ETSI TS 119 412-1 V1.4.0 (2020-04)

Electronic Signatures and Infrastructures (ESI);
Certificate Profiles;
Part 1: Overview and common data structures

Reference
RTS/ESI-0019412-1v140

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

The present document is part 1 of a multi-part deliverable covering the Certificate Profiles, as identified below:

ETSI TS 119 412-1: "Overview and common data structures";

ETSI EN 319 412-2: "Certificate profile for certificates issued to natural persons";

ETSI EN 319 412-3: "Certificate profile for certificates issued to legal persons";

ETSI EN 319 412-4: "Certificate profile for web site certificates";

ETSI EN 319 412-5: "QCStatements".

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 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.9] 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 defines requirements on specific types of certificates named "qualified certificates". Implementation of Directive 1999/93/EC [i.1], superseded by the Regulation (EU) No 910/2014 [i.9], 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 certificates 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 the Regulation (EU) No 910/2014 [i.9] and in the wider international environment.

1 Scope

The present document provides an overview of the Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3] based certificate profiles and the statements for EU Qualified Certificates specified in other parts of ETSI EN 319 412 [i.4] to [i.7]. It specifies common data structures that are referenced from other parts of ETSI EN 319 412 [i.4] to [i.7].

The profiles specified in this multi-part deliverable aim to support both the Regulation (EU) No 910/2014 [i.9] and use of certificates in a wider international context. Within the European context, it aims to support both EU Qualified Certificates and other forms of certificate.

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 at https://docbox.etsi.org/Reference/.

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 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[2] ISO 3166: "Codes for the representation of names of countries and their subdivisions".

[3] ETSI TS 119 495: "Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366".

[4] ISO 17442: "Financial services - Legal Entity Identifier (LEI)".

[5] eIDAS SAML Attribute Profile v1.2, 31 August 2019.

NOTE: Available at https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf?version=2&modificationDate=1571068651772&api=v2

[6] IETF RFC 5912: "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)".

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] 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 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 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons".

[i.5] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for certificates issued to legal persons".

[i.6] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate Profile for web site certificates".

[i.7] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.8] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.9] 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.10] Recommendation ITU-T X.520 (10/2012): "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[i.11] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.12] Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

[i.13] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 319 401 [i.2] and the following apply:

EU Qualified Certificate: qualified certificate that is stated to be in accordance with Annex I, III or IV of the Regulation (EU) No 910/2014 [i.9] or annex I of the Directive 1999/93/EC [i.1] whichever is in force at the time of issuance

short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the certificate practice statement

3.2 Symbols

Void.

3.3 Abbreviations

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

ASN.1 Abstract Syntax Notation 1
CA Certification Authority

OID Object IDentifier
LEI Legal Entity Identifier
TLS Transport Layer Security protocol

NOTE: As specified in IETF RFC 5246 [i.8].

SAML Security Assertion Markup Language
TSP Trust Service Provider
UN United Nations

4 ETSI EN 319 412 certificate profiles

4.1 General approach

All the certificate profiles specified in ETSI EN 319 412 are based upon IETF RFC 5280 [i.11] for generic profiling of Recommendation ITU-T X.509 | ISO/IEC 9594-8 [i.3]. The certificate profiles specify profiles for both EU Qualified Certificates and non-qualified certificates as relevant. Reference is made to ETSI EN 319 412-5 [i.7] for requirements relating to `QCStatements`.

4.2 Overview of other parts of ETSI EN 319 412

4.2.1 ETSI EN 319 412-2

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

Scope: This part specifies the requirements on certificate content for TSPs issuing certificates to natural persons. It provides a certificate profile, which facilitates interoperability of certificates issued to natural persons for the purposes of supporting digital signatures, peer entity authentication, data authentication as well as data confidentiality. It specifies a profile for both EU Qualified Certificates as specified in the Regulation (EU) No 910/2014 [i.9], and non-qualified certificates. When certificates for natural persons are issued as EU Qualified Certificates, it makes reference to ETSI EN 319 412-5 [i.7] for requirements relating to `QCStatements`.

4.2.2 ETSI EN 319 412-3

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

Scope: This part specifies the requirements on certificate content for TSPs issuing certificates to legal persons. It provides a certificate profile, which facilitates interoperability of certificates issued to legal persons for the purposes of supporting digital signatures, peer entity authentication, data authentication as well as data confidentiality. It specifies a profile for both EU Qualified Certificates and non-qualified certificates. When certificates for legal persons are issued as EU Qualified Certificates, it makes reference to ETSI EN 319 412-5 [i.7] for requirements relating to `QCStatements`.

4.2.3 ETSI EN 319 412-4

Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

Scope: This part specifies the requirements on certificate content for TSPs issuing website certificates for sites that are accessed via the TLS protocol [i.8]. It provides a certificate profile, which enables interoperability of website certificates issued to legal or natural persons. It specifies a profile for both EU Qualified Certificates and non-qualified certificates. When certificates for web site authentication are issued as EU Qualified Certificates, it makes reference to ETSI EN 319 412-5 [i.7] for requirements relating to `QCStatements`.

4.2.4 ETSI EN 319 412-5

Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles ; Part 5 : QCStatements.

Scope: This part specifies the requirements on the `QCStatements` as required for qualified certificates as specified in parts 2 to 4 [i.4], [i.5] and [i.6] of ETSI EN 319 412.

The `QCStatements` defined in clause 4.3 of ETSI EN 319 412-5 [i.7] may be applied to regulatory environments outside the EU. Other requirements specified in clause 4 are specific to Regulation (EU) No 910/2014 [i.9] but may be adapted for other regulatory environments.

5 Common data structures

5.1 Semantics identifiers

5.1.1 General

Subject and issuer names (X.509 [i.3]) can include attributes that do not disclose the semantics of its information content. `serialNumber` (X.509 [i.3]) and `organizationIdentifier` (X.520 [i.10]) are examples of such attributes. The `serialNumber` attribute can contain a national identification number, passport number or any type of locally defined identifier such as random or pseudo-random generated identifier. The `organizationIdentifier` attribute can contain several types of organizational identifiers.

IETF RFC 3739 [1], clause 3.2.6.1 defines the predefined statement "qcStatement-2" identified by the OID id-qcs-pkixQCSyntax-v2 with the `SemanticsInformation` syntax.

The `SemanticsInformation` type, when present, provides information about the semantics of data stored in attributes and/or names in the certificate.

The semantics identifiers in the following clauses use 2 character ISO 3166 [2] country codes (Alpha-2) to specify the country where the identifier is registered. Trans-national country codes as specified in ISO 3166 [2] may be used when relevant such as EU (European Union) and UN (United Nations). User-defined country code 'XG' may be used for identifiers allocated under a global scheme. Identifiers using user-defined country codes shall be interpreted under the context of the certificate issuer as there is no guarantee that such identifier is unique across all issuers. Unassigned codes should not be used.

NOTE: The semantics identifiers in the following clauses define semantics information for attributes stored in the subject field. No corresponding mechanism is defined in the present document for specifying semantics information for attributes in the issuer field. IETF RFC 5280 [i.11] path validation requires the issuer field to be consistent with the subject field of the CA certificate assigned to the issuing CA. Name attributes of the issuing CA can be constructed according the semantics identifier defined in the following clauses and stored in the subject field of the CA certificate. In such case, the appropriate place to include semantics identifiers for these attributes is in the CA certificate. Consequently, a relying party will have to consult information in the issuing CA certificate to obtain semantics information about attributes in the issuer field of a certificate.

5.1.2 ASN.1 module

This clause defines semantics identifiers for inclusion in qcStatement-2.

The syntax for the natural person semantics identifier and legal person semantics identifier shall be as defined by the following ASN.1 module:

```
ETSISemanticsIdentifierMod { itu-t(0) identified-organization(4) etsi(0) id-cert-
profile(194121) id-mod(0) id-mod-semantics-identifier(0) v2(1)}


DEFINITIONS EXPLICIT TAGS::=

BEGIN

-- EXPORTS All -

-- Semantics identifiers

id-etsi-qcs-semantics-identifiers     OBJECT IDENTIFIER ::= { itu-t(0) identified-
organization(4) etsi(0) id-cert-profile(194121) 1 }

-- Semantics identifier for natural person identifier

id-etsi-qcs-semanticsId-Natural     OBJECT IDENTIFIER ::= { id-etsi-qcs-semantics-
identifiers 1 }

-- Semantics identifier for legal person identifier

id-etsi-qcs-SemanticsId-Legal     OBJECT IDENTIFIER ::= { id-etsi-qcs-semantics-
identifiers 2 }

-- Semantics identifier for eIDAS natural person identifier
id-etsi-qcs-semanticsId-eIDASNatural OBJECT IDENTIFIER ::= { id-etsi-qcs-semantics-
identifiers 3 }

-- Semantics identifier for legal person identifier
id-etsi-qcs-SemanticsId-eIDASLegal  OBJECT IDENTIFIER ::= { id-etsi-qcs-semantics-
identifiers 4 }

END
```

The following clauses provide the semantics definitions of the natural person and legal person semantics identifiers.

5.1.3 Natural person semantics identifier

The semantics of `id-etsi-qcs-SemanticsId-Natural` shall be as follows.

When the natural person semantics identifier is included, any present `serialNumber` attribute in the subject field shall contain information using the following structure in the presented order:

- 3 character natural person identity type reference;
- 2 character ISO 3166 [2] country code;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- identifier (according to country and identity type reference).

The three initial characters shall have one of the following defined values:

1) "PAS" for identification based on passport number.
2) "IDC" for identification based on national identity card number.
3) "PNO" for identification based on (national) personal number (national civic registration number).

4) "TAX" for identification based on a personal tax reference number issued by a national tax authority. This value is **deprecated.** The value "TIN" should be used instead.

5) "TIN" Tax Identification Number according to the European Commission - Tax and Customs Union (https://ec.europa.eu/taxation_customs/tin/tinByCountry.html).

6) Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).

Other initial character sequences are reserved for future amendments of the present document.

EXAMPLES: "PASSK-P3000180", "IDCBE-590082394654" and "EI:SE-200007292386".

When a locally defined identity type reference is provided (two characters followed by ":"), the `nameRegistrationAuthorities` element of `SemanticsInformation` (IETF RFC 3739 [1]) shall be present and shall contain at least a `uniformResourceIdentifier` `generalName`. The two letter identity type reference preceding the ":" character shall be unique within the context of the specified `uniformResourceIdentifier`.

5.1.4 Legal person semantics identifier

The semantics of `id-etsi-qcs-SemanticsId-Legal` shall be as follows.

When the legal person semantics identifier is included, any present `organizationIdentifier` attribute in the subject field shall contain information using the following structure in the presented order:

- 3 character legal person identity type reference;
- 2 character ISO 3166 [2] country code;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- identifier (according to country and identity type reference).

The three initial characters shall have one of the following defined values:

1) "VAT" for identification based on a national value added tax identification number.

2) "NTR" for identification based on an identifier from a national trade register.

3) "PSD" for identification based on national authorization number of a payment service provider under Payments Services Directive (EU) 2015/2366 [i.13]. This shall use the extended structure as defined in ETSI TS 119 495 [3], clause 5.2.1.

4) "LEI" for a global Legal Entity Identifier as specified in ISO 17442 [4]. The 2 character ISO 3166 [2] country code shall be set to 'XG'.

5) Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).

Other initial character sequences are reserved for future amendments of the present document. In case "VAT" legal person identity type reference is used in combination with the "EU" transnational country code, the identifier value should comply with Council Directive 2006/112/EC [i.12], article 215.

EXAMPLES: "VATBE-0876866142" and "EI:SE-5567971433".

When a locally defined identity type reference is provided (two characters followed by ":"), the `nameRegistrationAuthorities` element of `SemanticsInformation` (IETF RFC 3739 [1]) shall be present and shall contain at least a `uniformResourceIdentifier` `generalName`. The two letter identity type reference following the ":" character shall be unique within the context of the specified `uniformResourceIdentifier`.

5.1.5 eIDAS Natural person semantics identifier

The semantics of `id-etsi-qcs-SemanticsId-eIDASNatural` shall be as follows.

When the eIDAS natural person semantics identifier is included, the values of attributes in the subject field shall meet the content requirements of corresponding attributes defined by the eIDAS SAML attribute profile [5] according to the following requirements.

- Any `serialNumber` attribute present in the subject field of the certificate shall comply with the content requirement specified for the eIDAS `PersonIdentifier` attribute .
- Attributes present in subject field of the certificate are equivalent to defined attributes in accordance with table 5.1.5-1. This means that the present attribute shall hold equivalent information, even if the format used to express that information differs.

Table 5.1.5-1: Attribute equivalence

Certificate attribute	Defined by	Equivalent eIDAS attribute (FriendlyName)
`serialNumber`	Recommendation ITU-T X.520 [i.10]	`PersonIdentifier`
`surname`	Recommendation ITU-T X.520 [i.10]	`FamilyName`
`givenName`	Recommendation ITU-T X.520 [i.10]	`FirstName`
`dateOfBirth`	IETF RFC 3739 [1]	`DateOfBirth`

5.1.6 eIDAS Legal person semantics identifier

The semantics of `id-etsi-qcs-SemanticsId-eIDASLegal` shall be as follows.

When the eIDAS legal person semantics identifier is included, the values of attributes in the subject field shall meet the content requirements of corresponding attributes defined by the eIDAS SAML attribute profile [5] according to the following requirements:

- Any `organizationIdentifier` attribute present in the subject field of the certificate shall comply with the content requirement specified for the eIDAS `LegalPersonIdentifier` attribute.
- Attributes present in the subject field of the certificate are equivalent to defined attributes in accordance with table 5.1.6-1. This means that the present attribute shall hold equivalent information, even if the format used to express that information differs.

Table 5.1.6-1: Attribute equivalence

Certificate attribute	Defined by	Equivalent eIDAS attribute (FriendlyName)
`organizationIdentifier`	Recommendation ITU-T X.520 [i.10]	`LegalPersonIdentifier`
`organizationName`	Recommendation ITU-T X.520 [i.10]	`LegalName`

5.2 Certificate Extensions regarding Validity Assured Certificate

5.2.1 Validity Assured General

The following certificate extensions indicate that the certificate issuer ensures that the validity of the certificate is assured at time of use of the corresponding private key.

NOTE 1: Upon presence of such statement in the certificate, the relying party can decide not to check the certificate revocation status, for example, when validating a digital signature.

NOTE 2: The upper part of the certificate path is not impacted by the presence of the extension in a certain certificate; upper certificates in the chain are to be validated as expressed by the certificate and/or the certificate policy/certificate practice statement (e.g. they can be validated with OCSP or CRL).

NOTE 3: In the present document only one extension is defined.

5.2.2 Validity Assured - Short Term

This extension indicates that the validity of the certificate is assured because the certificate is a "**short-term certificate**". That is, the time as indicated in the certificate attribute from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified by the certificate practice statement or certificate policy.

5.2.3 ASN.1 Module

The ASN.1 module defined in the present clause shall import the types and structures from IETF RFC 5912 [6] as written in the import part of the module.

```
ETSIValAssuredCertMod
    { itu-t(0) identified-organization(4) etsi(0) id-cert-profile(194121) id-mod(0)
    id-mod-validity-assured(1) v1(0) }

BEGIN

-- EXPORTS All --

IMPORTS

EXTENSION
FROM PKIX-CommonTypes-2009
    { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5)
           pkix(7)
    id-mod(0) id-mod-pkixCommon-02(57) }

-- Extensions

id-etsi-ext   OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)
                                     id-cert-profile(194121) 2 }

    -- Extension for short-term certificate

    id-etsi-ext-valassured-ST-certs     OBJECT IDENTIFIER ::= { id-etsi-ext 1 }

    ext-etsi-valassured-ST-certs    EXTENSION ::= { SYNTAX NULL IDENTIFIED BY
                                                    id-etsi-ext-valassured-ST-certs }

END
```

Annex A (informative): Change History

Date	Version	Information about changes
February 2016	1.1.1	Publication as ETSI EN 319 412-1
March 2018	1.1.2	1. Clause 5.1.4 Legal person semantics identifier add to list of initial characters. 3) "PSD" for identification based on national authorization number of a payment service provider under Payment Services Directive (EU) 2015/2366. This uses the extended structure as defined in ETSI TS 119 495, clause 5.2.1. 2. Clause 5.1.4 change numbering of current item 3) to item 4) 3. Add to clause 2.1 Normative references: ETSI TS 119 495 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU.
May 2018	1.2.1	Publication as ETSI TS 119 412-1 (same technical content as V1.1.2)
July 2019	1.2.2	Integration of CR ESI(18)64_017 to include LEIs
August 2019	1.3.1	Publication as ETSI TS 119 412-1
December 2019	1.3.2	Aligning EN with TS text and integrating CR on eID representation in ESI(17)59_061 & CR on validity assured certificates in ESI(19)68_073r4
January 2020	1.3.3	CR on country codes in ESI(20)69_007r1.
March 2020	1.3.4	Editorial corrections and update of reference [5] Version approved by TC ESI for submission to EN Approval Procedure
March 2020	1.3.5	Same version as 1.3.4 approved as TS
April 2020	1.4.0	Publication as TS

History

Document history		
V1.0.1	July 2015	Publication (Withdrawn)
V1.1.1	February 2016	Publication as ETSI EN 319 412-1
V1.2.1	May 2018	Publication
V1.3.1	August 2019	Publication
V1.3.4	March 2020	Approval Procedure AP 20200618: 2020-03-20 to 2020-06-18 (ETSI EN 319 412-1)
V1.4.0	April 2020	Publication