

ETSI TS 119 412-6 V1.2.1 (2026-04)



TECHNICAL SPECIFICATION

**Electronic Signatures and Trust Infrastructures (ESI);
Certificate Profiles;
Part 6: Certificate profile requirements for PID, Wallet, EAA,
QEAA, and PSBEAA providers**

Reference

RTS/ESI-0019412-6v121

Keywords

e-commerce, electronic signature, 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

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definition of terms, symbols, abbreviations and notations	7
3.1 Terms.....	7
3.2 Symbols.....	8
3.3 Abbreviations	8
3.4 Notations	8
4 PID Provider sign/seal certificate profile requirements	9
4.1 General requirements	9
4.2 Issuer	9
4.3 Subject.....	9
4.4 Extensions	9
4.4.1 Key usage.....	9
4.4.2 Subject Key Identifier.....	9
4.4.3 Authority Information Access.....	9
4.5 Indicator that the certificate is for a PID Provider sign/seal certificate	10
5 Wallet Provider sign/seal certificate profile requirements	10
5.1 General requirements	10
5.2 Indicator that the certificate is for a Wallet Provider sign/seal certificate.....	10
6 EAA Provider attribute sign/seal certificate profile requirements	10
6.1 General certificate requirements.....	10
6.2 Other requirements	10
7 QEAA Provider attribute qualified sign/seal certificate profile requirements	10
7.1 General certificate requirements.....	10
7.2 Extensions	11
7.2.1 Authority Information Access.....	11
7.3 Other requirements	11
8 PSBEAA Provider attribute issuer qualified sign/seal certificate profile requirements.....	11
8.1 General certificate requirements.....	11
8.2 Extensions	11
8.2.1 Authority Information Access.....	11
8.3 Set of data on the National or EU Law under which PSBEAA provider is established	11
8.4 Other requirements	12
Annex A (normative): ASN.1 declarations.....	13
History	14

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 6 of multi-part deliverable covering the Certificate Profiles. Full details of the entire series can be found in part 1 [i.4].

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

ITU and ISO issued standards for certification of public keys in Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3] which are used for the security of communications and data for a wide range of electronic applications.

Regulation (EU) No 910/2014 [i.5] 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.1] defines requirements on specific types of certificates named "qualified certificates". Implementation of Directive 1999/93/EC [i.1], superseded by Regulation (EU) No 910/2014 [i.5], and deployment of certificate infrastructures throughout Europe as well as in countries outside of Europe, have resulted in a variety of certificate implementations for use in public and closed environments, where some are declared as qualified certificates while others are not.

Applications need support from standardized and interoperable identity certificate profiles, in particular when applications are used for electronic signatures, authentication and secure electronic exchange in open environments and international trust scenarios, but also when certificates are used in local application contexts.

This multi-part deliverable aims to maximize the interoperability of systems issuing and using certificates both in the European context under Regulation (EU) No 910/2014 [i.5] and in the wider international environment.

1 Scope

The present document specifies requirements on the content end entity certificates issued to Person Identification Data (PID) providers, Public Sector Body's Electronic Attestation of Attributes (PSBEAA) providers, Electronic Attestation of Attributes (EAA) providers, Qualified Electronic Attestation of Attributes (QEAA) providers and Wallet providers. This profile is based on ETSI EN 319 412-2 [5] and ETSI EN 319 412-3 [6] which in turn build on IETF RFC 5280 [1] for generic profiling of Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3] and also uses IETF RFC 5755 [i.8] for attribute issuer certificate profiles.

This profile aims at supporting the requirements of the Regulation (EU) No 910/2014 [i.5] as amended by Regulation (EU) 2024/1183 [i.7]. The scope of the present document is primary limited to facilitate interoperable processing and display of certificate information. This profile therefore excludes support for some certificate information content options, which can be perfectly valid in a local context but which are not regarded as relevant or suitable for use in widely deployed applications.

The present document focuses on requirements on certificate content. Requirements on decoding and processing rules are limited to aspects required to process certificate content defined in the present document. Further processing requirements are only specified for cases where it adds information that is necessary for the sake of interoperability.

Certain applications or protocols impose specific requirements on certificate content. The present document is based on the assumption that these requirements are adequately defined by the respective application or protocol. It is therefore outside the scope of the present document to specify such application or protocol specific certificate content.

The present document aims to meet the requirements of the Regulation (EU) No 910/2014 [i.5] as amended by Regulation (EU) 2024/1183 [i.7], and architectural reference framework as available at time of preparation of the present document:

- Regulation (EU) No 910/2014 [i.5], Article 45f 1 b) requirements on qualified certificate of PSBEAA
- Regulation (EU) No 910/2014 [i.5], Annex V g) requirements on use of qualified electronic signature seal of QEAA
- Regulation (EU) No 910/2014 [i.5], Annex VII g) requirements on use of qualified electronic signature seal of PSBEAA

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] [IETF RFC 5280](#): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [2] Void.
- [3] Void.
- [4] [ETSI EN 319 412-5](#): "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

- [5] [ETSI EN 319 412-2](#): "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".
- [6] [ETSI EN 319 412-3](#): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".
- [7] [ISO 3166](#): "Codes for the representation of names of countries and their subdivisions".
- [8] [IETF RFC 3986](#): "Uniform Resource Identifier (URI): Generic Syntax".

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] [Directive 1999/93/EC](#) of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- [i.2] ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- [i.3] Recommendation ITU-T X.509 | ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
- [i.4] ETSI EN 319 412-1: "Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".
- [i.5] [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.6] ISO/IEC 18013-5:2021: "Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application".
- [i.7] [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.8] [IETF RFC 5755](#): "An Internet Attribute Certificate Profile for Authorization".
- [i.9] [IETF RFC 4519](#): "Lightweight Directory Access Protocol (LDAP): Schema for User Applications".

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 401 [i.2], ETSI EN 319 412-1 [i.4], Regulation (EU) No 910/2014 [i.5] and the following apply:

Electronic Attestation of Attributes (EAA) provider: trust service provider who provides electronic attestation of attributes

Person Identification Data (PID) provider: body responsible for ensuring that the person identification data is associated with the European Digital Identity Wallet in accordance with Article 5a(5), point (f) of Regulation (EU) No 910/2014 [i.5]

PID provider attribute sign/seal certificate: certificate corresponding to a private key used to sign the PID attribute attestations

Public Sector Body's Electronic Attestation of Attributes (PSBEAA) provider: issuer of electronic attestations of attributes by or on behalf of a public sector body responsible for an authentic source

Qualified Electronic Attestation of Attributes (QEAA) provider: qualified trust service provider who provides qualified electronic attestation of attributes

Wallet provider: provider of an European Digital Identity Wallet

Wallet provider sign/seal certificate: certificate corresponding to the private used to sign the output of the Wallet provider

3.2 Symbols

Void.

3.3 Abbreviations

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

ASN.1	Abstract Syntax Notation 1
EAA	Electronic Attestation of Attributes
OCSP	Online Certificate Status Protocol
PID	Person Identification Data
PSBEAA	Public Sector Body's Electronic Attestation of Attributes

NOTE: In other related specifications this is referred to as Pub-EAA or PubEAA.

QEAA	Qualified Electronic Attestation of Attributes
------	--

3.4 Notations

The requirements identified in the present document are preceded by a 3-letter prefix to denote the applicability to specific profiles as covered by the present multi-part deliverable.

Each requirement is identified as follows:

<3 letters profile> - < the clause number> - <2 digit number - incremental>.

The profile is identified as follows:

- **PID:** Requirements specifically applicable to PID provider certificate profiles.
- **WAL:** Requirements specifically applicable to Wallet provider certificate profiles.
- **EAA:** Requirements specifically applicable to Electronic Attribute Attestation (EAA) provider.
- **QEA:** Requirements specifically applicable to Qualified Electronic Attribute Attestation (QEAA) provider.
- **PSB:** Requirements specifically applicable to Public Sector Body Electronic Attribute Attestation (PSBEAA) provider.

The management of the requirement identifiers for 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 PID Provider sign/seal certificate profile requirements

4.1 General requirements

PID-4.1-01: All certificate fields and extensions shall comply with ETSI EN 319 412-2 [5] with the amendments specified in the present document.

PID-4.1-02: Certificate extensions shall not be marked critical unless criticality is explicitly allowed or required in the present document or in IETF RFC 5280 [1].

4.2 Issuer

PID-4.2-01: The issuer shall be:

- a) as specified in ETSI EN 319 412-2 [5], clause 4.2.3; or
- b) as defined for the subject if the certificate is selfsigned.

4.3 Subject

PID-4.3-01 [CONDITIONAL]: If the subject is a natural person the subject field shall be as specified in ETSI EN 319 412-2 [5], clause 4.2.4.

PID-4.3-02 [CONDITIONAL]: If the subject is a legal person the subject field shall be as specified in ETSI EN 319 412-3 [6], clause 4.2.1.

4.4 Extensions

4.4.1 Key usage

PID-4.4.1-01: The key usage extension shall be present and shall contain one (and only one) of the key usage settings Type A, Type B, Type C, or Type F defined in table 1 of ETSI EN 319 412-2 [5].

NOTE: Type C option is due to the requirements of ISO/IEC 18013-5 [i.6].

PID-4.4.1-02: void

4.4.2 Subject Key Identifier

PID-4.4.2-01: The subject key identifier shall be present, and shall be set as defined within IETF RFC 5280 [1], clause 4.2.1.2.

NOTE: Based on IETF RFC 5280 [1], this extension is non-critical.

4.4.3 Authority Information Access

PID-4.4.3-01 [CONDITIONAL]: If the certificate is not self signed (PID-4.2-01 option a) the Authority Information Access extension, as specified in ETSI EN 319 412-2 [5], clause 4.4.1, shall be present.

4.5 Indicator that the certificate is for a PID Provider sign/seal certificate

PID-4.5-01: The certificate shall contain at least the `qcType qcStatement` as defined in ETSI EN 319 412-5 [4], with the value `id-etsi-qct-pid` defined in Annex A of the present document.

NOTE: This means that additional `qcStatements` can be included in the certificate.

5 Wallet Provider sign/seal certificate profile requirements

5.1 General requirements

WAL-5.1-01: The requirements of clauses 4.1 to 4.4 of the present document on certificate profiles shall apply.

5.2 Indicator that the certificate is for a Wallet Provider sign/seal certificate

WAL-5.2-01: The certificate shall contain at least the `qcType qcStatement` as defined in ETSI EN 319 412-5 [4], and the values shall be set to `id-etsi-qct-wal` defined in Annex A of the present document.

NOTE: This means that additional `qcStatements` can be included in the certificate.

6 EAA Provider attribute sign/seal certificate profile requirements

6.1 General certificate requirements

EAA-6.1-01: If the Provider is a natural person ETSI EN 319 412-2 [5] on certificate profiles shall apply.

EAA-6.1-02: If the Provider is a legal person ETSI EN 319 412-3 [6] on certificate profiles shall apply.

6.2 Other requirements

EAA-6.2-01: If OCSP is used for the revocation validation of an Attribute Attestation, then the OCSP Responder certificate shall be issued (signed) by this sign/seal certificate.

EAA-6.2-02: If CRL is used for revocation of an Attribute Attestation, then the CRL shall be signed by this sign/seal certificate.

NOTE: These specifications are derived from the IETF RFC 5755 [i.8], clause 4.5.

7 QEAA Provider attribute qualified sign/seal certificate profile requirements

7.1 General certificate requirements

QEAA-7.1-01: If the Provider is a natural person ETSI EN 319 412-2 [5] on certificate profiles shall apply.

QEA-7.1-02: If the Provider is a legal person ETSI EN 319 412-3 [6] on certificate profiles shall apply.

QEA-7.1-03: The issuer of this certificate shall be a QTSP meeting the relevant regulatory requirements specified in Regulation (EU) No 910/2014 [i.5].

7.2 Extensions

7.2.1 Authority Information Access

QEA-7.2.1-01: The Authority Information Access extension as specified in ETSI EN 319 412-2 [5], clause 4.4.1, shall be present.

7.3 Other requirements

QEA-7.3-01: The requirements of clause 6.2 shall apply.

8 PSBEAA Provider attribute issuer qualified sign/seal certificate profile requirements

8.1 General certificate requirements

PSB-8.1-01: If the Provider is a natural person ETSI EN 319 412-2 [5] on certificate profiles shall apply.

PSB-8.1-02: If the Provider is a legal person ETSI EN 319 412-3 [6] on certificate profiles shall apply.

8.2 Extensions

8.2.1 Authority Information Access

PSB-8.2.1-01: The Authority Information Access extension as specified in ETSI EN 319 412-2 [5], clause 4.4.1, shall be present.

8.3 Set of data on the National or EU Law under which PSBEAA provider is established

PSB-8.3-01: The certificate shall contain the `QcPSB qcStatement`, as defined in Annex A of the present document.

PSB-8.3-02: The `QcPSB qcStatement` shall contain the identification for the law under which the PSBEAA is established responsible for the authentic source.

PSB-8.3-03 [CONDITIONAL]: If there is a well-defined Uniform Resource Identifier (URI) according to IETF RFC 3986 [8] for the unique identification of the legal basis upon which the PSBEAA is established as authentic source, it should be used here.

PSB-8.3-04: The `QcPSB qcStatement` shall contain an unambiguous identification for the authentic source.

NOTE: The identification of the authentic source, or the legally defined set of authentic sources for a specific purpose, may consist of a comma-separated list of relative distinguished names with the encoding defined in IETF RFC 4519 [i.9].

PSB-8.3-05: The `QcPSB qcStatement` shall contain either the ISO 3166 [7] alpha-2 country codes for applicable law, or in the case of European Union law 'EU'.

NOTE: The identifier is in the form as appropriate to national or European Union legislation.

8.4 Other requirements

PSB-8.4-01: The requirements of clause 6.2 shall apply.

Annex A (normative): ASN.1 declarations

```

ETSIQCstatementsMod { itu-t(0) identified-organization(4) etsi(0) qct-extension(194126) id-
mod(0) id-mod-qc-statements-extension(0) v1(0)}

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS All -

IMPORTS

QC-STATEMENT, qcStatement-2
    FROM PKIXqualified97 {iso(1) identified-organization(3) dod(6)
        internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
        id-mod-qualified-cert-97(35)};

-- new QC type identifiers
id-etsi-eidas2-qct-extensions OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)
qct-extension (194126) 1 }

id-etsi-qct-pid   OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 1 }
-- Certificate for PID provider sign/seal certificate

id-etsi-qct-wal   OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 2 }
-- Certificate for Wallet provider sign/seal certificate

-- PSB certificate mandatory data
id-etsi-qcs-QcPSB OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 }

    esi4-qcStatement-10 QC-STATEMENT ::= { SYNTAX QcPSB IDENTIFIED
    BY id-etsi-qcs-QcPSB }

QcPSB ::= SEQUENCE {
    countryOfLegislation      PrintableString (SIZE (2))
(CONSTRAINED BY { -- ISO 3166 alpha-2 country codes or 'EU' -- }),
    -- this field shall contain the alpha-2 country code of the legislation framework of public
sector body
    -- In the case of European Union law 'EU' shall be used in place of the country code

    authSourceIdentification  UTF8String,
    -- this field is for the unique identification of authentic source

    legislationIdentification  UTF8String
}

END

```

History

Version	Date	Status
V1.1.1	September 2025	Publication
V1.2.1	April 2026	Publication