Resolution of public comments on Draft ETSI *EN* 319 412-X (2015-01)

Public Review: comments on Draft ETSI *EN* 319 412-1 V0.0.10 (2015-01)

ESI Certificate Profiles; Part 1: Overview and common data structures

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
A	**5.1.3**		**General**	Natural person semantic identifiers are defined, whereas the eIDAS minimum data set on person identification is being defined in parallel (Art. 12. 4 (d), Implementing Act to be established by Sept. 18th, i.e. text being available soon). Defining semantic identifiers in EN 319 412-1 will lead to a situation where trust services person identifiers deviate from / are inconsistent with eIDAS eID identifiers.	Cease definition of semantic identifiers and await availability of eIDAS eID minimum data set. Align semantic identifiers to this Implementing Act.	**No change** **We can't do anything until the Implementing act has been finalised and we can't assume any publication date.** **If the implementing act just focuses on minimum dataset, then this should not impact the current definition of semantics identifier.** **This could delay publication beyond current deadlines, and it is not clear whether the regulation will have any impact on the content of this clause.** **No change**
A	**5.1.4**		**General**	As above legal person semantic identifiers are defined, whereas the eIDAS minimum data set on person identification is being defined in parallel (Art. 12. 4 (d), Implementing Act to be established by Sept. 18th, i.e. text being available soon). Defining semantic identifiers in EN 319 412-1 will lead to a situation where trust services person identifiers deviate from /	Cease definition of semantic identifiers and await availability of eIDAS eID minimum data set. Align semantic identifiers to this Implementing Act.	**No change** **see above**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				are inconsistent with eIDAS eID identifiers. The legal person identifiers are also somehow arbitrary and (by just using VAT and trade registers) by far not covering the various identifier schemes in use.		

Public Review: Comments on Draft ETSI EN 319412-1 V0010

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

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
B	**5.1.4**		**General**	**Only 3 legal person identity type references are possible, VAT, NTR, and country local specific definition.** **We have the opinion that it must be possible to use trans-national identification standards for organisations, and not only country local.** **Examples of such a trans-national identifiers are the ISO 17442 Legal Entity Identifier (LEI, already referred to as an recognised international identification system for organisations by other EU regulations such as EMIR,**	**In the paragraph starting with "The three initial characters shall have …", add an item 10), or edit item 9), to allow a trans-national scheme with associated name registration authority.**	**Agree. Similar concern may occur with UN, EU, Red Cross identifier** **New text:** The semantics identifiers in the following clauses use ISO 3166 [2] country codes 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 codes (AA, QM-QZ, XA-XZ and ZZ) may be used for other trans-national identifiers. Identifiers using user-defined country codes shall be interpreted under the context of the certificate issuer as there is no guarantee

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				MIFID II/MiFIR, EIOPA), and the ISO 9362 Business Identifier Code (BIC).		that such identifier is unique across all issuers.

Public Review: Comments on Draft ETSI EN 319 412-1 V0.0.10 (2015-01)

Certificate Profiles; Part 1: Overview and common data structures

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
C	**5.1.2**		**General**	**There are no semantics identifier for a natural person identified in association with a legal person described in ETSI EN 319 411-1 clause 4.5 b)** **The identifier for natural person (ETSI EN 319 411-1 clause 4.5 a)) may be used but the corresponding certificate profile for natural person (ETSI 319 412-2 does not specify how the association with a legal person should be encoded in the certificate. This may lead to lack of harmonization between Member States where certificates are issued to natural persons identified in association**	**A semantics identifier for a natural person identified in association with a legal person should be defined.** **A corresponding standard for a certificate profile for natural persons identified in association with a legal person in the ETSI EN 319 412-x series should be defined or the profile for natural person (ETSI 319 412-2) should be extended.**	**Text clarified** **This case is already covered by having two subject attributes. The OrganizationIdentifier attribute can provide an identifier of the organization while the serialNumber attribute can identify the person within that organization.** **Add note to 5.2.6. in 412-2 that organizationalIdentifer and serialNumber may be used in natural person certificates subject field in combination with organizational attributes such as organizationName and organizationIdentifier.**

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
				with a legal person.		
C	**5.1.2**		**General**	**There are no semantics identifier for devices or systems operated by or on behalf of a natural or legal person described in ETSI EN 319 411-1 clause 4.5 d)**	**A semantics identifier for devices or systems operated by or on behalf of a natural or legal person should be defined.** **A corresponding standard for a certificate profile for devices or systems in the ETSI EN 319 412-x series should be defined.**	**We have no certificate profile for devices.** **No change**

Email from D: Tue 10/02/2015 09:39

Certificate Profiles; Part 2: 5.2.4.1 Legal person issuers

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
D	**5.2.4.1**	**N/A**	**Editorial**	**The organizationIdentifier is somehow "equivalent" to the organization unit? or can this last be used as the organization identifier?**		No change - organization unit specifies a part of an organization under the organization name. organization identifier identifies the entire organization

Public Review: Comments on Draft ETSI EN 319 412-2 V2.0.12 (2015-01)

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

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
E			**General**	**Art. 28 (3) of the Regulation Nr. 910/2014 (eIDAS Regulation) provides that "Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures."** **In order to ensure interoperability, the handling of such extensions should be regulated.**	**Add a note in 5.1:** **A non-mandatory extension representing an additional specific attribute (e.g. a professional attribute like "Physician" or "Lawyer") may be present. This extension shall not be marked as critical. A client that does not implement this extension can safely ignore it. The validity of a signature shall not be affected solely based on the presence or absence of this extension.**	**The document already states that additional attributes may be present. Criticality is not a property of subject distinguished name attributes.** **No change**
E	**A.5.1**	**RFC6960** **[i.3]**	**General**	**RFC6960 provides in Clause 4.2.2.2 that when delegating OCSP signing, "This certificate MUST be issued directly by the CA that is identified in the request.". If a CA certificate is revoked or no longer valid, there is no OCSP signer that can provide information about the status of any EE certificate issued by that CA. This is contrary to Art. 24 (4) of the eIDAS Regulation ("…and beyond the validity period of the certificate…").**	**Add a note:** **When using Trusted Service Lists (TSL), in derogation from [i.3] Clause 4.2.2.2, an OCSP signer is authoritative for a particular EE certificate if it is registered as TSP Service in the same TSP Information Element as the CA that issued the EE certificate.**	**This goes beyond the scope of a certificate profile.** **This comment should be taken into account in the proposed new work on revocation information profiles including OCSP.** **No change**

Public Review: Comments on Draft ETSI *EN* 319 412-2 V2.0.2 (2015-01)

ESI Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
A	**5.2.6**		**General**	A subject serialNumber is defined mandatory, which creates several issues: - It exceeds what is required under eIDAS for qualified certificates, as just the person's name or a pseudonym is needed (Annex I c) - It violates data protection regulations and data minimisation principles, in particular as EN 319 412-1 includes national identifiers which are under particular data protection regimes - It ignores the Council negotiations where inclusions of identifiers in qualified certificates has intensively been discussed and the decision was to NOT include such identifiers. - It ignores the separation of eID and trust services introduced in eIDAS In its current form EN 319 421-2 cannot be used for qualified certificates.	The Subject serialNumber SHALL NOT be mandatory,	**Text clarified** **The comment seems to misunderstand the requirement for a present attribute and assumes this to be requirement for a particular type of identifier.** **The identifier could be a random generated number by the CA. It is just something that makes that certificate subject name unique.** **Added clarifying text on serialNumber :** The `serialNumber` attribute has no defined semantics beyond ensuring uniqueness of subject names. It may contain a number or code assigned by the CA or an identifier assigned by a government or civil authority. It is the CA's responsibility to ensure that the `serialNumber` is sufficient to resolve any subject name collisions.

Public Review: Comments on Draft ETSI EN 319 412-2 V2.0.12 (2015-01)

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

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
F			**General**	**eIDAS Regulation allows to include non-mandatory additional specific attributes. In order to ensure interoperability, the handling of these extensions should be regulated.** **Any attribute extension shall conform with X.509 or RFC 5480.**	**Add a note in 5.1** **Any other compliant withX.509 or RFC 5480 extension not listed in the EN 319412-x documents shall not be marked critical.** **A client not implementing such an extension can safely ignore it. The validity of a signature shall not depend on the fact that such an extension is present or not.**	**Text clarified** **Mixing up extensions with attributes.** **Requirement to not allow other extensions to be critical could be valid.** **Text added to clause 5.1 on criticality.**
F			**General**	**There are some references outdated, e.g. RFC 3279, which has are some followers and updaters (4055, 4491, 5480, 5758). As they are all related to algorithms it is suggested to refer to the Algo Paper TS 119 312 for guidance.**	**Check whether references (informative and normative) to algorithms can be removed.**	**Agree** **Remove reference to 3739 and make a reference to the algo paper (TS 119 312)**

Public Review: Comments on Draft ETSI <*EN*> <ETSI 319412-2> V<2.0.12>

<*Deliverable Title*>

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
G	**A.2.3**		**T**	"Requirement or Recommendation" – it is difficult to understand this part, since it is not in the sentence form. We do not understand is SHA256WithRSA mandatory or recommended? If mandatory, why the usage of ECC (elliptic curve cryptography) keys is not an option?	ECC respective keys should be an option if this is mandatory requirement.	Agree with changes Text deleted. TS 119 312 referenced for guidance on algorithms

Public Review: Comments on Draft ETSI EN 319 412-3 V2.0.10 (2015-01)

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

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
H			**General**	**We strongly encourage you to consider requiring a universal legal entity identifier (the LEI) that would more easily allow identification of entities for certification issued by legal entities and we believe the LEI would best achieve the objective of entity identification as compared with other options.**		No change Any legal person identifier can be stored in the current draft. The mechanisms defined in part 1 allow an entity to specify that the identifier holds a LEI identifier. In particular with the change proposed to allow transnational identifiers.

Public Review: Comments on Draft ETSI <*EN*> <*ETSI 319412-3*> V<0.0.10>

<*Deliverable Title*>

Organization name	**Clause/ Subclause**	**Paragraph Figure/ Table**	**Type of comment** (General/ Technical/Editorial)	**COMMENTS**	**Proposed change**	**RESOLUTION** on each comment submitted
G	**4.2.1**		**T**	Why the organizationIdentifier field is containing an identification of the certificate issuing organization whereas the clause is about subject dn? Probably it should contain an identification of the subject?		Text clarified The text is in error. The text should as suggested specify the use of this attributes for providing an organizational identifier of the subject organization.
G	**4.2.1**		**T**	It is a bit confusing - if certificate shall contain organizationIdentifier field and certificates may include one or more semantics identifiers as specified in clause 5 of EN 319 412-1, then which other options would be available? You cannot use this field with the exactly same name in the certificate (it is same for 312 412-2 p. 5.2.4.1). ETSI 319 422 refers that the explanation can be found in X.520. The same reference could be used also for ETSI 312412-2 and 3: (For legal person, an organizationIdentifier attribute should be used as defined in X.520 [i.4].)	Add the reference to the organizationIdentifier attribute (For legal person, an organizationIdentifier attribute should be used as defined in X.520 [i.4].)	No change This comment seems to be based on a misunderstanding. X.520 defines the attribute as a text string that may hold any data. The semantics identifier further specifies conventions for how this string may be constructed. This is not in conflict with X.520 as the semantics identifier is compatible with the generic definition in X.520.

Public Review: Comments on Draft ETSI EN 319 412-4 V0.0.11 (2015-01)

Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations

Organization name	Clause/ Subclause	Paragraph Figure/ Table	Type of comment (General/ Technical/Editorial)	COMMENTS	Proposed change	RESOLUTION on each comment submitted
C	**Title page**	**N/A**	**Editorial**	**The identification of the standard "Draft EN 319 412-4 V0.0.11 (2015-01)" is missing the word "ETSI"**	**"Draft ETSI EN 319 412-4 V0.0.11 (2015-01)"**	Agree Add "ETSI"

I comments

412-4:

- intro, 5th para: remove the whole paragraph to align the introduction with the other parties
- 2, 2nd line: For specific references,only => For specific references, only [i.e. blank missing]
- 2.2, [i.5]: why part 1 is referred to as informative (given that definitions and abbreviations are incorporated by reference from it and it can include semantic identifiers, see 4.1)??
- 4.2, title: EU Qualified certificate => EU Qualified Certificate
- 4.2, 1st line: EU qualified certificates => EU Qualified Certificates
- 4.2, 1st line: shall include qualified certificate statements as specified => shall include COURIER[QCstatement]s as specified
- 4.2, 1st line: as specified in clause 4 of EN 319 412-5 => as specified in clause 4 and 5 of EN 319 412-5
- 4.3, 1st line: EU Qualified certificates => EU Qualified Certificates

412-3:

- 1, 1st para, 2nd line: defined in part 2 of EN 319 412 [4] => update the reference number
- 1, 2nd para, 1st line: EU qualified certificates => EU Qualified Certificates
- 1, 2nd para, 1st line: Regulation (EU) No 910/2014 [8] => update the reference number

412-2:

- 5.2.4.1, 3rd para: countryName => COURIER[countryName]
- 5.2.4.1, 4th para: organizationName => COURIER[organizationName]
- 5.2.4.1, 4th para, 3rd line: of EN 319 412-1 [i.7] => why an informative reference, since the semantic identifiers can be incorporated from part 1?
- 5.2.4.1, NOTE: commonName => COURIER[commonName]
- 6, title: EU Qualified certificate requirements => EU Qualified Certificate requirements
- 6.1, title: EU Qualified Certificate Statements => EU Qualified Certificate statements
- 6.1, 1st line: EU Qualified certificates => EU Qualified Certificates
- 6.1, 1st line: qualified certificates statements => COURIER[QCstatement]s
- 6.2, 2nd line: EU qualified certificates => EU Qualified Certificates
- 6.2, 3rd line: Qualified Certificate Statements => COURIER[QCstatement]s

412-1:

- 1, 2nd para, 2nd line: EU qualified certificates => EU Qualified Certificates
- 4.1: there is a reference to ITU X.509 for all 412 parts while 412-2 explicitly builds on RFC5280 (that was a decision of ESI#48(bis) => fix this and make coherent in all parts
- 4.2: replace everywhere 'qualified certificate statements' with 'COURIER[QCstatement]s'
- 4.2: replace everywhere 'qualified certificate' with 'EU Qualified Certificate'
- 4.2.3, scope, 5th line: legal persons => web site authentication
- 4.2.4: replace everywhere 'QCstatements' with 'COURIER[QCstatement]s'
- the rest of the document was not reviewed