ETSI TS 119 411-8 V1.1.1 (2025-10)

TECHNICAL SPECIFICATION

Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 8: Access Certificate Policy for EUDI Wallet Relying Parties

Reference
DTS/ESI-0019411-8

Keywords
e-commerce, electronic signature, EUDI wallet,
security, trust services

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 7
3 Definition of terms, symbols, abbreviations and notations 8
3.1 Terms 8
3.2 Symbols 9
3.3 Abbreviations 9
3.4 Notations 9
4 General concepts 10
4.1 General policy requirements concept 10
4.2 Certificate policy and certification practice statement 10
4.2.1 Certification Practice Statement 10
4.2.2 Certificate Policy 10
4.2.3 Terms and conditions and PKI disclosure statement 10
4.3 Certification services 10
5 General provisions on Certification Practice Statement and Certificate Policies 10
5.1 General requirements 10
5.2 Certification Practice Statement Requirements 11
5.3 Certificate Policy name and identification 11
5.4 PKI Participants 11
5.4.1 Certification authority 11
5.4.2 Subscriber and subject 11
5.4.3 Others 12
5.5 Certificate Usage 12
5.5.1 NCP-n-eudiwrp 12
5.5.2 NCP-l-eudiwrp 12
5.5.3 QCP-n-eudiwrp 12
5.5.4 QCP-l-eudiwrp 12
6 Trust Service Providers practice 12
6.1 Publication and Repository Responsibilities 12
6.2 Identification and Authentication 12
6.2.1 Naming 12
6.2.2 Initial Identity Validation 12
6.2.3 Identification and authentication for Re-key requests 13
6.2.4 Identification and authentication for revocation requests 13
6.3 Certificate Life-Cycle Operational Requirements 13
6.3.1 Certificate Application 13
6.3.2 Certificate application processing 13
6.3.3 Certificate issuance 13
6.3.4 Certificate acceptance 13
6.3.5 Key Pair and Certificate Usage 13
6.3.6 Certificate Renewal 14
6.3.7 Certificate Re-key 14
6.3.8 Certificate Modification 14
6.3.9 Certificate Revocation and Suspension 14
6.3.10 Certificate Status Services 14
6.3.11 End of Subscription 14

6.3.12 Key Escrow and Recovery 14
6.4 Facility, Management and Operational Controls 14
6.4.1 General 14
6.4.2 Physical Security Controls 14
6.4.3 Procedural Controls 14
6.4.4 Personnel Controls 15
6.4.5 Audit Logging Procedures 15
6.4.6 Records Archival 15
6.4.7 Key Changeover 15
6.4.8 Compromise and Disaster Recovery 15
6.4.9 CA or RA Termination 15
6.5 Technical Security Controls 15
6.5.1 Key Pair Generation and Installation 15
6.5.2 Private Key Protection and Cryptographic Module Engineering Controls 15
6.5.3 Other Aspects of Key Pair Management 15
6.5.4 Activation Data 15
6.5.5 Computer Security Controls 16
6.5.6 Life Cycle Security Controls 16
6.5.7 Network Security Controls 16
6.6 Certificate, CRL, and OCSP Profiles 16
6.6.1 Certificate Profile 16
6.6.2 CRL Profile 17
6.6.3 OCSP Profile 17
6.7 Compliance Audit and Other Assessment 17
6.8 Other Business and Legal Matters 17
6.8.1 Fees 17
6.8.2 Financial Responsibility 17
6.8.3 Confidentiality of Business Information 17
6.8.4 Privacy of Personal Information 18
6.8.5 Intellectual Property Rights 18
6.8.6 Representations and Warranties 18
6.8.7 Disclaimers of Warranties 18
6.8.8 Limitations of Liability 18
6.8.9 Indemnities 18
6.8.10 Term and Termination 18
6.8.11 Individual notices and communications with participants 18
6.8.12 Amendments 18
6.8.13 Dispute Resolution Procedures 18
6.8.14 Governing Law 18
6.8.15 Compliance with Applicable Law 18
6.8.16 Miscellaneous Provisions 18
6.9 Other Provisions 19
6.9.1 Organizational 19
6.9.2 Additional testing 19
6.9.3 Disabilities 19
6.9.4 Terms and conditions 19

Annex A (informative): Bibliography 20

Annex B (informative): Change history 21

History 22

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Trust Infrastructures (ESI).

The present document is part 8 of a multi-part deliverable covering policy requirements for Trust Service Providers issuing certificates. Full details of the entire series can be found in part 1 [3].

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 eIDAS Regulation (EU) No 910/2014 [i.1], as amended by Regulation (EU) 2024/1183 [i.2] and Directive (EU) 2022/2555 [i.3], establishes a framework for electronic identification and trust services for electronic transactions in the internal market. The revised regulation, often referred to as eIDAS2, requires for wallet-relying parties to provide the necessary information for their identification and authentication when interacting with European Digital Identity Wallets (EUDIW).

CIR (EU) 2025/848 on the registration of wallet-relying parties [i.6] identifies wallet-relying party access certificates and registration certificates.

A wallet-relying party access certificate, issued by a designated provider under Member State supervision, serves to authenticate and validate the integrity and trustworthiness of the wallet-relying parties.

The wallet-relying party access certificates management process for wallet-relying parties is designed to enhance transparency, ensure accountability, and build trust in the use of the European Digital Identity Wallet across the EU.

1 Scope

The present document specifies requirements for qualified and non-qualified certificates for electronic seals/signatures for wallet-relying party access certificates to be used by wallet-relying parties aiming to meet the needs of eIDAS2 [i.2] and implementing acts, especially CIR (EU) 2025/848 [i.6] on the access certificates for wallet-relying parties.

The present document imposes no requirements on the functioning of Competent Authorities registering and overseeing the operation of wallet-relying parties.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

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 necessary for the application of the present document.

[1] ETSI EN 319 412-1: "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[2] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions; Part 1: Country codes".

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

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

[5] ETSI TS 119 475: "Electronic Signatures and Trust Infrastructures (ESI); Relying party attributes supporting EUDI Wallet user's authorization decisions".

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[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] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.3] 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) (Text with EEA relevance).

[i.4] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.5] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.6] CIR (EU) 2025/848: "Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties".

[i.7] IETF RFC 9162: "Certificate Transparency Version 2.0".

[i.8] Recommendation ITU-T X.520: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in European Digital Identity Framework [i.2], ETSI EN 319 412-1 [1], ETSI EN 319 411-1 [3], ETSI EN 319 411-2 [4] and the following apply:

competent authority: authority recognized under the applicable regulations as competent for the national registration policies relating to European Digital Identity wallet-relying parties

European digital identity wallet: electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and 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

NOTE: As defined in European Digital Identity Framework regulation [i.2].

national register of wallet-relying parties: national electronic register used by a Member State to make information on wallet-relying parties registered in that Member State publicly available

NOTE: As set out in Article 5b(5) of Regulation (EU) No 910/2014 [i.1].

provider of wallet-relying party access certificates: natural or legal person mandated by a Member State to issue wallet-relying party access certificates to wallet-relying parties registered in that Member State

NOTE 1: As defined in CIR (EU) 2025/848 [i.6].

NOTE 2: In the context of the present document, a provider of wallet-relying party access certificates is a trust service provider.

registrar of wallet-relying parties: body responsible for establishing and maintaining the list of registered wallet-relying parties established in their territory and who has been designated by a Member State

NOTE: As defined in CIR (EU) 2025/848 [i.6].

wallet-relying party: relying party that intends to rely upon wallet units for the provision of public or private services by means of digital interaction

NOTE: As defined in CIR (EU) 2025/848 [i.6].

wallet-relying party access certificate: certificate for electronic seals or signatures authenticating and validating the wallet-relying party issued by a provider of wallet-relying party access certificates

NOTE: As defined in CIR (EU) 2025/848 [i.6].

3.2 Symbols

Void.

3.3 Abbreviations

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

CRL	Certificate Revocation List
eIDAS	electronic IDentification, Authentication and trust Services

NOTE: Informal name for Regulation (EU) No 910/2014 [i.1].

eIDAS2	Regulation (EU) 2024/1183 amending eIDAS
EUDIW	European Digital Identity Wallet
eudiwrp	european digital identity wallet relying party
OCSP	Online Certificate Status Protocol
TSP	Trust Service Provider

NOTE: In the context of the present document trust service provider acting as a provider of wallet-relying party access certificates.

3.4 Notations

The requirements identified in the present document include:

a) requirements applicable to any certificate policy. Such requirements are indicated by clauses without any additional marking;

b) requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

c) requirements applicable to the services offered under the applicable certificate policy. Such requirements are indicated by clauses marked by the applicable certificate policy indicator: "[NCP-n-eudiwrp]" or "[NCP-l-eudiwrp]" or "[QCP-n-eudiwrp]" or "[QCP-l-eudiwrp]".

Each requirement is identified as follows:

<3 letters service component> - < the clause number> - <2 digit number – incremental>

The service components are:

- **OVR:** General requirement (requirement applicable to more than 1 component)
- **GEN:** Certificate Generation Services
- **REG:** Registration Services
- **REV:** Revocation Services
- **SDP:** Subject Device Provisioning
- **CSS:** Certificate Status Service

The management of the requirement identifiers throughout subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for a deleted requirement is left and completed with "Void".
- The requirement identifier for a modified requirement is left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 General concepts

4.1 General policy requirements concept

ETSI EN 319 411-1 [3], clause 4.1 applies.

4.2 Certificate policy and certification practice statement

4.2.1 Certification Practice Statement

The explanations identified in ETSI EN 319 411-1 [3], clause 4.2.1 apply.

4.2.2 Certificate Policy

The explanations identified in ETSI EN 319 411-1 [3], clause 4.2.2 apply.

OVR-4.2.2-01: Providers of wallet-relying party access certificates conforming to the present document normative requirements may use certificate policy OIDs defined in the present document in its documentation and in the wallet-relying party access certificates it issues.

OVR-4.2.2-02: The certificate policy and certificate practice statement applicable to the provision of wallet-relying party access certificates shall comply with at least the Normalised Certificate Policy (NCP) requirements as specified in ETSI EN 319 411-1 [3].

4.2.3 Terms and conditions and PKI disclosure statement

The guidelines identified in ETSI EN 319 411-1 [3], clause 4.2.3 apply.

4.3 Certification services

The guidelines identified in ETSI EN 319 411-1 [3], clause 4.3 apply.

5 General provisions on Certification Practice Statement and Certificate Policies

5.1 General requirements

OVR-5.1-01: The general requirements specified in ETSI EN 319 411-1 [3], clause 5.1 shall apply.

OVR-5.1-02 [QCP-n-eudiwrp]**:** All policy requirements defined for QCP-n as specified in ETSI EN 319 411-2 [4] shall apply.

OVR-5.1-03 [QCP-l-eudiwrp]**:** All policy requirements defined for QCP-l as specified in ETSI EN 319 411-2 [4] shall apply.

OVR-5.1-04 [NCP-n-eudiwrp] [NCP-l-eudiwrp]**:** All policy requirements relevant to wallet-relying party access certificates issued to legal persons or natural persons defined for NCP shall be applied as specified in ETSI EN 319 411-1 [3].

5.2 Certification Practice Statement Requirements

OVR-5.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 5.2 shall apply.

5.3 Certificate Policy name and identification

As described in IETF RFC 3647 [i.4], clause 3.3, certificates include a certificate policy identifier which can be used by relying parties in determining the certificates suitability and trustworthiness for a particular application.

The policy identifiers for the ETSI certificate policies described in clause 4.2.2 of the present document are:

1) NCP-n-eudiwrp: Normalized certificate policy for wallet-relying party access certificates issued to natural persons;

```
-- NCP-n-eudiwrp: certificate policy for certificates for electronic signature
-- issued to EUDIW wallet-relying parties in accordance with the revised eIDAS Regulation;
ncp-n-eudiwrp OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) eudiwrp(194118) policy-identifiers(1) ncp-natural (1)}
```

2) NCP-l-eudiwrp: Normalized certificate policy for wallet-relying party access certificates issued to legal persons;

```
-- NCP-l-eudiwrp: certificate policy for certificates for electronic seal
-- issued to EUDIW wallet-relying parties in accordance with the revised eIDAS Regulation;
ncp-l-eudiwrp OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) eudiwrp(194118) policy-identifiers(1) ncp-legal (2)}
```

3) QCP-n-eudiwrp: Qualified certificate policy for wallet-relying party access certificates issued to natural persons;

```
-- QCP-n-eudiwrp: certificate policy for qualified certificates for electronic signature
-- issued to EUDIW wallet-relying parties in accordance with the revised eIDAS Regulation;
qcp-n-eudiwrp OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) eudiwrp(194118) policy-identifiers(1) qcp-natural (3)}
```

4) QCP-l-eudiwrp: Qualified certificate policy for wallet-relying party access certificates issued to legal persons;

```
-- QCP-l-eudiwrp: certificate policy for qualified certificates for electronic seal
-- issued to EUDIW wallet-relying parties in accordance with the revised eIDAS Regulation;
qcp-l-eudiwrp OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) eudiwrp(194118) policy-identifiers(1) qcp-legal (4)}
```

5.4 PKI Participants

5.4.1 Certification authority

OVR-5.4.1-01: The requirements identified in ETSI EN 319 411-1 [3], clause 5.4.1 shall apply.

5.4.2 Subscriber and subject

OVR-5.4.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 5.4.2 shall apply.

5.4.3 Others

OVR-5.4.3-01: The requirements identified in ETSI EN 319 411-1 [3], clause 5.4.3 shall apply.

5.5 Certificate Usage

5.5.1 NCP-n-eudiwrp

Wallet-relying party access certificates issued under this policy identifier are based on NCP and aimed to support the advanced electronic signatures such as defined in article 3 (12) of the Regulation (EU) No 910/2014 [i.1].

5.5.2 NCP-l-eudiwrp

Wallet-relying party access certificates issued under this policy identifier are based on NCP and aimed to support advanced electronic seals such as defined in article 3 (27) of the Regulation (EU) No 910/2014 [i.1].

5.5.3 QCP-n-eudiwrp

Wallet-relying party access certificates issued under this policy identifier are based on QCP-n and aimed to support the advanced electronic signatures based on a qualified certificate defined in articles 26 and 28 of the Regulation (EU) No 910/2014 [i.1].

5.5.4 QCP-l-eudiwrp

Wallet-relying party access certificates issued under this policy identifier are based on QCP-l and aimed to support the advanced electronic seals based on a qualified certificate defined in articles 36 and 38 of the Regulation (EU) No 910/2014 [i.1].

6 Trust Service Providers practice

6.1 Publication and Repository Responsibilities

OVR-6.1-01: The requirements specified in ETSI EN 319 411-1 [3], clause 6.1 shall apply.

6.2 Identification and Authentication

6.2.1 Naming

REG-6.2.1-01: The requirements identified in ETSI EN 319 411-2 [4], clause 6.2.1 shall apply.

6.2.2 Initial Identity Validation

REG-6.2.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.2.2 or practices which are confirmed to provide equivalent assurance shall apply.

NOTE: Registrar of wallet-relying parties may provide written confirmation to the TSP that it validates the identity with equivalence assurance to that provided by ETSI EN 319 411-1 [3], clause 6.2.2.

REG-6.2.2-02 [QCP-n-eudiwrp] [QCP-l-eudiwrp]**:** The requirements identified in ETSI EN 319 411-2 [4], clause 6.2.2 shall apply.

In addition, the following shall apply:

- **REG-6.2.2-03:** The provider of wallet-relying party access certificates shall verify that the wallet-relying party is included, with a valid registration status, in a national register of wallet-relying parties of the Member State in which that wallet-relying party is established.
- **REG-6.2.2-04:** If the Competent Authority/Member State in which the wallet-relying party is established provides additional rules for validation of these wallet-relying party access certificates, the provider of wallet-relying party access certificates shall apply the given rules.

6.2.3 Identification and authentication for Re-key requests

REG-6.2.3-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.2.3 shall apply.

6.2.4 Identification and authentication for revocation requests

REV-6.2.4-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.2.4 shall apply.

In addition, the following shall apply:

- **REV-6.2.4-02:** The provider of wallet-relying party access certificates shall provide a procedure for submission of wallet-relying party access certificate revocation requests by competent supervisory bodies or data protection authorities in its certificate policy or practice statement.
- **REV-6.2.4-03:** In addition, the provider of wallet-relying party access certificates shall provide a communication method, for notifications from the competent supervisory bodies about changes of relevant regulatory information of the wallet-relying party which can affect the validity of the wallet-relying party access certificate.

6.3 Certificate Life-Cycle Operational Requirements

6.3.1 Certificate Application

NOTE: See also clause 6.2.2 regarding identity validation.

REG-6.3.1-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.3.1 shall apply.

6.3.2 Certificate application processing

REG-6.3.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.3.2 shall apply.

6.3.3 Certificate issuance

GEN-6.3.3-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.3.3 shall apply.

GEN-6.3.3-02 [QCP-n-eudiwrp] [QCP-l-eudiwrp]: The requirements identified in ETSI EN 319 411-2 [4], clause 6.3.3 shall apply.

6.3.4 Certificate acceptance

OVR-6.3.4-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.3.4 shall apply.

OVR-6.3.4-02 [QCP-n-eudiwrp] [QCP-l-eudiwrp]**:** The requirements identified in ETSI EN 319 411-2 [4], clause 6.3.4 shall apply.

6.3.5 Key Pair and Certificate Usage

OVR-6.3.5-01: The general obligations specified in ETSI EN 319 411-1 [3], clause 6.3.5 shall apply.

OVR-6.3.5-02 [QCP-n-eudiwrp] [QCP-l-eudiwrp]: The requirements identified in ETSI EN 319 411-2 [4], clause 6.3.5 shall apply.

6.3.6 Certificate Renewal

REG-6.3.6-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.3.6 shall apply.

6.3.7 Certificate Re-key

REG-6.3.7-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.3.7 shall apply.

6.3.8 Certificate Modification

REG-6.3.8-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.3.8 shall apply.

6.3.9 Certificate Revocation and Suspension

REV-6.3.9-01: The requirements specified in ETSI EN 319 411-1 [3], clause 6.3.9 shall apply.

In addition, the following shall apply:

REV-6.3.9-02: The provider of wallet-relying party access certificates shall implement measures and processes to continuously monitor any changes in the national register for wallet-relying parties in which wallet-relying parties to whom they have issued wallet-relying party access certificates are registered.

REV-6.3.9-03: The provider of wallet-relying party access certificates shall have a process and an agreement with the registrar to be informed by the registrar when the registration of the wallet-relying party is suspended or cancelled.

REV-6.3.9-04: The provider of wallet-relying party access certificates shall revoke any wallet-relying party access certificate when the registration of the wallet-relying party is suspended or cancelled.

6.3.10 Certificate Status Services

CSS-6.3.10-01: The requirements specified in ETSI EN 319 411-1 [3], clause 6.3.10 shall apply.

CSS-6.3.10-02 [QCP-n-eudiwrp] [QCP-l-eudiwrp]: The requirements specified in ETSI EN 319 411-2 [4], clause 6.3.10 shall apply.

6.3.11 End of Subscription

No policy requirement.

6.3.12 Key Escrow and Recovery

SDP-6.3.12-01: The requirements specified in ETSI EN 319 411-1 [3], clause 6.3.12 shall apply.

6.4 Facility, Management and Operational Controls

6.4.1 General

OVR-6.4.1-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.4.1 shall apply.

6.4.2 Physical Security Controls

OVR-6.4.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.4.2 shall apply.

6.4.3 Procedural Controls

OVR-6.4.3-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.4.3 shall apply.

6.4.4 Personnel Controls

OVR-6.4.4-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.4.4 shall apply.

6.4.5 Audit Logging Procedures

OVR-6.4.5-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.4.5 shall apply.

In addition, the following shall apply:

OVR-6.4.5-02: The provider of wallet-relying party access certificates shall provide, where relevant, a description on how those wallet-relying party access certificates have been logged which should be in compliance with IETF RFC 9162 [i.7].

NOTE: ETSI is working on a Technical Specification requirements for certificate transparency.

6.4.6 Records Archival

OVR-6.4.6-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.4.6 shall apply.

In addition, the following shall apply:

OVR-6.4.6-02: The provider of wallet-relying party access certificates shall keep those wallet-relying party access certificates for at least ten years after any certificate based on these records ceases to be valid.

6.4.7 Key Changeover

No policy requirement.

6.4.8 Compromise and Disaster Recovery

OVR-6.4.8-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.4.8 shall apply.

6.4.9 CA or RA Termination

OVR-6.4.9-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.4.9 shall apply.

6.5 Technical Security Controls

6.5.1 Key Pair Generation and Installation

OVR-6.5.1-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.5.1 shall apply.

6.5.2 Private Key Protection and Cryptographic Module Engineering Controls

GEN-6.5.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.5.2 shall apply.

6.5.3 Other Aspects of Key Pair Management

GEN-6.5.3-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.5.3 shall apply.

6.5.4 Activation Data

SDP-6.5.4-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.5.4 shall apply.

6.5.5 Computer Security Controls

OVR-6.5.5-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.5.5 shall apply.

6.5.6 Life Cycle Security Controls

OVR-6.5.6-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.5.6 shall apply.

6.5.7 Network Security Controls

OVR-6.5.7-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.5.7 shall apply.

6.6 Certificate, CRL, and OCSP Profiles

6.6.1 Certificate Profile

GEN-6.6.1-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.6.1 shall apply except those applicable uniquely for website authentication certificates as specified below.

NOTE: Neither website authentication certificates nor short-term certificates (validity assured) are applicable to wallet-relying party access certificates.

GEN-6.6.1-02 [QCP-n-eudiwrp] [QCP-l-eudiwrp]**:** The requirements identified in ETSI EN 319 411-2 [4], clause 6.6.1 shall apply.

GEN-6.6.1-03 [CHOICE]: The certificate shall include at least one of the following policy identifiers:

- [NCP-n-eudiwrp]:
  - the policy identifiers (defined in clause 5.3 1); and/or
  - an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- [NCP-l-eudiwrp]:
  - the policy identifiers (defined in clause 5.3 2); and/or
  - an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- [QCP-n-eudiwrp]:
  - the policy identifiers (defined in clause 5.3 3); and/or
  - an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.
- [QCP-l-eudiwrp]:
  - the policy identifiers (defined in clause 5.3 4); and/or
  - an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.

If the wallet-relying party access certificate is issued to legal persons, then the following apply:

GEN-6.1.1-04: The CommonName field of the subject DN may be either a trade name or service name that is recognisable to the user.

GEN-6.6.1-05: The organizationIdentifier field shall be present and be encoded as specified in ETSI EN 319 412-1 [1] clause 5.1.4 taking into account to use the ISO 3166-1 [2] country code "EL" when referring to Greece where applicable.

GEN-6.6.1-06: The cpsURI under Certificate policies shall indicate a URL where the CPS of the provider of wallet-relying party access certificates is.

GEN-6.6.1-07 [CHOICE]: Contact information of the wallet-relying party, shall be at least one of the following:

- a website where the wallet-relying party can be contacted for matters pertaining to provision of helpdesk and support. This shall be included in the SAN (Subject Alternative Name) as specified in IETF RFC 5280 [i.5], clause 4.2.1.6 encoded as GeneralName type uniformResourceIdentifier;
- a phone number where the wallet-relying party can be contacted for matters pertaining to its registration and intended use of the wallet units. This shall be included in the SAN (Subject Alternative Name) as specified in IETF RFC 5280 [i.5], clause 4.2.1.6 encoded as GeneralName type otherName with the type-id `id-at-telephoneNumber` as defined in Recommendation ITU-T X.520 [i.8], clause 6.7.1;
- an email address where the wallet-relying party can be contacted for matters pertaining to its registration and intended use of the wallet unit. This shall be included in the SAN (Subject Alternative Name) email as specified in IETF RFC 5280 [i.5], clause 4.2.1.6 encoded as GeneralName type rfc822Name.

GEN-6.6.1-08: Where different instances representing the same organization require additional certificates, these may be differentiated with the use of Organizational Units (OU) in the subject DN.

GEN-6.6.1-09: The CPS of the provider of wallet-relying party access certificates shall have contact information where the wallet-relying party can be contacted for matters pertaining to its registration and intended use of the wallet units.

GEN-6.6.1-10: The wallet relying party access certificates attributes shall be derived from the information held in the register as specified in clause 5.1.2 of ETSI TS 119 475 [5].

6.6.2 CRL Profile

CSS-6.6.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.6.2 shall apply.

6.6.3 OCSP Profile

CSS-6.6.3-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.6.3 shall apply.

6.7 Compliance Audit and Other Assessment

NOTE: See ETSI EN 319 411-1 [3], clause 6.7.

6.8 Other Business and Legal Matters

6.8.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP's services.

6.8.2 Financial Responsibility

OVR-6.8.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.8.2 shall apply.

6.8.3 Confidentiality of Business Information

No policy requirement.

6.8.4 Privacy of Personal Information

OVR-6.8.4-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.8.4 shall apply.

6.8.5 Intellectual Property Rights

No policy requirement.

6.8.6 Representations and Warranties

OVR-6.8.6-01: The requirements specified in ETSI EN 319 411-1 [3], clause 6.8.6 shall apply.

6.8.7 Disclaimers of Warranties

See clause 6.8.6.

6.8.8 Limitations of Liability

Limitations on liability are covered in the terms and conditions as per clause 6.9.4.

6.8.9 Indemnities

No policy requirement.

6.8.10 Term and Termination

No policy requirement.

6.8.11 Individual notices and communications with participants

No policy requirement.

6.8.12 Amendments

No policy requirement.

6.8.13 Dispute Resolution Procedures

OVR-6.8.13-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.8.13 shall apply.

6.8.14 Governing Law

Not in the scope of the present document.

6.8.15 Compliance with Applicable Law

OVR-6.8.15-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.8.15 shall apply.

6.8.16 Miscellaneous Provisions

No policy requirement.

6.9 Other Provisions

6.9.1 Organizational

OVR-6.9.1-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.9.1 shall apply.

6.9.2 Additional testing

OVR-6.9.2-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.9.2 shall apply.

6.9.3 Disabilities

OVR-6.9.3-01: The requirements identified in ETSI EN 319 411-1 [3], clause 6.9.3 shall apply.

6.9.4 Terms and conditions

OVR-6.9.4-01: The requirements specified in ETSI EN 319 411-1 [3], clause 6.9.4 shall apply.

In addition:

OVR-6.9.4-02 [QCP-n-eudiwrp] [QCP-l-eudiwrp]: The requirements specified in ETSI EN 319 411-2 [4], clause 6.9.4 shall apply.

Annex A (informative): Bibliography

- 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).

Annex B (informative): Change history

Date	Version	Information about changes
October 2025	V1.1.1	First publication

History

Version	Date	Status
V1.1.1	October 2025	Publication