] ETSI EN 319 532-2 [i.19] ETSI TS 119 461 [i.34] Clause 5 and 8 of ETSI EN 319 522-2 [i.10] Clause 5 of ETSI EN 319 522-3 [i.11]
Advanced Electronic Signature/Seal Service:	Advanced Electronic Signature/Seal Component	Article 44 1) d)	ETSI EN 319 521 [i.8] ETSI EN 319 522-1 [i.9] ETSI EN 319 531 [i.17] ETSI EN 319 532-2 [i.19] Clause 7 of ETSI EN 319 522-2 [i.10], ETSI EN 319 532-2 [i.19], ETSI EN 319 411 (all parts) [i.32]
Electronic Time-Stamping Service	Time-Stamping Component	Article 44.1)f)	ETSI EN 319 521 [i.8] ETSI EN 319 522-1 [i.9] ETSI EN 319 531 [i.17] ETSI EN 319 532-2 [i.19] ETSI EN 319 421 [i.33]
	Evidence component	Article 44. 1) e)	ETSI EN 319 521 [i.8] ETSI EN 319 522-1 [i.9] ETSI EN 319 531 [i.17] ETSI EN 319 532-2 [i.19] ETSI EN 319 522-2 [i.10] Clause 8 of ETSI EN 319 522-2 [i.10] Clause 5 of ETSI EN 319 522-3 [i.11] Clause 8 of ETSI EN 319 532-2 [i.19]

Trust Service Component (can be provided by an outsourcer) + interoperability elements	Trust service component (Technical perspective)	eIDAS2 [i.2] requirement (as per Version for Technical Meeting on 11 October, 2023, 09-10-2023 at 16h00)	Standards
	Security Component for Data Transfer	Implied in Article 44	ETSI EN 319 521 [i.8] ETSI EN 319 522-1 [i.9] ETSI EN 319 531 [i.17] ETSI EN 319 532-2 [i.19]
Interoperability		Article 44	ETSI EN 319 521 [i.8] ETSI EN 319 522-1 [i.9] ETSI EN 319 531 [i.17] ETSI EN 319 532-2 [i.19] Clauses 6 and 9 of ETSI EN 319 522-2 [i.10] Clauses 4 and 6 of ETSI EN 319 522-3 [i.11] ETSI EN 319 522-4-1 [i.12] ETSI EN 319 522-4-2 [i.13] ETSI EN 319 522-4-3 [i.14] Clause 9 of ETSI EN 319 532-2 [i.19] ETSI TS 119 524-1 [i.15] ETSI TS 119 524-2 [i.16] ETSI EN 319 532-4 [i.21] ETSI TS 119 534-1 [i.22] ETSI TS 119 534-2 [i.23]

5.2 Proposal on simplification and rationalization of ERDS standards

As a result of the review carried out in the present document, the following reorganization and rearrangement of the (Q)ERDS standards (Table 3) are proposed:

1) **New framework**. Update ETSI TR 119 500 [i.7] and ETSI SR 019 050 [i.6].

2) **Policy and security requirement**. Merge in a single document and update the following documents in view of the "TS components" approach:

   - ETSI EN 319 521 [i.8].
   - ETSI EN 319 522-1 [i.9].
   - ETSI EN 319 531 [i.17].
   - ETSI EN 319 532-1 [i.18].

3) Evidence and data integrity:

   3.1) Evidence. Standards to be developed would include:

   - Clause 8 of ETSI EN 319 522-2 [i.10].
   - Clause 5 of ETSI EN 319 522-3 [i.11].
   - A new clause defining a JSON format for Evidence.
   - The clause dealing with Evidence as PDF documents.
   - A new clause defining a JSON format for Evidence.

   3.2) Data structures. Standards to be developed would include the semantics of what is transferred. Build one document from:

   - ETSI EN 319 522-2 [i.10], EXCEPT clauses 8 and 9.

3.3) Bindings:

- Binding for Electronic Mail: ETSI EN 319 532-3 [i.20].
- Binding for AS4, ONE part composed of the following material:
    - Clause 4 of ETSI EN 319 522-3 [i.11].
    - ETSI EN 319 522-4-1 [i.12].
    - ETSI EN 319 522-4-2 [i.13].
    - Material in clauses 5 and 6 of ETSI EN 319 522-4-3 [i.14].

4) Interoperability

4.1) Interoperability Framework. Presentation of the CSI and even Trust building (Trusted Lists), if this is not included in policy and security requirements standards:

- ETSI EN 319 522-2 [i.10], clause 9.
- Material on Trust building and Trusted Lists if not in policy and security requirements standards.

4.2) Interoperability profiles. One sub-part for each interoperability profile:

- ETSI EN 319 532-4 [i.21]. This includes the REM Baseline.
- New ERDS - HTTP based baseline.

4.3) Testing:

- Merge in a single document the following:
    - ETSI TS 119 524-1 [i.15].
    - ETSI TS 119 534-1 [i.22].
- Merge in a single document the following:
    - ETSI TS 119 524-2 [i.16].
    - ETSI TS 119 534-2 [i.23].

Table 3 includes a detail reorganization of clause content from a component perspective:

Table 3

Domain	Subdomain	Content	Comments
New framework		Update ETSI TR 119 500 [i.7] and ETSI SR 019 050 [i.6].	
Policy and security requirement		Merge in a single document and update the following documents in view of the "TS components" approach: • ETSI EN 319 521 [i.8] . • ETSI EN 319 522-1 [i.9]. • ETSI EN 319 531 [i.17]. • ETSI EN 319 532-1 [i.18].	Policy and security requirement document could also consider the evidence component and its role in making compliant an existing electronic delivery service to ERDS/QERDS. It could provide checklists for compliance and evaluation.

Domain	Subdomain	Content	Comments
Evidence and data integrity	Evidence	Standards to be developed on evidence would include: • Clause 8 of ETSI EN 319 522-2 [i.10]. • Clause 5 of ETSI EN 319 522-3 [i.11]. • A new clause defining the Evidence component, including issuance, storage and retrieval of ERDS evidences and their API. • A new clause defining a JSON format for Evidence. • The clause dealing with Evidence as PDF documents. • A clause clarifying the mapping with the semantic and technical layers of the European interoperability framework.	
	Data structures	Standards to be developed on data structures would include the semantics of what is transferred. Build one document from: • ETSI EN 319 522-2 [i.10], EXCEPT clauses 8 (Evidence) and 9 (Common Service Interface: this should be part of the Interoperability component).	
	Bindings	Standards to be developed on bindings would include: • Binding for Electronic Mail: ETSI EN 319 532-3 [i.20]. • Binding for AS4, ONE part composed of the following material: – Clause 4 of ETSI EN 319 522-3 [i.11]. – ETSI EN 319 522-4-1 [i.12]. – ETSI EN 319 522-4-2 [i.13]. – Material in clauses 5 and 6 (of ETSI EN 319 522-4-3 [i.14]. • Binding for existing electronic delivery services, aiming to provide an evolution path to ERDS/QERDS that is as much as possible transparent for the users of the service.	
Interoperability	Interoperability Framework	Standards to be developed would include: • Presentation of the CSI and even Trust building (Trusted Lists), if this is not included in policy and security requirements standards: – ETSI EN 319 522-2 [i.10], clause 9 (Common Service Interface: this should be part of the Interoperability component). • Material on Trust building and Trusted Lists if not in policy and security requirements standards.	
	Interoperability profiles	One sub-part for each interoperability profile. • ETSI EN 319 532-4 [i.21]. This includes the REM Baseline. • New ERDS - HTTP based baseline.	
	Testing	Merge in a single document the following: • ETSI TS 119 524-1 [i.15]. • ETSI TS 119 534-1 [i.22]. Merge in a single document the following: • ETSI TS 119 524-2 [i.16]. • ETSI TS 119 534-2 [i.23].	Explicitly include baseline related testing.

Annex A: eIDAS2 Regulation impact on ERDS/REM standards

Legend for column "Type":

- D: Definition
- TS: Trusted Service
- AT: Text in Article
- ANN: Annex

Table A.1

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
1	D	'electronic identification' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a natural or legal person.	A natural person can now represent another natural person.
			No implications on the framework of standards for ERDS/REM.
2	D	'person identification data' means a set of data, issued in accordance with Union or national law, enabling the identity of a natural or legal person, or of a natural person representing a natural or legal person, to be established.	The personal data have to be issued now "in accordance with Union of national law"; also a natural person can now represent another natural person.
			No implications on the framework of standards for ERDS/REM.
3	D	'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing natural or legal persons.	A natural person can now represent another natural person.
			No implications on the framework of standards for ERDS/REM.
4	D	'authentication' means an electronic process that enables the electronic identification of a natural or legal person to be confirmed, or the origin and integrity of data in electronic form to be confirmed.	The authentication has to confirm the identification of a natural or legal person.
			Make it sure that the usage of authentication in the set of standards is aligned with this redefinition.
5	D	'electronic identification means' means a material and/or immaterial unit, containing person identification data and which is used for authentication to an online service or, where appropriate, to an offline service.	This introduces the provision of authenticating to an offline service.
			When the new framework is defined, the team in charge will have to assess whether this may have any impact.
6	D	'electronic identification scheme' means a system for electronic identification under which electronic identification means, are issued to natural or legal persons or natural persons representing natural or legal persons.	A natural person can now represent another natural person.
			No implications on the framework of standards for ERDS/REM.
7	D	'relying party' means a natural or legal person that relies upon an electronic identification, European Digital Identity Wallets or other electronic identification means, or a trust service.	This term was used in eIDAS [i.1] but not defined, and now this is directly connected to the EUDI Wallet.
			Assess the implications for ERDS framework.
8	D	'user' means a natural or legal person, or a natural person representing a natural or legal person, using trust services or electronic identification means, provided according to this Regulation.	No definition in eIDAS [i.1].
			Use this definition in ERDS standards.
9	D	'certificate for electronic signature' means an electronic attestation, which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.	
			Assess the impact of defining certificate as an electronic attestation.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
10		'trust service' means an electronic service normally provided for remuneration which consists of: (a) the issuing of certificates for electronic signatures, of certificates for electronic seals, of certificates for website authentication or of certificates for the provision of other trust services; (aa) the validation of certificates for electronic signatures, of certificates for electronic seals, of certificates for website authentication or of certificates for the provision of other trust services; (b) the creation of electronic signatures or of electronic seals; (c) the validation of electronic signatures or of electronic seals; (d) the preservation of electronic signatures, of electronic seals, of certificates for electronic signatures or of certificates for electronic seals; (e) the management of remote electronic signature creation devices or of remote electronic seal creation devices; (f) the issuing of electronic attestations of attributes; (fa) the validation of electronic attestation of attributes; (fb) the creation of electronic timestamps; (fc) the validation of electronic timestamps; (fd) the provision of electronic registered delivery services; (fe) the validation of data transmitted through electronic registered delivery services and related evidence; (ff) the electronic archiving of electronic data; or (fg) the recording of electronic data into an electronic ledger.	
			Impact of new services defined: (aa) Validation of certificates. (b) Creation of electronic signatures. (c) Validation of electronic signatures. (d) Preservation of electronic signatures. (e) Management of remote electronic signature creation devices. (f) Issuing of electronic attestation of attributes. (fa) Validation of electronic attestation of attributes. (fe) Validation of data transmitted through electronic registered delivery services and related evidence. (fg) The recording of electronic data into an electronic ledger. Cells below provide remarks on each of these services individually.
11		(aa) the validation of certificates for electronic signatures, of certificates for electronic seals, of certificates for website authentication or of certificates for the provision of other trust services.	New trusted service
			ERDS providers could externalize this task. This was not considered as a trusted service in eIDAS [i.1], so this will have an impact on the new framework of the standards: • In the policy documents for requirements on externalization. • Assess whether there should be some impact on the technical specs.
12		(b) the creation of electronic signatures or of electronic seals.	New trusted service
			An ERDS/REM service could externalize the generation of electronic signatures, seals and time-stamps to another service. Indeed, the generation of electronic signatures and seals was not considered as a trusted service in eIDAS [i.1], so this will have an impact on the new framework of the standards: • In the policy documents for requirements on externalization. • In technical specifications for making it clear that whenever they refer to the signature of the provider, readers have to understand that the signature generation may have been externalized.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
13		(c) the validation of electronic signatures or of electronic seals.	New trusted service
			ERDS providers could externalize this task. This was not considered as a trusted service in eIDAS [i.1], so this will have an impact on the new framework of the standards: • In the policy documents for requirements on externalization. • Assess whether there should be some impact on the technical specs.
14		(d) the preservation of electronic signatures, of electronic seals, of certificates for electronic signatures or of certificates for electronic seals.	New trusted service
			ERDS providers could externalize the preservation of signed data (evidence, for instance).
15		(e) the management of remote electronic signature creation devices or of remote electronic seal creation devices.	New trusted services
			An ERDS/REM service could externalize the management of the electronic signature creation devices of electronic signatures, to another service. This was not considered as a trusted service in eIDAS [i.1], so this will have an impact on the new framework of the standards: • In the policy documents for requirements on externalization. • Assess whether there should be some impact on the technical specs.
16		(f) the issuing of electronic attestations of attributes.	New trusted service
			The presence of electronic attestations of attributes will impact in the identification/authentication of users. See below.
17		(fa) the validation of electronic attestation of attributes.	New trusted service
			This task can be present during the authentication of users. Therefore, it has to be taken into account. Potential impact on the new framework of the standards: • In the policy documents for requirements on externalization. • Assess whether there should be some impact on the technical specs.
18		(fc) the validation of electronic timestamps.	New trusted service
			Assess whether this is a service that an ERDS/REM service could need, in which case it could be externalized.
19		(fe) Validation of data transmitted through electronic registered delivery services and related evidence.	New trusted service
			Indeed, this is a service directly connected with ERDS. Therefore there should be some standards in the framework.
20		(ff) the electronic archiving of electronic data.	New trusted service
			An ERDS/REM service could externalize the archival of selected electronic data. This was not considered as a trusted service in eIDAS [i.1], so this will have an impact on the new framework of the standards: • In the policy documents for requirements on externalization. • In the technical specs.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
21		(fg) the recording of electronic data into an electronic ledger.	New trusted service ISO is drafting a new part for using of PDLs by Trusted Transport Platforms in two ways, namely: as repository of users' identity data, and as repository of evidence generated by the service. The new framework will take into consideration the possibility of using a PDL, at least, as a repository of ERDS Evidence. The feasibility of using it also as what in ISO 19626 [i.28] is called TTP identity directory, which "provides registration functions to identify and confirm the trustworthiness of the identity information of communication participants (communication servers and communication clients).
22	D	(18) conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or to carry out certification of European Digital Identity Wallets or electronic identification means.	Definition A CAB also carries out certification of EUDI Wallet or electronic identification means. This has to be taken into account in the policy documents.
23		(21) 'product' means hardware or software, or relevant components of hardware and / or software, which are intended to be used for the provision of electronic identification and trust services.	This term also applies now to the provision of electronic identification services.
24		(23a) 'remote qualified electronic signature creation device' means a qualified electronic signature creation device managed by a qualified trust service provider in accordance with Article 29a on behalf of a signatory; (23b) 'remote qualified electronic seal creation device' means a qualified electronic seal creation device managed by a qualified trust service provider in accordance with Article 39a on behalf of a seal creator.	One term for each: qualified electronic signature and qualified electronic seal. Documents on policy when the ERDS/REM service is using remote creation devices for qualified signatures/seals.
25		(38) 'certificate for website authentication' means an electronic attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued; (39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV'.	No impact
26		(41) 'validation' means the process of verifying and confirming that data in electronic form are valid according to the requirements of this Regulation'.	Usually, in ERDS/REM specs validation applies to the validation of digital signatures/seals, etc. Assess the impact of this broader definition.
27	D	(42) 'European Digital Identity Wallet' means an electronic identification means, which allows the user to securely store, manage and validate identity data and electronic attestations of attributes, to provide them to relying parties and to other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals.	New object Relevant impact on the framework of standards: identity data and attestation of attributes, their provision, and signing/sealing.
28	D	(43) 'attribute' means a characteristic, quality, right or permission of a natural or legal person or of an object.	New object Potential impact on the authentication processes. Therefore impact on policy documents. Maybe also in technical documents.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
29	D	(44) 'electronic attestation of attributes' means an attestation in electronic form that allows the authentication of attributes.	New object Potential impact on the authentication processes. Therefore impact on policy documents. Maybe also in technical documents.
30	D	(45) 'qualified electronic attestation of attributes' means an electronic attestation of attributes, which is issued by a qualified trust service provider and meets the requirements laid down in Annex V.	New object: Potential impact on the authentication processes. Therefore impact on policy documents. Maybe also in technical documents.
31	D	(45a) 'electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source' means an electronic attestations of attributes issued by a public sector body responsible for an authentic source or by a public sector body designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45da and meeting the requirements laid down in Annex VIa.	New object: Potential impact on the authentication processes. Therefore impact on policy documents. Maybe also in technical documents.
32	D	(46) 'authentic source' is a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice.	New object: Assess whether, if the validation of attributes is incorporated in some process (authentication), this entity should be also taken into account.
33	D	(47) 'electronic archiving' means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to guarantee their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period.	New services: Already dealt with when talking about trusted services.
34	D	(48) 'qualified electronic archiving service' means an electronic archiving service that meets the requirements laid down in Article 45ga.	New services: Already dealt with when talking about trusted services. Assess whether this kind of service could be used by ERDS/REM providers during the provision of the services.
35	D	(49) 'EU Digital Identity Wallet Trust Mark' means a verifiable indication in a simple, recognisable and clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation.	New object Potential impact on the policy documents when dealing with EUDI Wallets.
36	D	(50) 'strong user authentication' means an authentication based on the use of at least two authentication factors from different categories of either knowledge (something only the user knows), possession (something only the user possesses) or inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.	New concept (process) Assess its impact in the policy requirements concerning authentication of users and service providers.
37	D	(53) 'electronic ledger' means a sequence of electronic data records, ensuring their integrity and the accuracy of their chronological ordering'.	New object, service See details of potential usages as per: • ISO 19626 [i.28]. • Outcome of draft DTR/ESI-0019540 (see bibliography). • Other technologies built on them, which could enrich the offer of ERDS providers (dapps, smart contracts).

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
38	D	(53a) 'qualified electronic ledger' means an electronic ledger that meets the requirements laid down in Article 45i.	New service See details of potential usages as per: • ISO 19626 [i.28]. • Outcome of DTR/ESI-0019540 (see bibliography). • Other technologies built on them, which could enrich the offer of ERDS providers (dapps, smart contracts).
39	D	(54) 'Personal data' means any information as defined in point 1 of Article 4 of Regulation (EU) 2016/679'	New object Assess whether this is something that has to be present somewhere in the framework.
40	D	(55) 'identity matching means a process where person identification data or person identification means are matched with or linked to an existing account belonging to the same person.	New process: Likely to impact in the policy documents. Assess whether this has also to be incorporated to some of the technical documents (i.e. processes showing interactions).
41		(55b) 'data record' means electronic data recorded with related meta-data supporting the processing of the data.	New object Assess whether this is something that has to be present somewhere in the framework.
42		(55c) 'offline use of European Digital Identity Wallets' means an interaction between a user and a third party at a physical location using close proximity technologies, whereby the Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction.	New interaction Assess whether there is a use case for ERDS/REM that could match it.
43	AT	**Pseudonyms in electronic transaction** Without prejudice to specific rules of Union or national law requiring users to identify themselves and without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms, chosen by the user, shall not be prohibited Dropped: 1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.	Recital (6) says: "Regulation (EU) 2016/679 [i.26] applies to the processing of personal data in the implementation of this Regulation. Therefore, this Regulation should lay down specific safeguards to prevent providers of electronic identification means and electronic attestation of attributes from combining personal data from other services with the personal data relating to the services falling within the scope of this Regulation." Assess whether this has any implication at the level of requirements in policy documents.
44	AT 6a	Article 6a: European Digital Identity Wallets 1. For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet within 24 months after the entry into force of the implementing acts referred to in paragraph 11 and Article 6c(4).	No direct impact on the policy documents other than mentioning EU DI Wallet. Assess correctness of assuming that entities in ERDS/REM will have an EU DI Wallet issued. Do legal persons include ERDS/REMS providers? If so, take it into account in the specifications (both policy and technical).
45	AT 6a	Article 6a: European Digital Identity Wallets 2. European Digital Identity Wallets shall be provided: (a) directly by a Member State; (b) under a mandate from a Member State; (c) independently of a Member State but recognised by a Member State.	Maybe EU DI Wallets issued by different entities could deserve different treatment or privileges. If so, take this into account in policy documents.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
46		Article 6a: European Digital Identity Wallets 2a. The source code of the application software components of the European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, specific components other than those installed on user devices shall not be disclosed.	Implications on ERDS policy and security requirements.
47		Article 6a: European Digital Identity Wallets 3. European Digital Identity Wallets are electronic identification means that shall enable the user in a manner that is user-friendly, transparent, and traceable by the user to: (a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, offline in order to use public and private services, while ensuring that selective disclosure of data is possible.	Relevant for authentication process, at least.
			Impact on policy and technical documents. Impact on disclosure on policy / technical documents.
48		Article 6a: European Digital Identity Wallets 3.(..) (ac) generate pseudonyms and store them encrypted and locally within it.	Use of pseudonyms stored in EUDI Wallets.
			Revise requirements in policy documents.
49		Article 6a: European Digital Identity Wallets 3.(..) (ad) securely authenticate another person's European Digital Identity Wallet, and receive and share identity data and electronic attestations of attributes in a secured way between the two wallets.	
			If legal persons may have EUDI Wallets, and an ERDS/REMS provider has one, a wallet to wallet authentication is also allowed. Implications in policy and technical docs.
50		Article 6a: European Digital Identity Wallets 3.(..) (ae) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard enabling the user to: (i) view an up to date list of relying parties with whom the user has established a connection and where applicable all data exchanged; (ii) easily request to a relying party the deletion of personal data pursuant to Article 17 of the Regulation (EU) 2016/679; iii) easily report to the national data protection authority where a relying party is established when an allegedly unlawful or suspicious request of data is received.	
			Requirements in policy on deletion of personal data.
51		Article 6a: European Digital Identity Wallets 3.(..) (b) sign by means of qualified electronic signatures and seal by means of qualified electronic seals.	
			Policy/technical documents: will be impacted by the fact that EUDI Wallet enable to sign and seal.
52		Article 6a: European Digital Identity Wallets 3.(..) (b) sign by means of qualified electronic signatures and seal by means of qualified electronic seals.	
			Policy/technical documents: use of EUDI wallet of the ERDS/REMS Provider for generating qualified signatures/seals.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
53	AT 6a	Article 6a: European Digital Identity Wallets 3.(..) (ba) download, to the extent technically feasible, users' data, electronic attestation of attributes and configurations.	Provision for downloading users' data from ERDS/REMS in policy / technical documents.
54		Article 6a: European Digital Identity Wallets 3.(..) (bb) exercise users' rights to data portability.	
55		Article 6a: European Digital Identity Wallets 4. European Digital Identity Wallets shall, in particular: (a) support common protocols and interfaces: (1) for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet.	No direct impact on ERDS/REMS framework of standards.
56		Article 6a: European Digital Identity Wallets 4.(..) (2) for relying parties to request and validate person identification data and electronic attestations of attributes.	Common to all the 6.a(a) (2) to 6.a(a) (4j) Related to ETSI TS 119 462 (see bibliography). In ERDS/REM technical specs a number of interfaces are shown and recurrently mentioned. Implication in policy and technical docs (protocols/interfaces).
57		Article 6a: European Digital Identity Wallets 4.(..) (3) for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, also offline.	Implication in policy and technical docs (protocols/interfaces). Take into account disclosure.
58		Article 6a: European Digital Identity Wallets 4. (..) (4a) to securely on-board the user with the electronic identification means associated pursuant to Article 6a(11a).	No direct impact on ERDS/REMS standards framework.
59		Article 6a: European Digital Identity Wallets 4.(..) (4c) for interaction with another person's European Digital Identity Wallet for the purpose of receiving, validating and sharing identity data and electronic attestations of attributes in a secured way between two wallets.	Assuming that ERDS provider is a legal person, which may have own an EUDI Wallet, the ERDS provided should also support protocols and interfaces for interacting with clients, owners of EUDI Wallets. This will impact policy and technical documents.
60		Article 6a: European Digital Identity Wallets 4.(..) (4d) for authenticating relying parties by implementing authentication mechanisms in accordance with Article 6b.	Clear implication in the policy and technical docs (authentication processes).
61		Article 6a: European Digital Identity Wallets 4. (..) (4e) for relying parties to verify the authenticity and validity of European Digital Identity Wallets.	No direct requirements for ERDS standards.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
62		Article 6a: European Digital Identity Wallets 4.(..) (4h) for requesting to a relying party the deletion of personal data pursuant to Article 17 of Regulation (EU) 2016/679).	No direct requirements for ERDS standards.
63		Article 6a: European Digital Identity Wallets 4.(..) (4i) for reporting to the national data protection authority where a relying party is established when an allegedly unlawful or suspicious request of data is received.	No direct requirements for ERDS standards.
64		Article 6a: European Digital Identity Wallets 4.(..) (4j) for the creation of qualified electronic signatures or seals by means of qualified signature or seal creation devices.	Already mentioned: requirements in policy documents on the use of qualified signatures/seals creation devices.
65		Article 6a: European Digital Identity Wallets 4. European Digital Identity Wallets shall, in particular: (b) not provide any information to trust service providers of electronic attestations of attributes about the use of these attributes.	Asses the worthiness of a mandatory requirement in policy documents forbidding ERDS/REM services not to provide any information of the use of any attribute that users may have presented to them during authentication UNLESS USER EXPRESSLY REQUESTS THIS (see New article 6b bullet 7 below). Assess the worthiness of a mandatory requirement in policy documents forbidding ERDS/REM services not to keep any information of the use of these attributes.
66		Article 6a: European Digital Identity Wallets 4.(..) (ba) Ensure that the identity of relying parties can be validated by implementing authentication mechanisms in accordance with Article 6b.	Impact in policy documents. Assess impact also on technical documents (authentication mechanisms).
67		Article 6a: European Digital Identity Wallets 4.(..) (c) meet the requirements set out in Article 8 with regards to assurance level "high", in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication.	Assess whether this wording for EU DI Wallet, specially the reference to assurance level "high" may affect policy documents, especially regarding authentication (and other processes where EU DI Wallet could be used).
68		Article 6a: European Digital Identity Wallets 4. (..) (ca) in the case of electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform that the requesting relying party or the requesting user of European Digital Identity Wallets have the permission to access it.	Impact on policy and technical docs (disclosure policies and associated mechanisms in technical docs).
69		Article 6a: European Digital Identity Wallets 4. (..) (e) ensure that the person identification data, which is available from the electronic identification scheme under which the EUDIW is provided, uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with the Wallet;	No apparent implications for ERDS/REM framework in terms of policy documents or technical specifications.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
70		Article 6a: European Digital Identity Wallets 4. (..) (ec) offer the ability to sign by means of qualified electronic signatures to all natural persons by default and free of charge. Member States may provide for proportionate measures to ensure that the free-of-charge.	Policy documents: allow natural persons to sign using EUDI Wallet.
71		Article 6a: European Digital Identity Wallets 4a Member State shall inform users, without delay, of any security breach that may have entirely or partially compromised their European Digital Identity Wallet or its content and in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 6da.	Not apparent impact on ERDS/REMS standards framework.
72	AT 6a	Article 6a: European Digital Identity Wallets 5. Member States shall provide free-of-charge validation mechanisms to: (a) ensure that the authenticity and validity of European Digital Identity Wallets can be verified.	Related with the process of verification of the authenticity and validity of attributed person identification data (relevant, at least, for authentication). The policy and the technical documents will take into consideration these validation mechanisms provided by the EU Member states when trying to verify the EUDI Wallets.
73		Article 6a: European Digital Identity Wallets 5. Member States shall provide free-of-charge validation mechanisms to: (ca) allow European Digital Identity Wallet users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 6b.	Should there be relying parties acting between users and ERDS services, the policy and the technical documents will take into consideration these validation mechanisms provided by the EU Member states when trying to verify the EUDI Wallets.
74		Article 6a: European Digital Identity Wallets 5a. Member States shall provide means to revoke the validity of the European Digital Identity Wallet (a) upon the explicit request of the user; (b) when its security has been compromised; (c) upon the death of the user or cease of activity of the legal person.	Relevant to processes where EUDI Wallets take part. Impact on policy / technical documents: take into account status of the EUDI Wallets.
75		Article 6a: European Digital Identity Wallets 5c. Providers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the provision of services of the European Digital Identity Wallet.	Requirement on the EUDI Wallets providers No impact on ERDS/REM standards framework.
76	AT 6a	Article 6a: European Digital Identity Wallets 6. The European Digital Identity Wallets shall be provided under a notified electronic identification scheme of level of assurance 'high'.	Requirement for issuance of EU DI Wallets Assess the worthiness of adding an explicit mention to this identification scheme electronic notification and the level of assurance 'high' in the policy documents.
77		Article 6a: European Digital Identity Wallets 6a. European Digital Identity Wallets shall ensure security-by-design.	Requirement on the EUDI Wallets issuers No impact on ERDS/REM standards framework.
78		Article 6a: European Digital Identity Wallets 6b The issuance, use and revocation of the European Digital Identity Wallets shall be free of charge to all natural persons.	Requirement on the EUDI Wallets issuers No impact on ERDS/REM standards framework.

#	Type	eIDAS 2.0 provisions	Discussion	Actions to perform / Questions to answer
79	AT 6a	Article 6a: European Digital Identity Wallets 7. The users shall be in full control of the use of the European Digital Identity Wallet amd pf the data om their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this provider or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held by the provider of European Digital Identity Wallets. If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.	Other reference to data coming from services different than EU DI Wallet issuers, UNLESS THE USER HAS expressly requested it.	Requirements in policy documents prohibiting share of information about use of wallet in the context of ERDS/REMS provision if when specifying policy requirements for EUDI Wallet there are not general requirements that makes unnecessary to include there.
80		Article 6a: European Digital Identity Wallets 7a The use of the European Digital Identity Wallet shall be voluntary. Access to public and private services, access to labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous for natural or legal persons not using European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.		Policy / technical documents will allow use of alternatives to EUDI Wallets in all the processes where they can be used. Use of these alternatives will not be disadvantageous.
81		Article 6a: European Digital Identity Wallets 7b The technical framework of the European Digital Identity Wallet shall: (a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows for tracking, linking, correlating or otherwise obtain knowledge of transactions or user behaviour unless explicitly authorised by the user; (b) enable privacy preserving techniques which ensure unlinkability, where attestation of attributes do not require the identification of the user.		Policy docs to add requirements for achieving (a). Assess whether technical docs should include technical requirements for this. Assess whether 7b (b) has impact on ERDS/REMS standards framework.
82		Article 6a: European Digital Identity Wallets 7c Any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of the European Digital Identity Wallets as electronic identification means shall implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with Regulation (EU) 2016/679. Member States shall be allowed to introduce national provisions to further specify the application of such rules.	Requirements for providers of EUDI Wallets	No direct impact on ERDS/REM standards framework.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
83		Article 6a: European Digital Identity Wallets 7d Member States shall notify to the Commission, without undue delay information about: (a) the body responsible for establishing and maintaining the list of registered relying parties that rely on the European Digital Identity Wallets in accordance with Article 6b(1e), and the location of such a list; (b) the bodies responsible for the provision of the European Digital Identity Wallets in accordance with Article 6a(1); (c) the bodies responsible for ensuring that the person identification data is associated with the Wallet in accordance with Article 6a(4)(e); (d) the mechanism allowing for the validation of the person identification data referred to in 6a(4)(e) and of the identity of the relying parties. (e) the mechanism to validate the authenticity and validity of the European Digital Identity Wallets. The Commission shall make available to the public, through a secure channel, the information referred in this paragraph in electronically signed or sealed form suitable for automated processing.	No direct impact on ERDS framework of standards.
84	AT 6a	Article 6a: European Digital Identity Wallets 8. Article 11 shall apply mutatis mutandis to the European Digital Identity Wallet without prejudice to Art. 6a(10a).	Article 11 is about Liability of EU DI Wallet. Assess whether a reference to liability of EU DI Wallet should appear in the policy documents.
85	AT 6a	Article 6a: European Digital Identity Wallets 9. Article 24(2), points (b), (d) (e), (f), (fa), (fb), (g), and (h) shall apply mutatis mutandis to Member States issuing the European Digital Identity Wallets.	About article 24 which suffers changes. See discussions and potential actions in the corresponding rows.
86	AT 6a	Article 6a: European Digital Identity Wallets 10. The European Digital Identity Wallet shall be made accessible for use, in accordance with Directive 2019/882, by persons with disabilities, on an equal basis with other users.	Persons with disabilities Check whether mention to persons with disabilities is present in the policy documents; if not, assess whether they should include requirements related to them.
87		Article 6a: European Digital Identity Wallets 10a For the purposes of the provision of the EUDIW, the EUDIW and the electronic identification schemes under which they are provided shall not be subject to the requirements referred to in Articles 7, 9, 10, 12 and 12a.	Requirements on EUDIW and the electronic identification schemes Assess implications, especially regarding EUDIW.
88	AT 6a	Article 6a: European Digital Identity Wallets 11. By 6 months after the date of the entering into force of this amending Regulation, the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for the requirements referred to in paragraphs 3, 4 5 and 7c on the implementation of the European Digital Identity Wallet. These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Reference to technical specifications on EU DI Wallet Identify the places where specific references have to be made within the policy documents and technical specifications.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
89	AT 6a	Article 6a: European Digital Identity Wallets 11a. The Commission shall reference standards and when necessary establish technical and operational specifications in order to facilitate the on-boarding to the European Digital Identity Wallet of users using either electronic identification means conforming to level 'high' or electronic identification means conforming to level 'substantial' in conjunction with additional remote on-boarding procedures that together meet the requirements of level of assurance 'high'. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Reference standards and specifications on on-boarding to the EUDIW No direct impact on the ERDS/REM standards framework.
90	AT 6b	**Article 6b European Digital Identity Wallets Relying Parties**	Definition in eIDAS [i.1] not changed. (6) 'relying party' means a natural or legal person that relies upon an electronic identification or a trust service.
91	AT 6b	Article 6b: European Digital Identity Wallets Relying Parties 1. Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services it shall register in the Member state where the relying party is stablished.	Obligation to register in the EU MS New requirements in the policy documents.
92		Article 6b: European Digital Identity Wallets Relying Parties 1a The registration process shall be cost-effective and proportionate-to-risk. Relying parties shall provide at least: a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes: i) the Member State in which they are established; and ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record; b) contact details; c) the intended use of the European Digital Identity Wallet, including the data to be requested.	Requirements for the registration process
93		Article 6b: European Digital Identity Wallets Relying Parties 1c Relying parties shall not request any data beyond what they have registered for according to paragraphs 1 and 1a.	Requirement on what a relying party may request Impact on policy docs and maybe for technical docs. As there will be some standard on relying parties, reference in technical docs this standard.
94		Article 6b: European Digital Identity Wallets Relying Parties 1d Paragraphs 1 and 1a shall be without prejudice to requirements in accordance with Union or national law, applicable for the provision of specific services.	Potential Union or national law Impact on policy documents
95		Article 6b: European Digital Identity Wallets Relying Parties 1e Member States shall make the information referred to in paragraph 1a publicly available online in electronically signed or sealed form suitable for automated processing.	Requirement for EU MS: Lists of EUDI Wallets registry If ERDS need to interact with Relying Parties, then the ERDS will make use of this list. Impact in policy and technical documents.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
96		Article 6b: European Digital Identity Wallets Relying Parties 1g Relying parties registered in accordance with this Article shall inform Member States without delay about any changes in to the information provided.	Requirement on Relying parties
			Impact on policy documents.
97		Article 6b: European Digital Identity Wallets Relying Parties 2 Member States shall provide a common mechanism for allowing the identification and authentication of relying parties, as referred to in Article 6a(4)(ba) [GA].	ERDS/REM will use this common mechanism for authentication.
			New requirement in policy document. Assess whether this mechanism will also play some role in the technical specifications.
98		Article 6b: European Digital Identity Wallets Relying Parties 2a Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall identify themselves to the user of the European Digital Identity Wallet.	Requirement for ERDS/REM service
			Assess impact on policy/technical documents
99		Article 6b: European Digital Identity Wallets Relying Parties 3 Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets. Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.	Not refusal of pseudonyms wherever is allowed
			Impact on policy and technical documents
100		Article 6b: European Digital Identity Wallets Relying Parties 3a Intermediaries acting on behalf of relying parties are to be considered relying parties and shall not store data about the content of the transaction.	No direct impact on ERDS framework: whatever it is required for relying parties, will be required to intermediaries.
101	AT 6b	Article 6b: European Digital Identity Wallets Relying Parties 4. By ... [6 months after the date of the entering into force of this amending Regulation], the Commission shall establish technical and operational specifications for the requirements referred to in paragraphs 1a, 1e, 1g, 2, 2a and 3 by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11). This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).	There will be technical and operational specs for the mechanisms for authentication and the communication by ERDS/REM providers of their intention of using EU DI Wallets.
			Assess where the specific mentions to these Technical and Operational specs have to appear, policy documents (and if worth, within technical specs). Ensure that references to these documents are present wherever the mechanisms and communication means are explicitly mentioned.
102	AT 6c	**Article 6c Certification of the European Digital Identity Wallets**	Requirements for certifying the EU DI Wallets. Apart from requiring the usage of certified EU DI Wallets, it does not seem that this article can bring additional requirements/objects to ERDS/REM standards
			Ensure that the policy documents require the usage of certified EU DI Wallets.
103	AT 6c	Article 6c Certification of the European Digital Identity Wallets 1. The conformity of European Digital Identity Wallets and of the electronic identification scheme under which they are provided with the requirements laid down in Article 6a(3), (4), (5), with the requirement for logical separation laid down Article 6a(7) and, where applicable, in accordance with standards and technical specifications referred to in Article 6a(11a), shall be certified by conformity assessment bodies designated by Member States.	No requirements for ERDS/REM

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
104	AT 6c	Article 6c Certification of the European Digital Identity Wallets 2. Certification of the conformity of European Digital Identity Wallets with cybersecurity relevant requirements referred to in paragraph 1, or parts thereof, shall be carried out in accordance with cybersecurity schemes adopted pursuant to Regulation (EU) 2019/881 and referenced in the implementing acts referred to in paragraph 4.	No requirements for ERDS/REM
105	AT 6c	Article 6c Certification of the European Digital Identity Wallets 2a. For those non-cybersecurity requirements referred to in paragraph1 and, for as long as cybersecurity certification schemes referred to in paragraph 2 do not or do not fully cover the relevant cybersecurity requirements, for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 4. Member States shall transmit their draft national certification schemes to the EDICG, which may issue opinions and recommendations.	No requirements for ERDS/REM
106	AT 6c	Article 6c Certification of the European Digital Identity Wallets 2b. The certification referred to in paragraph 1 shall be valid for not more than five years, conditional upon a regular two-year vulnerabilities assessment.	No direct impact on ERDS
107	AT 6c	Article 6c Certification of the European Digital Identity Wallets 3. Compliance with the requirements set out in Article 6a related to the personal data processing operations may be certified pursuant to Regulation (EU) 2016/679.	No requirement for ERDS/REM
108	AT 6c	Article 6c Certification of the European Digital Identity Wallets 4. By ... [6 months after the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary establish specifications and procedures for the certification of the European Digital Identity Wallets referred to in paragraph 1 to 2a. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2) of this Regulation.	No requirement for ERDS/REM
109	AT 6d	**Article 6d Publication of a list of certified European Digital Identity Wallets**	
110	AT 6d	Article 6d Publication of a list of certified European Digital Identity Wallets 1. Member States shall inform the Commission and the EDICG referred to in Art.46e without undue delay of the European Digital Identity Wallets that have been provided pursuant to Article 6a and certified by the conformity assessment bodies referred to in Article 6c paragraph 1. They shall also inform the Commission and the EDICG referred to in Art.46e, without undue delay where the certification is cancelled and state the reasons for such cancellation.	This is a requirement for EUMS. It seems that it does not directly impact the policy documents.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
111		Article 6d Publication of a list of certified European Digital Identity Wallets 1a Without prejudice to Art.6a(7c), the information provided by Member States referred to in paragraph 1 shall include at least: a) the certificate and certification assessment report of the certified EUDIW; b) a description of the electronic identification scheme under which the EUDIW is provided; c) the applicable supervisory regime and information on the liability regime with respect to the party providing the EUDIW; d) the authority or authorities responsible for the electronic identification scheme; e) arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.	This is a requirement for EUMS. It seems that it does not directly impact the policy documents.
112	AT 6d	Article 6d Publication of a list of certified European Digital Identity Wallets 2. On the basis of the information received, the Commission shall establish, publish, maintain and update in a machine-readable form a list of certified European Digital Identity Wallets.	This list should be standardized. And in addition, this list should play a role during the process of verification of EUDI Wallets.
			Include within the policy reference to the processing of this list in the context of usage of EU DI Wallet in ERDS/REM. Assess whether ERDS/REM technical specs will also need to make a reference to this list.
113		Article 6d Publication of a list of certified European Digital Identity Wallets 2a. A Member State may submit to the Commission a request to remove an EUDIW and the electronic identification scheme under which it is provided from the list referred to in paragraph 2. A Member State shall submit updates to the provided information referred to in paragraph 1. The Commission shall publish in the list referred to in paragraph 2 the corresponding amendments to the list within one month from the date of receipt of the Member State's request or updated information.	These are requirements for EUMS and the Commission. It seems that they do not directly impact the policy documents.
114	AT 6d	Article 6d Publication of a list of certified European Digital Identity Wallets 3. By… 6 months after the date of entry into force of this amending Regulation, the Commission shall define formats and procedures applicable for the purposes of paragraph 1 and 2a by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11). This implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	The legal framework will refer to some technical specs.
			Include these references in the policy documents and in the technical specifications, if explicit mentions to the list are also done there.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
115		**Article 6da Security breach of the European Digital Identity Wallets**	
116		Article 6da Security breach of the European Digital Identity Wallets 1. Where European Digital Identity Wallets provided pursuant to Article 6a or the validation mechanisms referred to in Article 6a(5), or the electronic identification scheme under which the wallets are provided, are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the providing Member State shall, without undue delay, suspend the provision and the use of the European Digital Identity Wallet. The Member States where concerned Wallets were provided shall inform the affected users, the single points of contact designated pursuant to Article 46c, the relying parties and the Commission accordingly.	Requirements for EUDI Wallet. No direct impact on ERDS standards
117		Article 6da Security breach of the European Digital Identity Wallets 2. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension, the Member State concerned shall withdraw the European Digital Identity Wallets concerned and have their validity revoked. Member States concerned shall inform the affected users, the single points of contact designated pursuant to Article 46c, the relying parties and the Commission of the withdrawal accordingly. Where it is justified by the severity of the breach, the European Digital Identity Wallet concerned shall be withdrawn without undue delay.	Requirement for EUMS Policy documents and technical specifications should take into consideration that EUDI Wallets can be revoked and withdrawn.
118		Article 6da Security breach of the European Digital Identity Wallets 3. Where the breach or compromise referred to in paragraph 1 is remedied, the providing Member State shall re-establish the issuance and the use of the European Digital Identity Wallets and inform the affected users and relying parties, the single points of contact designated pursuant to Article 46c and the Commission without undue delay.	Requirement for EUMS Policy documents and technical specifications should take into consideration that EUDI Wallets can be re-established.
119		Article 6da Security breach of the European Digital Identity Wallets 4. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 6d without undue delay.	Requirement for EC. No impact on policy documents Assess whether this link between the changes in the status of EU DI Wallet with this list, should be mentioned in policy documents.
120		Article 6da Security breach of the European Digital Identity Wallets By ... [6 months after the entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish the reference standards and when necessary, establish specifications and procedures for the measures referred to in paragraphs 1, 2 and 3. These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts Assess whether this impacts in the policy documents.
121		**Article 6db Cross-border reliance on European Digital Identity Wallets**	
122		Article 6db Cross-border reliance on European Digital Identity Wallets 1. Where Member States require an electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets provided in accordance with this Regulation.	Requirement for Trusted services provided by public sector bodies Insert requirement ERDS/REMS provided by public sector bodies in the policy documents.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
123		Article 6db Cross-border reliance on European Digital Identity Wallets 2. Where private relying parties providing services, with the exception of microenterprises and small enterprises as defined in Commission Recommendation 2003/361/EC, are required by national or Union law to use strong user authentication for online identification or where strong user authentication for(8), (9a), (9b) online identification is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall, no later than 36 months after the entry into force of the implementing acts referred to in [Article 6a] paragraph 11 and Article 6c(4)] and strictly upon voluntary request of the user, also accept the use of European Digital Identity Wallets provided in accordance with this Regulation.	Requirement for services provided by private parties identified in this bullet Insert requirement ERDS/REMS provided by these entities in the policy documents.
124		Article 6db Cross-border reliance on European Digital Identity Wallets 3. Where providers of very large online platforms as referred to in Article 33 of Regulation (EU) 2022/2065 require users to authenticate to access online services, they shall also accept and facilitate the use of European Digital Identity Wallets provided in accordance with this Regulation, for authentication of the user strictly upon voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested.	Requirement for very large online platforms The policy documents should take into account this.
125		Article 6db Cross-border reliance on European Digital Identity Wallets 4. In cooperation with Member states, the Commission shall facilitate the development of codes of conduct in close collaboration with all relevant stakeholders, including civil society, in order to contribute to wide availability and usability of European Digital Identity Wallets within the scope of this Regulation, and to encourage service providers to complete the development of codes of conduct.	Development of codes of conduct Assess whether the development of these codes of conduct would impact the policy documents (f.i. requirement of having them).
126		Article 6db Cross-border reliance on European Digital Identity Wallets 5. Within 24 months after deployment of the European Digital Identity Wallets, the Commission shall carry out an assessment on demand, availability and usability of the European Digital Identity Wallets, considering criteria such as users' take up, cross-border presence of service providers, technological developments, evolution in usage patterns and consumer demand.	Requirement for the EC It seems that this does not affect ERDS/REMS standards framework.
127		**Article 7 Eligibility for notification of electronic identification schemes CHANGES**	
128	AT 7	Article 7 Eligibility for notification of electronic identification schemes Point (g) replaced by (g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(6).	This does not seem to directly impact ERDS/REM standards.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
129		**Article 8 Assurance levels of electronic identification schemes** **CHANGES**	
130		Article 8 Assurance levels of electronic identification schemes paragraph 3, the introductory paragraph is replaced by the following: 3. By 18 September 2025, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means.	Implementing act setting out standards, specs and procedures for assurance levels.
131		**Article 9 Notification** **CHANGES**	
132		Article 9 Notification paragraphs 2 and 3 are replaced by the following: 2. The Commission shall, without undue delay, publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.	Requirement for the EC. No direct impact on ERDS standards framework
133	AT 9	Article 9 Notification paragraphs 2 and 3 are replaced by the following: 3. The Commission shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within one month from the date of receipt of that notification.	Requirement for the EC. No direct impact on ERDS standards framework
134	AT 10	**Article 10 Security breach of the electronic identification schemes**	
135		**Article 11a Cross-border identity matching**	
136		Article 11a Cross-border identity matching 1. Member States, when acting as relying parties for cross-border services shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets.	Requirement on EUMS
			Impact on ERDS/REM: maybe a note mentioning that, within the EU, the EU MS will always assume that EU MS are ensuring unique identification. Requirements in policy documents differentiating between EU and non-EU contexts. Impact on technical documents EU vs non-EU.
137		Article 11a Cross-border identity matching 2b. Member States shall provide for technical and organisational measures to ensure high level of protection of personal data used for identity matching and to prevent the profiling of users.	Requirement on EUMS
			In a previous version of Article 11a, there was a bullet 2 which mentioned that among the minimum set of person identification data there was "a unique and persistent identifier in conformity with Union law, to identify the user upon their request in those cases where identification of the user is required by law" This has been dropped. Anyway, if such identifier is at the end one of the technical measures, it could have an impact on ERDS/REM where EUDIW is used for authentication.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
138		Article 11a Cross-border identity matching 3. By ... [6 months after the date of entry into force of this amending Regulation], the Commission shall establish the reference standards and when necessary, establish specifications and procedures for the requirements referred to in paragraph 1 by means of an implementing act. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing act for requirements on EUMSs
			ERDS/REM will refer to these specs in both policy documents and technical specs.
139	AT 12	**Article 12 Interoperability**	
140	AT 12	Article 12 Interoperability In paragraph 3, points (c) is replaced by the following: (c) it facilitates the implementation of privacy and security by design.	Requirement on the framework of the national electronic identification schemes
			It does not seem to have a direct impact on the ERDS/REM standards. Review whether the deleted points had an impact in the ERDS/REM framework and if so, assess what impact has their dropping for the new framework.
141		Article 12 Interoperability In paragraph 3, point (d) is deleted	It was a requirement on the processing of personal data according to Directive 95/46/EC [i.35].
			Assess whether there is a mention to this directive or this requirement in the ERDS/REM policy documents. If so, delete it.
142	AT 12	Article 12 Interoperability In paragraph 4, point (d) is replaced by the following: (d) a reference to a minimum set of person identification data necessary to uniquely represent a natural person, legal person or a natural person representing natural or legal persons which is available from electronic identification schemes.	
			Potential impact in policy and technical documents. At least because it differentiates different types of persons.
143		Article 12 Interoperability paragraph 5 is replaced by the following: (5) Member States shall carry out peer reviews of electronic identification schemes falling under this Regulation, to be notified pursuant to Article 9(1).	Requirement on EUMSs
			It seems that this does not impact the ERDS/REM standards framework.
144	AT 12	Article 12 Interoperability paragraph 6 is replaced by the following (6) By 18 March 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements for the peer reviews referred to in paragraph 5 with a view to fostering a high level of trust and security appropriate to the degree of risk.	Requirement for EU MSs
			No direct impact on the ERDS/REM standards
145		Article 12 Interoperability paragraph 7 is deleted;	Requirement for EC of an implementing act (replaced by the new paragraph 6)
			No impact the ERDS/REM standards framework
146		Article 12 Interoperability By 18 September 2025, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4.	Implementing acts on the interoperability framework
			Assess whether reference to be added in policy/technical docs.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
147		Article 12 Interoperability paragraph 9 is replaced by the following: (9) The implementing acts referred to in paragraphs 6 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Requirement on how to adopt the implementing acts It seems that this does not impact the ERDS/REM standards framework.
148	AT 12a	**Article 12a Certification of electronic identification schemes**	
149	AT 12a	Article 12a Certification of electronic identification schemes 1. The conformity of notified electronic identification schemes to be notified with cybersecurity requirements laid down in this Regulation shall be certified by conformity assessment bodies designated by Member States.	Requirements for electronic identification schemes to be certified It seems that this does not impact the ERDS/REM standards framework.
150	AT 12a	Article 12a Certification of electronic identification schemes 2. Certification referred to in paragraph 1 including the conformity with cybersecurity relevant requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes shall be carried out under a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 or parts thereof, in so far as the cybersecurity certificate or parts thereof cover those cybersecurity requirements.	Requirements on the certification process No direct impact on ERDS/REM standards
151		Article 12a Certification of electronic identification schemes 2a. The certification referred to in paragraph 1 shall be valid for not more than five years, conditional upon a regular two-year vulnerabilities assessment. Where vulnerabilities are identified and not remedied within three months, the certification shall be cancelled.	Requirements on the certification No direct impact on ERDS/REM standards
152		Article 12a Certification of electronic identification schemes 2b. Notwithstanding paragraph 2 of this Article, Member States may request additional information about electronic identification schemes or part thereof certified according to paragraph 2 of this Article from a notifying Member State.	Option for EUMSs to request additional information on the electronic identification schemes. No direct impact on ERDS/REM standards
153		Article 12a Certification of electronic identification schemes 2c. The peer-review of electronic identification schemes referred to in paragraph 5.c of Article 46e shall not apply to electronic identification schemes or part of such schemes certified in accordance with paragraph 1 of this Article. Member States may use a certificate or a statement of conformity, issued in accordance with a relevant certification scheme or parts of such schemes, with the non-cybersecurity requirements set out in Article 8(2) of this Regulation regarding the assurance levels of electronic identification schemes.	No peer-review of EUMS It seems that this does not impact the ERDS/REM standards framework.
154	AT 12a	Article 12a Certification of electronic identification schemes 3. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to Member States.	Obligation of EUMS No direct impact to ERDS/REM standards.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
155		**Article 12 b Access to hardware and software features** When providers of European Digital Identity Wallets and issuers of notified electronic identification means acting in a commercial or professional capacity and using core platform services as defined in Article 2(2) of Regulation (EU) 2022/1925 for the purpose of, or in the course of, providing European Digital Identity Wallet services and electronic identification means to end-users are business users in accordance with Article 2(21) of Regulation (EU) 2022/1925, gatekeepers shall allow them, free of charge, effective interoperability with, and access for the purposes of interoperability to the same operating system, hardware or software features, regardless of whether those features are part of the operating system, as (17) are available to, or used by, that gatekeeper when providing such services, within the meaning of Article 6(7) of Regulation (EU) 2022/1925. This provision is without prejudice to Article 6a(7).	Requirements for providers
			It seems that this does not impact ERDS/REM standards framework.
156		**Article 13 Liability and burden of proof**	
157	AT 13	Article 13 Liability and burden of proof Paragraph 1 is replaced by the following: 1. Notwithstanding paragraph 2 of this Article and without prejudice to Regulation (EU) 2016/679, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation. Any natural or legal person who has suffered material or non-material damage as result of an infringement of this Regulation by trust service providers shall have the right to seek compensation in accordance with Union and national law. The burden of proving intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph. The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.	Requirement for any TSP
			To ensure that this will be captured in the Policy documents.
158	AT 14	**Article 14 International aspects**	
159	AT 14	Article 14 International aspects 1. Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country or international organisation are recognised under an implementing decision or an agreement concluded between the Union and the third country or international organisation in accordance with Article 218 of the Treaty.	
			To ensure that the policy documents include the requirement of considering QERDS a third country service that meets the requirements mentioned in this bullet.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
160	AT 14	Article 14 International aspects 2. The implementing decisions and agreements referred to in paragraph 1 shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations and by the trust services they provide. Third countries and international organisations shall in particular establish, maintain and publish a trusted list of recognised trust service providers.	Requirements on the implementing decisions. Requirement on trusted lists To ensure that the policy documents mention, at least, these third countries trusted lists.
161		Article 14 International aspects (2a) The agreements referred to in paragraph 1 shall ensure that the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded.	EU TSP to be recognized in third countries Add note(s) in the policy documents making reference to this.
162		Article 14 International aspects 2b. The implementing decisions referred to in paragraph 1 shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Requirement on adoption of the implementing decisions No direct impact on the ERDS/REM standards framework
163	AT 15	**Article 15 Accessibility for persons with disabilities and special needs**	
164	AT 15	Article 15 is replaced by the following text: The provision of electronic identification means, trust services and end-user products used in the provision of those services shall be available in plain and intelligible language and in accordance with the United Nations Convention on the Rights of Persons with Disabilities. Further, alignment with the requirements set out in Annex I of Directive (EU) 2019/8821, should also benefit persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies.	Check whether this is covered within the Policy documents somehow.
165		**Article 16 Penalties**	
166		Article 16 Penalties 1. Without prejudice to Article 31 of the Directive (EU) 2022/2555 , Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties shall be effective, proportionate and dissuasive.	Requirement for EUMSs Reference in the policy documents to these rules established by EUMSs.
167		Article 16 Penalties 2. Member States shall ensure that infringements by qualified and non-qualified trust service providers of the obligations of this Regulation be subject to administrative fines of a maximum of at least EUR 5,000,000 when the trust service provider is a natural persons or EUR 5,000,000 or 1 % of the total worldwide annual turnover of the undertaking to which the trust service provider belonged in the financial year preceding the year in which the infringement occurred, whichever is higher.	Obligations of EUMSs Add note(s) in the policy documents making reference to this.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
168		Article 16 Penalties 3. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts. The application of such rules in those Member States shall ensure that those legal remedies are effective and have an equivalent effect to administrative fines imposed directly by supervisory authorities.	Procedures for application of fines It seems that this does not have a direct impact on ERDS/REM standards framework.
169	AT 17	Articles 17 Supervisory body, 18 Mutual assistance, and 19 Security requirements applicable to trust service providers **are deleted**	At least 19 dealing with requirements applicable to TSPs is relevant. Articles 17 and 18 did not seem to impact on ERDS/REM standards framework as they contained rules applicable to supervisory bodies. Article 19, though, defined security requirements for TSPs. Therefore, the policy documents will be reviewed in the light of its deletion. Also, assess whether this deletion also impacts some technical document.
170		**Article 19a Requirements for non-qualified trust service providers**	
171		Article 19a Requirements for non-qualified trust service providers 1. A non-qualified trust service provider providing non-qualified trust services shall: (a) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the non-qualified trust service. Notwithstanding the provisions of Article 18 of Directive EU 2022/2555, those measures shall include at least the following: (i) measures related to registration and on-boarding procedures to a trust service; (ii) measures related to procedural or administrative checks needed to provide trust services; (iii) measures related to the management and implementation of trust services.	Non-qualified TSPs Impact on policy documents. Applicable to Non-qualified ERDS/REM services. Some requirements will be defined for any type of non-qualified any TSP and in the ERDS policy documents a reference has to be inserted to this any-Non-Qualified-TSP-applicable document.
172		Article 19a Requirements for non-qualified trust service providers 1. A non-qualified trust service provider providing non-qualified trust services shall: b) notify the supervisory body, the identifiable affected individuals, the public if it is of public interest and, where applicable, other relevant competent authorities, of any breaches or disruptions in the provision of the service or the implementation of the measures referred to in paragraph (a), points (i), (ii) and (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours after having become aware of any breaches or disruptions.	Non-qualified TSPs Some requirements will be defined for any type of non-qualified any TSP and in the ERDS policy documents a reference has to be inserted to this any-Non-Qualified-TSP-applicable document.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
173		Article 19a Requirements for non-qualified trust service providers 2. By [12 months after the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards, and when necessary, establish specifications and procedures for paragraph 1(a). Compliance with the requirements laid down in this Article shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts If ENs defining common requirements for non-qualified TSPs are referenced in the implementing acts, they should also be referenced in the ERDS/REM policy documents.
174	AT 17	Article 17-4.(c) (a) paragraph 4 is amended as follows: (1) point (c) of paragraph 4 is replaced by the following: (c) to inform the relevant national competent authorities of the Member States concerned, designated pursuant to Directive (EU) XXXX/XXXX [NIS2], of any significant breaches of security or loss of integrity they become aware of in the performance of their tasks. where the significant breach of security or loss of integrity concerns other Member States, the supervisory body shall inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX (NIS2).	Ensure that the policy documents incorporate this requirement and its procedure.
175		**Article 20 Supervision of qualified trust service providers** Article 20 is amended as follows:	
176	AT 20	Article 20 Supervision of qualified trust service providers (a) paragraph 1 is replaced by the following: 1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. the audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555. qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.	Requirement for TSPs ERDS/REM policy documents for eIDAS-TSPs will directly or indirectly (by reference to another EN including requirements for any eIDAS-TSP) incorporate: The auditing requirement. The submission of the conformity assessment report to the supervisory body (qualified TSPs).
177		Article 20 Supervision of qualified trust service providers (aa) the following paragraphs 1a and 1b are inserted: 1a. Qualified trust service providers shall inform the supervisory body at the latest one month in advance about planned audits and allow for the participation of the supervisory body as an observer upon request.	Requirement for QTSPs This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
178		Article 20 Supervision of qualified trust service providers 1b. Member States shall notify, without undue delay, to the Commission the names, addresses and accreditation details of the conformity assessment bodies referred to in paragraph 1 and any subsequent changes thereto. The Commission shall make that information available to all Member States.	Requirements for EUMSs It seems that this does not directly impact ERDS/REM standards framework.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
179		Article 20 Supervision of qualified trust service providers (b) in paragraph 2, the last sentence is replaced by the following: Where personal data protection rules appear to have been breached, the supervisory body shall, without undue delay, inform the competent supervisory authorities under Regulation (EU) 2016/679.	Rule for supervisory bodies It seems that this does not directly impact ERDS/REM standards framework.
180		Article 20 Supervision of qualified trust service providers c) paragraph 3 is replaced by the following: 3. Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable. Where that provider does not provide a remedy and, where applicable within the time limit set by the supervisory body, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.	Rule for QTSPs This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
181		Article 20 Supervision of qualified trust service providers c) paragraph 3 is replaced by the following: 3a. Where the supervisory body is informed by the national competent authorities under Directive (EU) 2022/2555 that the qualified trust service provider fails to fulfil any of the requirements set out by Article 21 of Directive (EU) 2022/2555, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.	Rule for supervisory body It seems that this does not directly impact ERDS/REM standards framework.
182		Article 20 Supervision of qualified trust service providers c) paragraph 3 is replaced by the following: 3b. Where the supervisory body is informed by the supervisory authorities under Regulation (EU) 2016/679 that the qualified trust service provider fails to fulfil any of the requirements set out by Regulation (EU) 2016/679. The supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.	Rule for supervisory body It seems that this does not directly impact ERDS/REM standards framework.
183		Article 20 Supervision of qualified trust service providers c) paragraph 3 is replaced by the following: 3c. The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned. The supervisory body shall inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1) and the national competent authority referred to in Directive (EU) 2022/2555.	Rule for supervisory body It seems that this does not directly impact ERDS/REM standards framework.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
184		Article 20 Supervision of qualified trust service providers c) paragraph 4 is replaced by the following: 4. By ... [12 months after the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for the following: (a) the accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1; (b) the auditing requirements for the conformity assessment bodies to carry out their conformity assessment, including composite assessment, of the qualified trust service providers as referred to in paragraph 1; (c) the conformity assessment schemes for carrying out the conformity assessment of the qualified trust service providers by the conformity assessment bodies and for the provision of the report referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts controlling the setting up of conformity assessment bodies and their work. It seems that this does not directly impact ERDS/REM standards framework.
185		Article 21 Initiation of a qualified trust service Article 21 is amended as follows:	
186		Article 21 Initiation of a qualified trust service (a) paragraph 1 is replaced by the following: 1. Where trust service providers intend to start providing a qualified trust service, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body confirming the fulfilment of the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555.	Rule for any QTSP This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
187	AT 21	Article 21 Initiation of a qualified trust service (b) paragraph 2 is replaced by the following: 2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, and in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide. In order to verify the compliance of the trust service provider with the requirements laid down in Article 21 of Directive (EU) 2022/2555, the supervisory body shall request the competent authorities referred to in Directive (EU) 2022/2555 to carry out supervisory actions in that regard and to provide information about the outcome without undue delay, and no later than two months from the receipt of this request by the competent authorities referred to in Directive (EU) 2022/2555. If the verification is not concluded within two months of the notification, the competent authorities referred to in Directive (EU) 2022/2555 shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded. Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article. Where the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.	Requirements for Supervisory Bodies It seems that this does not directly impact ERDS/REM standards framework.
188	AT 21	Article 21 Initiation of a qualified trust service (c) paragraph 4 is replaced by the following: 4. By 12 months after the date of entering into force of this amending Regulation, the Commission shall, by means of implementing acts, define the formats and procedures of the notification and verification for the purposes of paragraphs 1 and 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts affecting paragraphs 1 and 2 Requirements on the formats and procedures related to paragraph 1 are likely to be captured into the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
189		**Article 24 Requirements for qualified trust service providers** **Article 24 is amended as follows:**	
190	AT 24	Article 24 Requirements for qualified trust service providers (a) paragraph 1 is replaced by the following: 1. When issuing a qualified certificate or a qualified electronic attestation of attributes for a trust service, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attributes will be issued. The verification of the identity referred to in the first subparagraph shall be verified, by appropriate means, by the qualified trust service provider, either directly or by relying on a third party, based on one of the following methods or a combination thereof when needed, and in accordance with the implementing acts referred in paragraph 1a: (a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance level 'high'; (b) by means of qualified electronic attestations of attributes or a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a), (c) or (d); (c) by using other identification methods which ensure the identification of the natural person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body; (d) through the physical presence of the natural person or of an authorised representative of the legal person by appropriate procedures and in accordance with national laws if other means are not available.'; (da) The verification of the attributes referred to in the first subparagraph shall be verified, by appropriate means, by the qualified trust service provider, either directly or by relying on a third party, based on one of the following methods or on a combination thereof when needed, and in accordance with the implementing acts referred to in paragraph 1a: (i) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance level 'high'; (ii) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a), (c) or (d); (iii) by means of a qualified electronic attestation of attributes; (iv) by using other methods, which ensure the verification of the attributes with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body; (v) through the physical presence of the natural person or of an authorised representative of the legal person by appropriate [evidences,] procedures and in accordance with national laws.'	This seems to be a requirement for issuers of QC or QEAAs. This seems to be requirements for BEFORE ERDS enters into play.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
191	AT 24	Article 24 Requirements for qualified trust service providers (b) the following paragraph is inserted: 1a. By 12 months after the date of entry into force of this amending Regulation, the Commission shall by means of implementing acts, establish a list of reference standards and when necessary, establish technical specifications and procedures for the verification of identity and attributes in accordance with paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	As this references the paragraph 1, it again seems to apply to QC and QEAA issuers.
192		Article 24 Requirements for qualified trust service providers c) paragraph 2 is amended as follows: (-1) point (a) is replaced by the following: (a) inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities. The supervisory body may request additional information or the result of a conformity assessment and may condition the granting of the permission to implement the intended changes to the qualified trust services. If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider, specifying the reasons for the delay and the period within which the verification is to be concluded.	Rule for any QTSP
			This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
193	AT 24	Article 24 Requirements for qualified trust service providers (c) paragraph 2 is amended as follows: (1) point (d) is replaced by the following: (d) before entering into a contractual relationship, inform, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use.	Rule for any QTSP
			This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
194	AT 24	Article 24 Requirements for qualified trust service providers (c) paragraph 2 is amended as follows: (1) point (e) is replaced by the following: (e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic techniques.	Rule for any QTSP
			This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
195	AT 24	Article 24 Requirements for qualified trust service providers (2) the new points (fa) and (fb) are inserted: (fa) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the qualified trust service. Notwithstanding the provisions of Article 21 of Directive EU 2022/2555, those measures shall include at least the following: (i) measures related to registration and on-boarding procedures to a service. (ii) measures related to procedural or administrative checks. (iii) measures related to the management and implementation of services.	Rule for any QTSP
			This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
196	AT 24	Article 24 Requirements for qualified trust service providers (2) the new points (fa) and (fb) are inserted: (fb) notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any breaches or disruptions in the provision of the service or the implementation of the measures referred to in paragraph (fa), points (i), (ii) and, (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours after the incident.	Rule for any QTSP
			This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
197	AT 24	Article 24 Requirements for qualified trust service providers (3) point (g) and (h) are replaced by the following: (g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible.	Rule for any QTSP
			This is likely to be captured within the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
198	AT 24	Article 24 Requirements for qualified trust service providers (3) point (g) and (h) are replaced by the following: (h) record and keep accessible for as long as necessary after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;'	Rule for any QTSP
			This is likely to be captured in the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
199	AT 24	Article 24 Requirements for qualified trust service providers (3) point (g) and (h) are replaced by the following: (i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 46b(4).	Rule for any QTSP
			This is likely to be captured in the EN(s) defining policy requirements for any type of QTSP. ERDS/REM Policy documents will reference them.
200	AT 24	Article 24 Requirements for qualified trust service providers (4) point (j) is deleted	Affects any type of QTSP
			This deletion will likely be captured within the EN(s) defining policy requirements for any type of QTSP

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
			ERDS/REM Policy documents will reference them.
201	AT 24	Article 24 Requirements for qualified trust service providers (d) the following paragraph 4a is inserted: 4a. Paragraphs 3 and 4 shall apply accordingly to the revocation of qualified electronic attestations of attributes.	This affects services issuing QEAA.
			This does not seem to impact on ERDS/REM standards framework.
202	AT 24	Article 24 Requirements for qualified trust service providers (e) paragraph 5 is replaced by the following: 5. By 12 months after the date of entering into force of this amending Regulation, the Commission shall, by means of implementing acts, establish a list of reference standards and where necessary, establish specifications and procedures for the requirements referred to in paragraph 2(b) to (h) of this Article. Compliance with the requirements laid down in this paragraph of this Article shall be presumed, where those standards, specifications, and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts
			ERDS/REM Policy documents will reference them.
203	AT 24	Article 24 Requirements for qualified trust service providers (f) the following paragraph 6 is inserted: 6. The Commission shall be empowered to adopt delegated acts in accordance with Article 47, establishing additional measures referred to in paragraph 2(fa) of this Article.	Potential additional delegated acts affecting paragraph 2(fa).
			As this paragraph captures rules for any type of QTSP, any additional delegated act referring to it should impact the EN(s) capturing requirements for any type of QTSP. Ensure that the ERDS/REM policy documents reference these EN(s). Assess the suitability of some explicit reference to these potential delegated acts or to the additional measures.
204	AT 24a	**Article 24a Recognition of qualified trust services**	
205	AT 24a	Article 24a Recognition of qualified trust services 1. Qualified electronic signatures based on a qualified certificate created in one Member State, and qualified electronic seals based on a qualified certificate issued in one Member State, shall be recognised respectively as qualified electronic signatures and qualified electronic seals in all other Member States.	Recognition of QESigs and QESeals
			No direct impact on ERDS/REM standards framework.
206	AT 24a	Article 24a Recognition of qualified trust services 2. Qualified electronic signature creation devices certified in one Member State, and qualified electronic seal creation devices certified in one Member State, shall be recognised respectively as qualified electronic signature creation devices and qualified electronic seal creation devices in all other Member States.	Recognition of QESig and QESeal creation devices
			No direct impact on ERDS/REM standards framework.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
207	AT 24a	Article 24a Recognition of qualified trust services 3. A qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices, a qualified trust service for the management of remote qualified electronic seal creation devices, provided in one Member State shall be respectively recognised as a qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices, a qualified trust service for the management of remote qualified electronic seal creation devices in all other Member States.	Recognition of Qcerts, QTSPs related with the management of remote QESig and QESeal creation devices
			If this recognition impacts some ENs, this impact will be in those specifying policies for the aforementioned QTSPs types. ERDS/REM policy documents will incorporate them by referencing the former ENs when dealing with externalization of these services.
208	AT 24a	Article 24a Recognition of qualified trust services 4. A qualified validation service for qualified electronic signatures, a qualified validation service for qualified electronic seals provided in one Member State shall be respectively recognised as a qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals in all other Member States.	Recognition of QESig and QESeals validation services
			If this recognition impacts some ENs, this impact will be in those specifying policies for the aforementioned QTSPs types. ERDS/REM policy documents will incorporate them by referencing the former ENs when dealing with externalization of these services.
209	AT 24a	Article 24a Recognition of qualified trust services 5. A qualified preservation service for qualified electronic signatures, a qualified preservation service for qualified electronic seals provided in one Member State shall be respectively recognised as a qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals in all other Member States.	Recognition of preservation services for QESig and QESeals
			If this recognition impacts some ENs, this impact will be in those specifying policies for the aforementioned QTSPs types. ERDS/REM policy documents will incorporate them by referencing the former ENs when dealing with externalization of these services.
210	AT 24a	Article 24a Recognition of qualified trust services 6. A qualified electronic time stamp provided in one Member State shall be recognised as a qualified electronic time stamp in all other Member States.	Recognition of Q electronic time-stamp
			If this recognition impacts some ENs, this impact will be in those specifying policies for the aforementioned QTSPs types. ERDS/REM policy documents will incorporate them by referencing the former ENs when dealing with qualified time-stamp from other EUMSs.
211	AT 24a	Article 24a Recognition of qualified trust services 7. A qualified certificate for website authentication provided in one Member State shall be recognised as a qualified certificate for website authentication in all other Member States.	Recognition of Q certificates
			If this recognition impacts some ENs, this impact will be in those specifying policies for the aforementioned QTSPs types. ERDS/REM policy documents will incorporate them by referencing the former ENs when dealing with qualified certificates from other EUMSs.
212	AT 24a	Article 24a Recognition of qualified trust services 8. A qualified electronic registered delivery service provided in one Member State shall be recognised as a qualified electronic registered delivery service in all other Member States.	Recognition of a QERDS
			Ensure that this is captured in the policy documents dealing with QERDS.
213	AT 24a	Article 24a Recognition of qualified trust services 9. A qualified electronic attestation of attributes provided in one Member State shall be recognised as a qualified electronic attestation of attributes in all other Member States.	Recognition of QEAA
			If this recognition impacts some ENs, this impact will be in those specifying policies for the aforementioned QTSPs types. ERDS/REM policy documents will incorporate them by referencing the former ENs when dealing with QEAAs from other EUMSs (of special relevance in authentication). Assess impact in technical docs.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
214	AT 24a	Article 24a Recognition of qualified trust services 10. A qualified electronic archiving service provided in one Member State shall be recognised as a qualified electronic archiving service in all other Member States.	Recognition of qualified electronic archiving services If this recognition impacts some ENs, this impact will be in those specifying policies for the aforementioned QTSPs types. ERDS/REM policy documents will incorporate them by referencing the former ENs when dealing with externalization of these services.
215	AT 24a	Article 24a Recognition of qualified trust services 11. A qualified electronic ledger provided in one Member State shall be recognised as a qualified electronic ledger in all other Member States.'	Recognition of a qualified electronic ledger If this recognition impacts some ENs, this impact will be in those specifying policies for the aforementioned QTSPs types. ERDS/REM policy documents will incorporate them by referencing the former ENs when dealing with ledgers from other EUMSs.
216	AT 25	**Article 25 Legal effects of electronic signatures**	
217	AT 25	Article 25 Legal effects of electronic signatures Paragraph 3 is deleted.	Drop recognition of QES in other EUMS As this has been now moved to new Article 24a paragraph 1, considerations made there apply here.
218	AT 26	**Article 26 Requirements for advanced electronic signatures** Article 26 is amended as follows:	
219	AT 26	Article 26 Requirements for advanced electronic signatures 2. Within 24 months after the entry into force of this Regulation, the Commission shall carry out an assessment on whether it is necessary to adopt an implementing act, establishing a list of reference standards and when necessary, establishing specifications and procedures for advanced electronic signatures. Based on the outcome of this assessment, the Commission may adopt such an implementing act. Compliance with the requirements for advanced electronic signatures shall be presumed when an advanced electronic signature meets those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Potential implementing acts Potential impact on ERDS/REM policy standards. Assess potential impact on ERDS/REM technical docs.
220	AT 27	**Article 27 Electronic signatures in public services** Is deleted.	Assess whether this deletion has some impact on ERDS/REM standards framework.
221	AT 28	Article 28 Qualified certificates for electronic signatures	
222	AT 28	Article 28 Qualified certificates for electronic signatures Paragraph 6 is replaced by the following: 6. By 12 months after the date of the entering into force of this amending Regulation, the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	This is about QCs. It seems that it does not have a direct impact on ERDS/REM standards framework.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
223	1	**Article 29 Requirements for qualified electronic signature creation devices**	
224	2	Article 29 Requirements for qualified electronic signature creation devices The following new paragraph 1a is added: 1a. Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes may only be done on behalf of and at the request of the signatory by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.	As this is related to a new service, this will impact the policy documents. Ensure that this new type of service is taken into account in the policy documents.
225	3a	**Article 29a Requirements for a qualified service for the management of remote electronic signature creation devices**	
226	4a	Article 29a Requirements for a qualified service for the management of remote electronic signature creation devices 1. The management of remote qualified electronic signature creation devices as a qualified service may only be carried out by a qualified trust service provider that: (a) Generates or manages electronic signature creation data on behalf of the signatory. (b) Notwithstanding point (1)(d) of Annex II, may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: (i) the security of the duplicated datasets must be at the same level as for the original datasets. (ii) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service. (c) Complies with any requirements identified in the certification report of the specific remote qualified signature creation device issued pursuant to Article 30.	New service As before: ERDS/REM providers may externalize the management of signature creation devices.
227	AT 29a	Article 29a Requirements for a qualified service for the management of remote electronic signature creation devices 2. By 12 months after the entry into force of this amending Regulation, the Commission shall, by means of implementing acts, establish reference standards and, when necessary, technical and operational specifications for the purposes of paragraph 1. These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts on remote signature creation devices. ERDS/REM policy documents to reference the standards listed within the implementation acts in the policy documents.
228	AT 30	Article 30 Certification of qualified electronic signature creation devices	
229	AT 30	Article 30 Certification of qualified electronic signature creation devices The following paragraph 3a is inserted: 3a. The certification referred to in paragraph 1 shall be valid for 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be withdrawn.	As this is related to the former services, this also has to be taken into consideration. Assess whether it is required that ERDS/REM policy documents reference the certification of ES creation devices.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
230	AT 31	**Article 31 Publication of a list of certified qualified electronic signature creation devices**	
231	AT 31	Article 31 Publication of a list of certified qualified electronic signature creation devices Paragraph 3 is replaced by the following: 3. By 12 months after the date of entry into force of this amending Regulation, the Commission shall, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	As this article is about generating lists of certified qualified electronic signature creation devices, and these are used by services with which the QERDS Provider could contract services, this could have an impact. If ENs dealing with requirements for any QTSPs and TSPs include requirements mentioning these lists, and ERDS/REM policy documents reference the mentioned ENs, then this is covered. Otherwise mention this in the ERDS/REM policy documents.
232	AT 32	**Article 32 Requirements for the validation of qualified electronic signatures** Article 32 is amended as indicated in rows 234 and 235	
233	AT 32	Article 32 Requirements for the validation of qualified electronic signatures (a) in paragraph 1, the following sub-paragraph is added: 'Compliance with the requirements laid down in the first sub-paragraph shall be presumed where the validation of qualified electronic signatures meet the standards, specifications and procedures referred to in paragraph 3.'	Refers to validation of QESig It does not seem that this impacts the ERDS/REM standards framework.
234	AT 3232	Article 32 Requirements for the validation of qualified electronic signatures (b) paragraph 3 is replaced by the following: 3. By 12 months after the date of the entering into force of this amending Regulation, the Commission shall, by means of implementing acts, establish a list of reference of standards and when necessary, establish specifications and procedures for the validation of qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts on validation of QESig Assess if technical docs will have to refer to the standards, specs, and procedures when dealing with validation of QES.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
235	AT 32a	**Article 32a Requirements for the validation of advanced electronic signatures based on qualified certificates**	
236		Article 32a Requirements for the validation of advanced electronic signatures based on qualified certificates 1. The process for the validation of an advanced electronic signature based on qualified certificate shall confirm the validity of an advanced electronic signature based on qualified certificate provided that: (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I; (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing; (c) the signature validation data corresponds to the data provided to the relying party; (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party; (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing; (f) the integrity of the signed data has not been compromised; (g) the requirements provided for in Article 26 were met at the time of signing.	Rules for validating No direct impact on ERDS/REM standards framework.
237		Article 32a Requirements for the validation of advanced electronic signatures based on qualified certificates 2. The system used for validating the advanced electronic signature based on qualified certificate shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.	Rules for validating No direct impact on ERDS/REM standards framework.
238		Article 32a Requirements for the validation of advanced electronic signatures based on qualified certificates 3. By.... [12 months after the date of the entering into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for the validation of advanced electronic signatures based on qualified certificates. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of advanced electronic signature based on qualified certificates meets those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementation acts on validation Assess whether the technical documents need to reference the standards/specs/procedures listed in these implementing acts.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
239		**Article 33 Qualified validation service for qualified electronic signatures** Article 33 is amended as indicated in row 241	
240		Article 33 Qualified validation service for qualified electronic signatures 2. By.... [12 months after the date of the entering into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the qualified validation service for qualified electronic signatures meets those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts for standards/specs/procedures for qualified validation service ERDS/REM providers may externalize the service of validating qualified electronic signatures. ERDS/REM technical documents may refer to the standards/specs/procedures listed in the implementation acts.
241	AT 34	**Article 34 Qualified preservation service for qualified electronic signatures** Article 34 is replaced by the contents of rows 243, 244, and 245.	
242	AT 34	Article 34 Qualified preservation service for qualified electronic signatures 1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.	On QTSP for preservation of signatures Ensure that when mentioned in the policy documents the possibility of using this service, to include requirements satisfying this change.
243	AT 34	Article 34 Qualified preservation service for qualified electronic signatures 2. Compliance with the requirements laid down in the paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet the standards, specifications and procedures referred to in paragraph 3	On QTSP for preservation of signatures Ensure that when mentioned in the policy documents the possibility of using this service, to include requirements satisfying this change.
244	AT 34	Article 34 Qualified preservation service for qualified electronic signatures 3. By 12 months after the date of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for the qualified preservation service for qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to In Article 48(2).'	Implementation acts Ensure that ERDS/REM policy documents reference the standards/specs/procedures listed in the implementation acts when dealing with the externalization of. Preservation of QESig.
245		**Article 35 Legal effects of electronic seals**	
246		Article 35 Legal effects of electronic seals Paragraph 3 is deleted	On recognition of QESeal generated in one EUMS in another EUMS. This has already been taken into account in the new Article 24a.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
247		**Article 36 Requirements for advanced electronic seals** The new paragraph 2 in row 249, is added:	
248		Article 36 Requirements for advanced electronic seals 2. By... [24 months after the date of the entering into force of this amending Regulation], the Commission shall carry out an assessment on whether it is necessary to adopt an implementing act, establishing a list of reference standards and when necessary, establishing specifications and procedures for advanced electronic seals. Based on the outcome of this assessment, the Commission may adopt such an implementing act. Compliance with the requirements for advanced electronic seals shall be presumed when an advanced electronic seal meets those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing act on advanced electronic seals Assess impact on ERDS/REM standards framework of the creation of this implementing act.
249		**Article 37 Electronic seals in public services** Is amended as indicated in row 251	
250		Article 37 Electronic seals in public services Paragraph 4 is deleted	Paragraph on implementing acts deleted No special requirements for ESeals in public services. The requirements will be common for all ESeals regardless they are used in public services or non-public services. Likely, if the ENs specifying requirements for ESeals contained some reqs specific for ESeals in public services, they will be dropped.
251		**Article 38 Qualified certificates for electronic seals** Is amended as indicated in rows 253 and 254	
252	AT 38	Article 38 Qualified certificates for electronic seals (a) paragraph 1 is replaced by the following: 1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.	Article 38 is on QCs for electronic seals. Likely, these requirements will be met by the ENs specifying requirements for QCs for ESeals. ERDS/REM policy documents (assess also whether or not the technical documents) will incorporate them by reference to the former ENs if QESeals are required there.
253	AT 38	Article 38 Qualified certificates for electronic seals (b) paragraph 6 is replaced by the following: 6. By 12 months after the date of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts on QCs for ESeals Assess whether this has impact on ERDS/REM specs (QEseals usage).

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
254		**Article 39a Requirements for a qualified service for the management of remote qualified electronic seal creation devices**	
255	AT 39a	Article 39a Requirements for a qualified service for the management of remote electronic seal creation devices Article 29a shall apply mutatis mutandis to a qualified service for the management of remote qualified electronic seal creation devices.'	As for Qualified electronic signature creation devices.
			Same comments apply here as for Article 29a.
256		**Article 40a Requirements for the validation of advanced electronic seals based on qualified certificates**	
257		Article 40a Requirements for the validation of advanced electronic seals based on qualified certificates Article 32a shall apply mutatis mutandis to the validation of advanced electronic seals based on qualified certificates.	As for validation of advanced electronic signatures based on qualified certificates.
			Same comments apply here as for Article 32a.
258		**Article 41 Legal effect of electronic time stamps**	
259		Article 41 Legal effect of electronic time stamps Paragraph 3 is deleted.	Recognition of a qualified time stamp generated in one EUMS in another EUMS.
			This requirement has been incorporated in the new Article 24a.
260		**Article 42 Requirements for qualified electronic time stamps** Is amended as indicated in rows 262 and 263.	
261	AT 42	Article 42 Requirements for qualified electronic time stamps (a) the following new paragraph 1a is inserted: 1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accuracy of the time source meet the standards, specifications and procedures referred to in paragraph 2.'	Presumption of compliance if meeting the standards, specs and procedures listed in implementing acts.
			No impact on ERDS/REM standards framework
262	AT 42	Article 42 Requirements for qualified electronic time stamps (b) paragraph 2 is replaced by the following: 2. By 12 months after the date of the entering into force of this amending Regulation, the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for the binding of date and time to data and for establishing the accuracy of time sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts
			Ensure referencing the standards/specs/procedures listed in these implementing acts in the ERDS/REM policy and technical documents when referring to Qtime-stamps.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
263		**Article 44 Requirements for qualified electronic registered delivery services**	Being the article specifc to requirements for ERDS, it is completely copied below, not only the changes from eIDAS [i.1] to eIDAS 2.0 [i.2].
264	AT 44	Article 44 Requirements for qualified electronic registered delivery services 1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets the standards and specifications and procedures referred to in paragraph 2.	 It is intended that the ERDS/REM standards framework become the standards referred in the corresponding implementing acts of paragraph 2. Therefore, these standards will meet the requirements defined in this Article 44.
265		Article 44 Requirements for qualified electronic registered delivery services 1. Qualified electronic registered delivery services shall meet the following requirements: (a) they are provided by one or more qualified trust service provider(s); (b) they ensure with a high level of confidence the identification of the sender; (c) they ensure the identification of the addressee before the delivery of the data; (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp. In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.	Requirements for QERDS/QREM Ensure that the ERDS/REM standards meet all these requirements when dealing with QRERDS/QREM. Ensure that the use case of data being transferred between two or more QERDS is also covered.
266	AT 44	Article 44 Requirements for qualified electronic registered delivery services 2. By 12 months after the date of the entering into force of this amending Regulation, the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts The standards generated by ETSI TC ESI should be these standards. Ensure that they are compatible with/incorporate the specifications/procedures the EC could have in mind to list in the implementing acts.
267		Article 44 Requirements for qualified electronic registered delivery services 2a. Providers of qualified electronic registered delivery services may agree on the interoperability between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1. The compliance shall be confirmed by a conformity assessment body.	Provisions on interoperability of QERDS Ensure that the technical documents makes it possible interoperability. Policy documents will also incorporate some requirement for interoperability of at least QERDS: there is an auditing process by a conformity assessment body involved.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
268		Article 44 Requirements for qualified electronic registered delivery services (2b) The Commission may, by means of implementing acts, establish a list of reference standards and, when necessary, establish specifications and procedures for the interoperability framework referred to in paragraph 2a. The technical specifications and content of standards shall be cost-effective and proportionate. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	Implementing acts specific for interoperability
			The technical documents of ERDS/REM standards frameworks should be these standards. Ensure that they actually define a proper interoperability framework. Ensure that they are compatible with/incorporate the specifications/procedures the EC could have in mind to list in these implementing acts.
269	AT 45	**Article 45 Requirements for qualified certificates for website authentication** Article 45 is amended as indicating in rows 271, 272, and 273.	No impact on standards for ERDS
270	AT 45	Article 45-1 1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. Qualified certificates for website authentication shall be deemed compliant with the requirements laid down in Annex IV where they meet the standards referred to in paragraph 3.	No impact on standards for ERDS
271	AT 45	Article 45-2 2. Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. For those purposes web-browsers shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1, with the exception of enterprises, considered to be microenterprises and small enterprises in accordance with Commission Recommendation 2003/361/EC in the first 5 years of operating as providers of web-browsing services.	No impact on standards for ERDS
272	AT 45	Article 45-3 3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide the specifications and reference numbers of standards for qualified certificates for website authentication referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).'	No impact on standards for ERDS
273	AT 45a	**Article 45a Legal effects of electronic attestation of attributes**	
274	AT 45a	Article 45a-1 1. An electronic attestation of attributes shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.	Legal prescription. No impact on standards for ERDS
275	AT 45a	Article 45a-2 2. A qualified electronic attestation of attributes shall have the same legal effect as lawfully issued attestations in paper form.	Legal prescription. No impact on standards for ERDS

#	Type	eIDAS 2.0 provisions	Discussion	Actions to perform / Questions to answer
276	AT 45a	Article 45a-3 3. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.		Ensure that in the framework this is incorporated when specifying usage of QEA for authentication.
277	AT 45b	**Article 45b Electronic attestation of attributes in public services**		
278		Article 45b When an electronic identification using an electronic identification means and authentication is required under national law to access an online service provided by a public sector body, person identification data in the electronic attestation of attributes shall not substitute electronic identification using an electronic identification means and authentication for electronic identification unless specifically allowed by the Member State or the public sector body. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.		Ensure this requirement is included in the policy documents.
279	AT 45c	**Article 45c Requirements for qualified attestation of attributes**		
280	AT 45c	Article 45c-1 1. Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V. A qualified electronic attestation of attributes shall be deemed to be compliant with the requirements laid down in Annex V, where it meets the standards referred to in paragraph 4.	No direct impact on ERDS framework of standards	
281	AT 45c	Article 45c-2 2. Qualified electronic attestations of attributes shall not be subject to any mandatory requirement in addition to the requirements laid down in Annex V.	No direct impact on ERDS framework of standards	
282	AT 45c	Article 45c-3 3. Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.		Ensure to mention (by referencing another TS?) revocation in policy/technical specs documents.
283	AT 45c	Article 45c-4 4. Within 6 months of the entering into force of this Regulation, the Commission shall establish reference numbers of standards for qualified electronic attestations of attributes by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).		Ensure referencing these docs in the framework.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
284	AT 45d	**Article 45d Verification of attributes against authentic sources**	
285	AT 45d	Article 45d-1 1. Member States shall ensure that, at least for the attributes listed in Annex VI, wherever these attributes rely on authentic sources within the public sector, measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the attribute directly against the relevant authentic source at national level or via designated intermediaries recognised at national level in accordance with national or Union law.	No direct impact on ERDS framework
286	AT 45d	Article 45d-2 2. Within 6 months of the entering into force of this Regulation, taking into account relevant international standards, the Commission shall set out the minimum technical specifications, standards and procedures with reference to the catalogue of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).	Review the list of standards and ensure the presence of references to the relevant ones in the standards.
287	AT 45e	**Article 45e Issuing of electronic attestation of attributes to the European Digital Identity Wallets**	
288		Article 45e Providers of qualified electronic attestations of attributes shall provide an interface with the European Digital Identity Wallets issued in accordance in Article 6a.	No direct impact on ERDS framework
289	AT 45f	**Article 45f Additional rules for the provision of electronic attestation of attributes services**	
290	AT 45f	Article 45f-1 1. Providers of qualified and non-qualified electronic attestation of attributes services shall not combine personal data relating to the provision of those services with personal data from any other services offered by them.	Policy documents should require that providers of QEA and EAs used in authentication processes fulfil the requirements specified here.
291	AT 45f	Article 45f-2 2. Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held.	As before
292	AT 45f	Article 45f-3 3. Personal data relating to the provision of qualified electronic attestation of attributes services shall be kept physically and logically separate from any other data held.	As before
293	AT 45f	Article 45f-4 4. Providers of qualified electronic attestation of attributes' services shall provide such services under a separate legal entity.	As before

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
294	AT 45g	**Article 45g Qualified electronic archiving services**	
295		Article 45g A qualified electronic archiving service for electronic documents may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the electronic document beyond the technological validity period. Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for electronic archiving services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	An ERDS provider might interested in externalizing the archiving of Evidence/messages. If so, include provisions in policy and technical documents and ensure references to the relevant specifications.
296	AT 45h	**Article 45h Legal effects of electronic ledgers**	
297	AT 45h	Article 45h-1 1. An electronic ledger shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.	Indeed Electronic Ledgers need to be included in policy and technical documents.
298	AT 45h	Article 45h-2 2. A qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger.	As before
299	AT 45i	**Article 45i Requirements for qualified electronic ledgers**	As before
300	AT 45i	Article 45i-1 1. Qualified electronic ledgers shall meet the following requirements: (a) they are created by one or more qualified trust service provider or providers; (b) they ensure the uniqueness, authenticity and correct sequencing of data entries recorded in the ledger; (c) they ensure the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry; (d) they record data in such a way that any subsequent change to the data is immediately detectable.	As before
301	AT 45i	Article 45i-2 2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger meets the standards referred to in paragraph 3.	As before

#	Type	eIDAS 2.0 provisions	Discussion	Actions to perform / Questions to answer
302	AT 45i	Article 45i-3 3. The Commission may, by means of implementing acts, establish reference numbers of standards for the processes of execution and registration of a set of data into, and the creation, of a qualified electronic ledger. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).'		Ensure references to these documents in the framework.
303		The following heading is inserted before Article 46a **CHAPTER IVa GOVERNANCE FRAMEWORK** **Article 46a Supervision of the EUDIW framework**		
304		Article 46a 1. Member States shall designate one or more supervisory bodies established in their territory. Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks in an effective, efficient and independent manner.	No direct impact on ERDS framework of standards	
305		Article 46a 2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.	No direct impact on ERDS framework of standards	
306		Article 46a 3. The role of the supervisory bodies shall be: (a) to supervise providers of European Digital Identity Wallets established in the designating Member State and to ensure, through ex ante and ex post supervisory activities, that those issuers and the European Digital Identity Wallets they provide meet the requirements laid down in this Regulation. (b) to take action, if necessary, in relation to providers of European Digital Identity Wallets established in the territory of the designating Member State, through ex post supervisory activities, when informed that those issuers and the European Digital Identity Wallets they provide allegedly do not meet the requirements laid down in this Regulation.	Impact	In policy documents it will be required that EUDI Wallets interacting with ERDS will have to be issued by supervised providers.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
307		Article 46a 4. The tasks of the supervisory bodies shall include in particular: (a) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e; (b) to request information necessary to monitor the compliance with the relevant provisions of this Regulation; (c) to inform the relevant national competent authorities of the Member States concerned, designated pursuant to Directive (EU) 2022/2555, of any significant breaches of security or loss of integrity they become aware of in the performance of their tasks and, in the case of a significant breach of security or loss of integrity which concerns other Member States, to inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) 2022/2555 and single points of contact designated pursuant to Article 46c of this Regulation in the other Member States concerned. The notified supervisory body shall inform the public or require the European Digital Identity Wallet provider to do so where it determines that disclosure of the breach of security or loss of integrity is in the public interest; (d) to carry out on-site inspections and off-site supervision; (e) to require that providers of European Digital Identity Wallets remedy any failure to fulfil the requirements laid down in this Regulation; (f) to suspend or cancel the registration and inclusion of relying parties in the mechanism referred to in Article 6b(2) in the case of illegal or fraudulent use of the European Digital Identity Wallet; (g) to cooperate with competent supervisory authorities established under Regulation (EU) 2016/679, in particular, by informing them without undue delay, where personal data protection rules appear to have been breached and about security breaches which appear to constitute personal data breaches;	No impact on ERDS framework of standards
308		Article 46a 5. Where the supervisory body requires the provider of a European Digital Identity Wallet to remedy any failure to fulfil requirements under this Regulation pursuant to paragraph 4 (d) and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may order the provider to suspend or to cease the issuance of the European Digital Identity Wallet. The supervisory bodies shall inform the supervisory bodies of other Member States, the Commission, relying parties and users of the European Digital Identity Wallet without undue delay of the decision to require the suspension or cessation of the European Digital Identity Wallet.	No impact on ERDS framework of standards
309		Article 46a 6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities.	No impact on ERDS framework of standards

#	Type	eIDAS 2.0 provisions	Discussion	Actions to perform / Questions to answer
310		Article 46a 7. The Commission shall make the annual reports referred to in paragraph 6 available to the European Parliament and the Council.	No impact on ERDS framework of standards	
311		Article 46a 8. By ... [12 months after the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	No impact on ERDS framework of standards	
312		**Article 46b** **Supervision of trust services**		
313		Article 46b 1. Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State. Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.	No impact on ERDS framework of standards	
314		Article 46b 2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.	No impact on ERDS framework of standards	
315		Article 46b 3. The role of the supervisory body shall be: (a) to supervise qualified trust service providers established in the territory of the designating Member State through ex ante and ex post supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation; (b) to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through ex post supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation;	Impact	In policy documents it will be required QERDS (and any other external QTSP whose services the QERDSP uses for providing its QERDS) have to be supervised. Also ERDS and any other external TSP whose services the ERDSP uses for providing its ERDS will meet the requirements laid down in the regulation.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
316		Article 46b 4. The tasks of the supervisory body shall include in particular: (a) to inform the relevant national competent authorities of the Member States concerned, designated pursuant to Directive (EU) 2022/2555, of any significant breaches of security or loss of integrity they become aware of in the performance of their tasks and, in the case of a significant breach of security or loss of integrity which concerns other Member States, to inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) 2022/2555 and single points of contact designated pursuant to [Article 46c] of this Regulation in the other Member States concerned. The notified supervisory body shall inform the public or require the trust service provider to do so where it determines that disclosure of the breach of security or loss of integrity is in the public interest;'; (b) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e; (c) to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1); (d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article; (e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2); (f) to cooperate with competent supervisory authorities established under Regulation (EU) 2016/679, in particular, by informing them without undue delay where personal data protection rules appear to have been breached and about security breaches which appear to constitute personal data breaches;' (g) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21; (h) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body; (i) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with Article 24(2), point (h); (j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation. (k) to investigate claims made by web-browsers pursuant to Article 45a and to take action if necessary.	Indirect impact TSPs have to remedy failures. Policy document.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
317		Article 46b 5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.	Trust building Include in policy document the requirement on a (Q)ERDS to be listed in the TL.
318		Article 46b 6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities.	No impact on ERDS framework of standards
319		Article 46b 7. The Commission shall make the annual reports referred to in paragraph 6 available to the European Parliament and the Council.	No impact on ERDS framework of standards
320		Article 46b 8. By ... [12 months after the date of entry into force of this amending Regulation], the Commission shall adopt guidelines on the exercise by the Supervisory bodies of the tasks referred to in paragraph 4, and, by means of implementing acts adopted in accordance with the examination procedure referred to in Article 48(2), define the formats and procedures for the report referred to in paragraph 6.';	No impact on ERDS framework of standards
321		**Article 46c** **Single points of contact**	
322		Article 46c 1. Each Member State shall designate one national single point of contact for trust services, European Digital Identity Wallets and notified electronic identification schemes.	No impact on ERDS framework of standards
323		Article 46c 2. Single points of contact shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and between the supervisory bodies for the providers of the European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity and with other competent authorities within its Member State.	No impact on ERDS framework of standards
324		Article 46c 3. Each Member State shall make public and, without undue delay, notify to the Commission the names and the addresses of the designated single point of contact referred to in paragraph 1 and any subsequent change thereto.	No impact on ERDS framework of standards
325		Article 46c 4. The Commission shall publish a list of the notified single points of contact.	No impact on ERDS framework of standards

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
326		**Article 46d** **Mutual assistance**	
327		Article 46d 1. In order to facilitate the supervision and enforcement of obligations under this Regulation, supervisory bodies responsible for trust services and for European Digital Identity Wallets may seek, including through the EDICG, mutual assistance from supervisory bodies of another Member State where the trust service provider or the provider of the European Digital Identity Wallet is established, its network and information systems are located, or its services are provided.	No impact on ERDS framework of standards
328		Article 46d 2. The mutual assistance shall at least entail that: (a) the supervisory body applying supervisory and enforcement measures in one Member State, shall inform and consult the supervisory body from the other Member State concerned; (b) a supervisory body may request the supervisory body of another Member State concerned to take supervisory or enforcement measures, including, for instance requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21 regarding the provision of trust services; (c) where appropriate, supervisory bodies may carry out joint investigations with other Member States' supervisory bodies. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.	No impact on ERDS framework of standards
329		Article 46d 3. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds: (a) the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Articles 46a and 46b; (b) the supervisory body is not competent to provide the requested assistance; (c) providing the requested assistance would be incompatible with this Regulation.	No impact on ERDS framework of standards
330		Article 46d 4. By ... [12 months after the date of entry into force of this amending Regulation] [and every two years thereafter], the EDICG shall issue guidance on the organisational aspects and procedures for the mutual assistance referred to in paragraphs 1 and 2.	No impact on ERDS framework of standards

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
331		**Article 46e The European Digital Identity Cooperation Group**	
332		Article 46e 1. In order to support and facilitate Member States' cross-border cooperation and exchange of information on trust services, European Digital Identity Wallets and notified electronic identification schemes, the European Digital Identity Cooperation Group (the 'EDICG'), shall be established by the Commission.	No impact on ERDS framework of standards
333		Article 46e 2. The EDICG shall be composed of representatives appointed by the Member States and of the Commission. The EDICG shall be chaired by the Commission who shall provide the EDICG Secretariat.	No impact on ERDS framework of standards
334		Article 46e 3. Representatives of relevant stakeholders may be invited to attend meetings of the EDICG and to participate in its work as observers, on an ad hoc basis.	No impact on ERDS framework of standards
335		Article 46e 4. The European Union Agency for Cybersecurity shall be invited to participate as observer in the workings of the EDICG when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, the use of cybersecurity certificates or standards are addressed.	No impact on ERDS framework of standards

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
336		Article 46e 5. The EDICG shall have the following tasks: (a) exchange advice and cooperate with the Commission on emerging policy initiatives in the field of digital identity wallets, electronic identification means and trust services; (b) advise the Commission, as appropriate, in the early preparation of draft implementing and delegated acts to be adopted pursuant to this Regulation; (c) in order to support the supervisory bodies in the implementation of the provisions of this Regulation, the EDICG shall: (i) exchange best practices and information regarding the implementation: of the provisions of this Regulation; (ii) assess the relevant developments in the digital wallet, electronic identification and trust services sectors; (iii) organise joint meetings with relevant interested parties from across the Union to discuss activities carried out by the cooperation group and gather input on emerging policy challenges; (iv) with the support of ENISA, exchange views, best practices and information on relevant cybersecurity aspects concerning European Digital Identity Wallets, electronic identification schemes and trust services; (v) exchange best practices in relation to the development and implementation of policies on notification of breaches, and common measures as referred to in Articles 10 and 10a; (vi) organise joint meetings with the NIS Cooperation Group established under Directive EU 2022/2555 to exchange relevant information in (39b) relation to trust services and electronic identification related cyber threats, incidents, vulnerabilities, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications capacity as well as standards and technical specifications; (vii) organise peer reviews of electronic identification schemes to be notified falling under this Regulation; (viii) discuss, upon a request of a supervisory body, specific requests for mutual assistance as referred to in Article 46d; (ix) facilitate the exchange of information between the supervisory bodies by providing guidance on the organisational aspects and procedures for the mutual assistance referred to in Article 46d.	No impact on ERDS framework of standards
337		Article 46e 6. Member States shall ensure effective and efficient cooperation of their designated representatives in the EDICG.	No impact on ERDS framework of standards

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
338		Article 46e 7. Within 12 months of the entry into force of the Regulation, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in point (vii) of paragraph 5 . That implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).'	No impact on ERDS framework of standards
339		**Article 47** This article is amended as indicated in rows 341, 342, and 343.	
340		Paragraph 2 is replaced by the following: 2. The power to adopt delegated acts referred to in Article 6c(6), Article 24(6), and Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.	No impact on ERDS framework of standards
341		Paragraph 3 is replaced by the following: 3. The delegation of power referred to in Article 6c(6), Article 24(6), and Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	No impact on ERDS framework of standards
342		Paragraph 5 is replaced by the following: 5. A delegated act adopted pursuant to Article 6c(6), Article 24(6), or Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of (b) notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	No impact on ERDS framework of standards
343	AT 48a	**Article 48a Reporting requirements**	No direct impact on ERDS framework
344	AT 48a	Article 48a-1 1. Member States shall ensure the collection of statistics in relation to the functioning of the European Digital Identity Wallets and the qualified trust services.	No direct impact on ERDS framework

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
345	AT 48a	Article 48a-2 2. The statistics collected in accordance with paragraph 1, shall include the following: (a) the number of natural and legal persons having a valid European Digital Identity Wallet; (b) the type and number of services accepting the use of the European Digital Wallet; (c) incidents and down time of the infrastructure at national level preventing the use of Digital Identity Wallet Apps.	No direct impact on ERDS framework
346	AT 48a	Article 48a-3 3. The statistics referred to in paragraph 2 shall be made available to the public in an open and commonly used, machine-readable format.	No direct impact on ERDS framework
347	AT 48a	Article 48a-4 4. By March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.	No direct impact on ERDS framework
348	AT 49	**Article 49** This article is replaced by the contents of rows 350, 351, and 353.	No direct impact on ERDS framework
349	AT 49	Article 49-1 1. The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council within 24 months after its entering into force. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal for amendment of this Regulation.	No direct impact on ERDS framework
350	AT 49	Article 49-2 2. The evaluation report shall include an assessment of the availability and usability of the identification means including European Digital Identity Wallets in scope of this Regulation and assess whether all online private service providers relying on third party electronic identification services for users authentication, shall be mandated to accept the use of notified electronic identification means and European.	No direct impact on ERDS framework
351	AT 49	Article 49-3 3. In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.	No direct impact on ERDS framework

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
352	AT 51	**Article 51 Transitional measures** This article is replaced by the contents of rows 324, and 355.	
353	AT 51	Article 51-1 1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall continue to be considered as qualified electronic signature creation devices under this Regulation until [date - OJ please insert period of four years following the entry into force of this Regulation].	No direct impact on ERDS framework
354	AT 51	Article 51-2 2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until [date - PO please insert a period of four years following the entry into force of this Regulation].'	No direct impact on ERDS framework
355	ANN I	**(43) Annex I is amended in accordance with Annex I to this Regulation**	Impact as the impact by the body text that references this annex.
356		In Annex I, point (i) is replaced by the following: (i) the information, or the location of the services that can be used to enquire, about the validity status of the qualified certificate.	No change in the impact of Annex I
			Added "information" in addition to "location".
357	ANN II	**(44) Annex II is replaced by the text set out in Annex II to this Regulation**	Impact as the impact by the body text that references this annex.
358		Annex II **Dropped:** 3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider. 4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: (a) the security of the duplicated datasets must be at the same level as for the original datasets; (b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.	Assess impact on policy documents
			Check if in the policy documents there is any requirement to the dropped points.
359	ANN III	**(45) Annex III is amended in accordance with Annex III to this Regulation**	Impact as the impact by the body text that references this annex
360		In Annex III, point (i) is replaced by the following: (i) the information, or the location of the services that can be used to enquire, about the validity status of the qualified certificate.	No change in the impact of Annex III
			Added "information" in addition to "location", as in (i) of Annex I.

#	Type	eIDAS 2.0 provisions	Discussion Actions to perform / Questions to answer
361	ANN IV	**(46) Annex IV is amended in accordance with Annex IV to this Regulation** Annex IV is amended as indicated in rows 363 and 364:	Impact as the impact by the body text that references this annex.
362		(1) point (c) is replaced by the following: (c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated; (ca) for legal persons: a unique set of data unambiguously representing the legal person to whom the certificate is issued, with at least the name of the legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official records;	No impact on ERDS framework of standards This annex defines requirements for QCs for Website authentication.
363		(2) point (j) is replaced by the following: (j) the information, or the location of the certificate validity status services that can be used to enquire, about the validity status of the qualified certificate.	No impact on ERDS framework of standards This annex defines requirements for QCs for Website authentication.
364	ANN V	**(47) a new Annex V is added as set out in Annex V to this Regulation** **Annex V: Requirements for qualified electronic attestation of attributes**	Impact as the impact by the body text that references this annex.
365		Annex V Qualified electronic attestation of attributes shall contain: (a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes; (b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and: - for a legal person: the name and, where applicable, registration number as stated in the official records, - for a natural person: the person's name; (c) a set of data unambiguously representing the entity to which the attested attributes are referring to; if a pseudonym is used, it shall be clearly indicated; (d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes; (e) details of the beginning and end of the attestation's period of validity; (f) the attestation identity code, which must be unique for the qualified trust service provider and if applicable the indication of the scheme of attestations that the attestation of attributes is part of; (g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider; (h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge; (i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation.	Impact on ERDS In policy documents requirements on QEAAs if they are used for authentication. Also impact in technical specs.

#	Type	eIDAS 2.0 provisions	Discussion
			Actions to perform / Questions to answer
366	ANN VI	**(48) a new Annex VI is added to this Regulation** **Annex VI: Minimum list of attributes**	Impact as the impact by the body text that references this annex.
367		Annex VI Further to Article 45d, Member States shall ensure that measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with Union or national law and in cases where these attributes rely on authentic sources within the public sector: 1. Address; 2. Age; 3. Gender; 4. Civil status; 5. Family composition; 6. Nationality or citizenship; 6a. 7. Educational qualifications, titles and licenses; 8. Professional qualifications, titles and licenses; 8a. Powers and mandates to represent natural or legal persons 9. Public permits and licenses; 10. For legal persons, financial and company data.	Impact on ERDS framework of standards
			Check whether in the policy documents some reference to these requirements has to be made when dealing with authentication with (Q)EAA. Assess any potential impact (reference to these requirements) in technical documents. NOTE: Bullet 6a was empty in the draft version of eIDAS 2.0 [i.2] analysed for building the present table.

Annex B: ETSI ERDS baseline - an example of a possible transport module

The transport module of the ERDS baseline consists of a set of supporting technological functions and options.

An **example** of a possible configuration representing an ERDS baseline model - aiming to cover, amongst others, the requirements of eIDAS 2.0 [i.2] for EU *qualified electronic registered delivery service* - is detailed in Figure B.1.

NOTE 1: qualified electronic registered delivery services are provided by one or more qualified trusted service providers (e.g. see for instance Article 44 paragraph 1(a)).

It is composed by the following instantiation of the modules and of relevant options:

- Common Service Infrastructure (CSI) configured with **TL** and according to what is necessary for *addressing*, *routing* and *trusting* purposes.

NOTE 2: The trusted lists (**TL**) are a requirement of eIDAS 2.0 regulation [i.2] for ***qualified trusted service providers*** (e.g. see for instance *Article 22 paragraph 1*).

- JSON format to wrap the ERD dispatch or the ERDS receipt (composed by the fundamental components packed as illustrated in clauses 4.2.2.3 and 4.2.2.4) and the information of the transport (e.g. *relay metadata*).

NOTE 3: **JSON** is currently one of the most preferred data interchange formats, at protocol level, through web services due to its simplicity and neutrality (since it is an open, human-readable and language-independent data format - currently defined in IETF RFC 7159 [i.30]). Under this rationale the present example shows JSON to accompany the transfer of data between distributed systems of more ***qualified trusted service providers***.

- JAdES option for securing the relevant transport metadata information and securing the relevant transport metadata information.

NOTE 4: **JAdES** option for signing and securing transport metadata information can be used to meet the requirements of *qualified electronic signatures* and *seals* for ***qualified trusted service providers*** as defined in eIDAS 2.0 Regulation [i.2] - according to ETSI TS 119 182-1 [i.29]. It is a JSON format extension for AdES standard signatures (built on top of JSON Web Signatures as specified in IETF RFC 7515 [i.31] by a dedicated set of JSON header parameters).

- Ledger option for recording the transport metadata information on a *Permission Distributed Ledger* (PDL).

NOTE 5: **PDL** option for recording the transport metadata information can be used, among other things, for instance, for the opportune tracking requirements and to ensure the accuracy in chronological ordering of each transaction.

- REST technology for a reliable transfer of potentially *huge contents* (and provided by an auto-resume option for recovering of issues during the transfer).

NOTE 6: The **REST** option represents, currently, the most preferred architectural style to facilitate a large-scale adoption through its robustness, high degree of scalability and neutrality (since it allows - by design - an independent deployment of components). Under this rationale the present example shows REST for implementing the interactions between distributed systems of more ***qualified trusted service providers***.

- TLS technology for a protected transfer, optionally improved by the DNSSEC additional technology.

NOTE 7: **TLS** represents, currently, the most preferred cryptographic transport protocol, due to its widely usage in providing, by design and with a high degree of neutrality, security measures like confidentiality, integrity and authenticity in communicating network applications. Under this rationale the present example includes TLS international standard for implementing **the transport** interactions between distributed systems of more ***qualified trusted service providers***.

Note that other cryptographic and security measures can obviously be provided on top of it. For instance, further encryptions at *user content* level, or directly at *packaging* level (see clauses 4.2.2.3 and 4.2.2.4 to identify the *user content* component and the *packaging* process).

The **DNSSEC** option represents, an additional security that can be added to canonical domain name system able to provide measures protecting the qualified electronic registered delivery services from accepting forged or manipulated DNS information during the interactions between distributed systems of more ***qualified trusted service providers***.

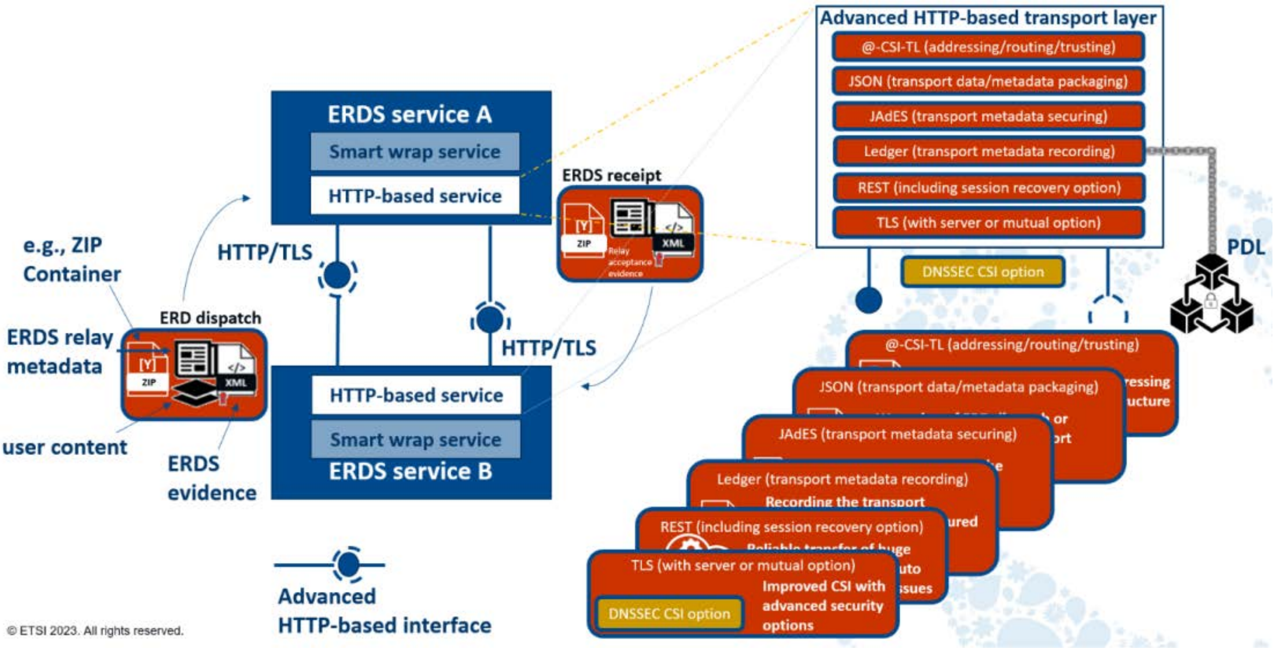

Advanced HTTP-based transport layer
@-CSI-TL (addressing/routing/trusting)
JSON (transport data/metadata packaging)
JAdES (transport metadata securing)
Ledger (transport metadata recording)
REST (including session recovery option)
TLS (with server or mutual option)
DNSSEC CSI option
PDL
ERDS service A
Smart wrap service
HTTP-based service
ERDS receipt
ZIP
XML
Relay acceptance evidence
e.g., ZIP Container
HTTP/TLS
ERD dispatch
ERDS relay metadata
HTTP/TLS
HTTP-based service
Smart wrap service
ERDS service B
user content
ERDS evidence
@-CSI-TL (addressing/routing/trusting)
ressing
ucture
JSON (transport data/metadata packaging)
or
ort
JAdES (transport metadata securing)
Ledger (transport metadata recording)
Recording the transport
ured
REST (including session recovery option)
Reliable transfer of huge
uto
ssues
TLS (with server or mutual option)
Improved CSI with advanced security options
DNSSEC CSI option
Advanced HTTP-based interface

Figure B.1: ERDS Baseline - Transport details example

The optional supporting technological functions can be used in a combined way to obtain a *crescendo* of different levels of service.

Figure B.2 demonstrates a full-options scenario, incorporating ZIP packaging for content and metadata, along with JAdES, Ledger, and DNSSEC CSI options for data transport (CSI-TL, JSON, REST, and TLS are standard functions for ERDS baseline transport).

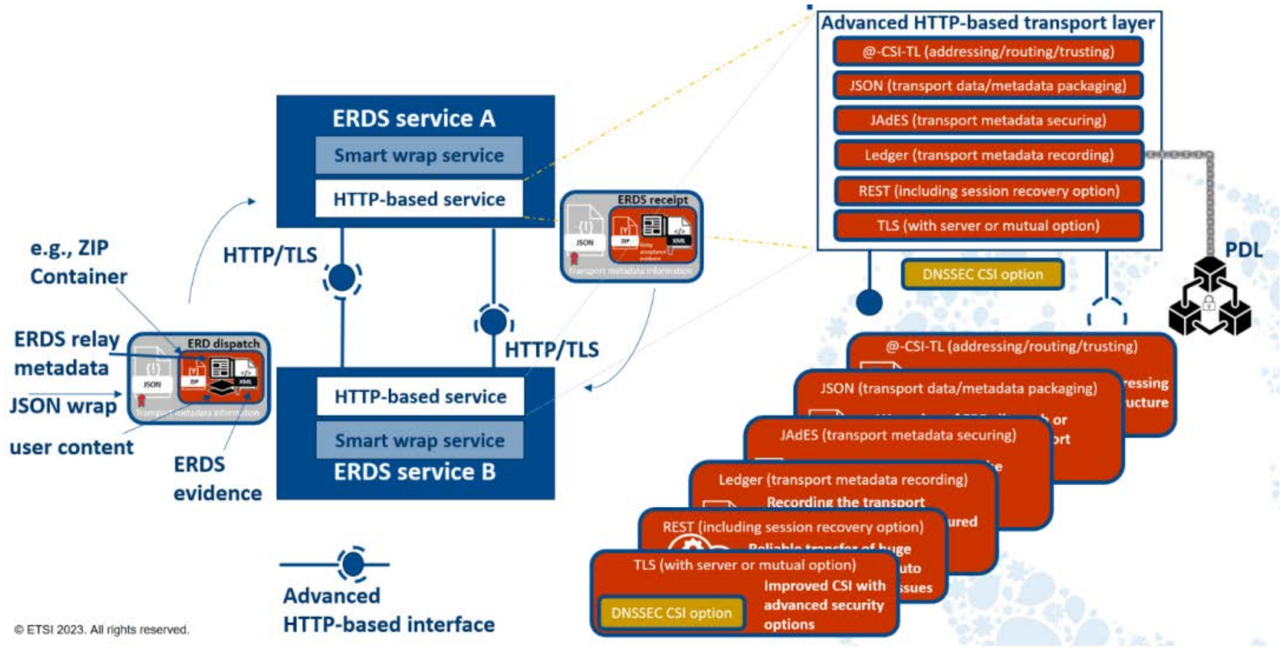

Advanced HTTP-based transport layer
@-CSI-TL (addressing/routing/trusting)
JSON (transport data/metadata packaging)
JAdES (transport metadata securing)
Ledger (transport metadata recording)
REST (including session recovery option)
TLS (with server or mutual option)
DNSSEC CSI option
PDL
ERDS service A
Smart wrap service
HTTP-based service
ERDS receipt
JSON
ZIP
XML
Transport metadata information
e.g., ZIP
Container
HTTP/TLS
ERDS relay
metadata
ERD dispatch
JSON wrap
user content
ERDS
evidence
HTTP/TLS
HTTP-based service
Smart wrap service
ERDS service B
@-CSI-TL (addressing/routing/trusting)
JSON (transport data/metadata packaging)
JAdES (transport metadata securing)
Ledger (transport metadata recording)
Recording the transport
REST (including session recovery option)
TLS (with server or mutual option)
Improved CSI with
advanced security
options
DNSSEC CSI option
Advanced
HTTP-based interface
© ETSI 2023. All rights reserved.

Figure B.2: ERDS Baseline - Full options transport example

This example in Figure B.2 showcases the practical application and representation of the ERDS baseline as a small, lightweight layer, as introduced in Figure 2.

Annex C:
Bibliography

ETSI TR 119 540: "Electronic Signatures and Trust Infrastructures (ESI); Standardisation requirements for smart contracts based on electronic ledgers".

ETSI TS 119 462: "Electronic Signatures and Trust Infrastructures (ESI); Wallet interfaces for trust services and signing".

History

Document history		
V1.1.1	April 2024	Publication