Guidance for the application of the Qualified certificates for electronic signatures and electronic Seals which support the eIDAS Regulation

Note on using the guidance: examples are used throughout – they are not normative or exclusive, but there to make the guidance easier to understand as points of reference.

ARTICLE 28

Art.28.1 Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.

GUIDANCE :

Guidance related to Annex 1 is provided further in this document.

Art. 28.2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.

No specific guidance given at this time.

Art. 28.3. 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.

GUIDANCE:

Certificates format allows to add, within the certificate, non-mandatory specific attributes, expressing, for example, the locality of the organization or the Organizational Unit the physical person is attached to..We provide example of non-mandatory additional specific attributes that may affect or may not affect the interoperability.

*Examples of non-mandatory additional specific attributes that **do not affect** the interoperability may include:*

- *Any additional standard attributes in Subject or Issuer field such as:*
  - *Organizational Unit*
  - *State or Province Name*
  - *Locality*
  - *Title*
- *Additional extensions such as*
  - *Subject Key Identifier*
  - *Authority Key Identifier*

- *Certificate policies extension*
- *Extended key usages*

Examples of non-mandatory additional specific attributes that <u>may affect</u> the interoperability may include:

- *Any extended key usage extension or proprietary extension set as critical in the certificate.*

Art 28.4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

No specific guidance given at this time.

Art 28.5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:

GUIDANCE :

Due to the actual state of art of the industry regarding the verification of signature, and particularly the fact that the majority of verification tools are unable to verify the validity of a signature generated by a certificate that has been temporarily suspended, it is recommended that each Member State forbids the practice of temporary suspension of a qualified certificate for electronic signature. However, if Members States still lay down national rules on temporary suspension, we suggest that verification mechanisms able to handle the suspension are provided together with the authorization to suspend qualified certificates.

(a)if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;

No specific guidance given at this time.

(b)the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

No specific guidance given at this time.

6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

No specific guidance given at this time.

ANNEX 1.

GUIDANCE:

Annex 1 provides a list of ten requirements that shall be fulfilled by the Qualified TSP. There are divergent ways for a TSP to fulfil these requirements. The purpose of this guidance is to allow TSP that want to use convergent implementations of these requirements to do so. For each requirement, this guidance includes:

- Contextual information about the requirement (aim, scope, mandatory elements, optional elements)
- The technical elements that have to be included to be compliant to the requirement
- The standards that exist and can be applied to ensure compliance to the requirement and to maximize interoperability
- A rationale explaining how these standards meet the requirement.
- When applicable, additional guidance on how to apply the standard in conformance with the regulation.

This guidance targets three different objectives:

- automatic legal compliance to eIDAS Regulation for TSPs choosing to follow the guidance;
- largest possible certificates uses for TSPs choosing to follow the guidance;
- maximized usage of European certificates for users and third parties, thanks to TSPs convergent implementations.

Annex 1. Qualified certificates for electronic signatures shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;

GUIDANCE :

When receiving a certificate and an electronic signature, it is important for Users and Third Parties to easily identify if this certificate is qualified or not. Therefore, it is mandatory for TSP to provide, within the certificate, if it is qualified or not.

The regulation let the TSP to freely choose the way to indicate if a certificate is qualified or not, as long as the form is suitable for an automated process. However, to enhance the interoperability between the TSP, adoption of a common way to provide this indication is recommended, since multiple mechanisms for indicating the qualification of a certificate means more complexity for any service provider for verifying the signatures. [ETSI EN 319 412-5] provides certificate extension, suitable for an automated process, that complies with this requirement of the Regulation. A TSP issuing qualified certificates compliant with [ETSI EN 319 412-5] fulfils this requirement of the regulation and issues certificates that may be more easily be accepted by the industry.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding information about the qualification of the certificate, to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary:

[ETSI EN 319 412-5] specifies the qcStatements certificate extension, that provide the information that the certificate is issued as qualified.

Details:

ETSI EN 319 412-5 provides the definition of the *qcStatements* certificate extensions. These extensions have been designed in the aim of being « *a declaration that the certificate fulfils specific legal requirements for qualified certificates according to a defined legal framework* » (ETSI EN 319 412-5 § Introduction). One qcStatement extension means that the certificate is qualified for electronic signature:

> *The certificate is issued according to Directive 1999/93/EC [i.3] or Annex I of the Regulation (EU) No 910/2014 (…) (for electronic signatures).*

ETSI EN 319 412-5 § 4.2.2 specifies another *qcStatements* that specifies the type of the certificate. This extension may be used to express that the certificate is a:

> - *Certificate for electronic signatures as defined in Regulation (EU) No 910/2014*
> - *Certificate for electronic seals as defined in Regulation (EU) No 910/2014*
> - *Certificate for website authentication as defined in Regulation (EU) No 910/2014*

The indication is suitable for automated processing, since it is compliant with the ASN.1 format, that is industry commonly used data structure.

Therefore, a certificate that is compliant with ETSI EN 319 412-5 is then compliant with the clause (a) of Annexe 1.

(b)a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established

GUIDANCE :

The Regulation specifies that a set of data, within the certificate, shall contain:

- **a non-ambiguous identification of the Qualified Trust Service;**
- **a non-ambiguous identification of the Member State, in which that provider is established.**

The Regulation puts no more constraint on how a TSP must achieve this. TSP are free to specifiy this information by any set of data, as long as it is non-ambiguous. However, in x509 certificate, the most widely used certificate format, a specific set of data, the issuer field is designed to handle such identification and this practice is commonly spread in the industry. Therefore, it is recommended, for interoperability reasons, to identify the Qualified Service and the TSP.

Since the issuer field provides lots of flexibility, there's several ways to encode the TSP in that field.

Therefore, interoperability will be enhanced if all the TSPs share a common way to identify themselves in the certificate. [ETSI EN 319 412] specified a standardized way to identify the service issuing the qualified certificates and the information (including the Member State, in which that provider is established) regarding the TSP. Adoption of this method of encoding by a TSP is not mandatory, but will help Users and Third Parties to identify more easily the Qualified Service and the Qualified Service Provider.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the representation of the Qualified Trust Service Provider within the certificate to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary:

[ETSI EN 319 412-2] specifies a set of attributes, within the issuer field of the certificate that identifies the issuer of the qualified certificates.

Details:

[ETSI EN 319 412-2] § 5.2.4.1 states that:

> *« The identity of the issuer, when the issuer is a legal person, shall contain at least the following attributes (…) :*
>
> *– countryName;*
>
> *– organizationName;*
>
> *– organizationIdentifier ; and*
>
> *– commonName.*

When issued in compliance with [ETSI EN 319 412-2], the certificate shall contain a countryName attribute that identifies *the Member State in which that provider is established*.

> *The countryName attribute shall specify the country in which the issuer of the certificate is established.*

Therefore, such a certificate meets the requirement of the Regulation.

The fields organizationName, organizationIdentifier, and commonName are designed to identify the TSP in a non-ambiguous way. Especially, the organizationName attribute shall contain the name of the TSP, as stated in [ETSI EN 319 412-2] § 5.2.4.1

> *The organizationName attribute shall contain the full registered name of the certificate issuing organization.*

The commonName attribute also identifies the organization but may contains an alternative name, e.g. a commercial name, as stated in the standard:

> *The commonName attribute value shall contain a name commonly used by*

> *the subject to represent itself. This name need not be an exact match of the fully registered organization name.*

These two attributes may not be sufficient to identify an organization, since several organizations may share the same registered name. Therefore, another attribute is mandatory within the issuer field as stated in [ETSI EN 319 412-1] § 5.1.4. This clause explicitly describes that any Legal Person Identifier, such as the issuer field, SHALL include an organizationIdentifier attribute. This organization identifier contains a structured set of data that identifies the trusted service provider and the member state in a non-ambiguous way. This structured set includes:

- the information of the type of reference that is used to identify the organization. It can be either
  - a *3 character legal person identity type reference*, such as a VAT number or a national registration number ;
  - *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)*.
- the country in which the identification number shall be interpreted. The country is encoded in a non-ambiguous way, based on a *2 character ISO 3166 (…) country code*;
- the *identifier (according to country and identity type reference)* already defined above.

Example :

if the attribute contains the "VATBE-0876866142", it shall be interpreted as follows :

- the provider is established is Belgium (BE)
- it is uniquely identified by its Belgian VAT number 0876866142

This triple constitutes a unique identifier that TSPs may use to identify themselves. By this way, they meet the requirement of the Regulation to provide *a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established*

It is important to notice that [ETSI EN 319 412] allows physical person to identify themselves as issuer of the certificate. This shall obviously be not used for Qualified certificates, since in the Regulation, TSP are legal person and not physical person.

Therefore, a certificate with a format including a legal person issuer field conform with ETSI EN 319 412-2 § 5.2.4.1 and ETSI EN 319 412-1 § 5.1.4 satisfies this part of the requirement (b) of Annex.

and:

— for a legal person: the name and, where applicable, registration number as stated in the official records,

GUIDANCE :

It is crucial that a qualified certificate identifies a legal person without any ambiguity. Therefore name of the legal person and a registration number are needed. Regulation does not require a way to identify the subject of the certificate, but Industry common practice use the subject field of the certificate to identify the legal person. There is several ways for TSP to encore the legal name and registration number of the subject within the the subject field. However, interoperability and ease of use for Certificates Users and Third parties will be enhanced if the subject field is encoded in in the same way by all the TSPs. [ETSI EN 319 412] provides a way for subject field encoding that satisfies this requirement of the Regulation. Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of a legal person to ensure their compliance with the Regulation.

Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: Certificates compliant with [ETSI EN 319 412] issued to legal person shall include a Subject field that contains:

- the legal person name, within the organizationName attribute;
- the registration number of the legal person, within the organizationIdentifier attribute.

Details:

ETSI EN 319 412 provide a Subject field that may represent either a legal or a natural person. In case of a legal person, ETSI EN 319 412-3 § 4.2.1 states that the structure of the Subject shall be as follow :

> *The subject field shall include at least the following (…):*
>
> *countryName*
>
> *organizationName;*
>
> *organizationIdentifier; and*
>
> *commonName.*

The rules applying to these attributes and the associated semantics are the same than the ones of the issuer field (see the preceding requirement).

Therefore, *name* and *identification number* of the legal person are provided within the certificate. Then, [**E**TSI EN 319 412] certificates issued to legal person are compliant with this requirement of the Regulation.

—for a natural person: the person's name;

GUIDANCE :

According to the Regulation, certificate issued to a natural person shall include its name. As for legal person, the subject field is the most common way to identify the subject of the certificate. In the scope of the Regulation, TSPs are free to use another way to identify the natural person, and, if they choose the common practice of the subject, the certificate syntax offers many ways to do it.

[ETSI EN 319 412] proposes a way to encode names in the subject field that is widely used by the industry and will enhance interoperability.

A certificate issued to a physical person compliant with [ETSI EN 319 412] with the choice of including givenName and surname instead of pseudonym satisfies this clause of the EU Regulation.

TSP may use other ways to encode person names. However, lot of widely used software use the commonName **attribute of the certificate to identify the certificate holder. Even if it is not an obligation of the Regulation, it seems therefore to be a good practice to include such an attribute.**

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of a natural person to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: **[ETSI EN 319 412] requires the inclusion of the fields** givenName and surname, **that are used to represent the person's name.**

Details:
If the subject field represent a natural person, ETSI EN 319 412-2 § 5.2.6 states that

> *The subject field shall include the following attributes (…) :*
>
> *– countryName;*
>
> *– choice of (givenName and surname) or pseudonym; and*
>
> *– commonName.*

A certificate of natural person that includes the givenName and surname, provides a non-ambiguous identification of the *person's name*.

(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

GUIDANCE :

Regulation allows the use of a pseudonym, however, Certificate Users and Third Parties shall be aware that a pseudonym is used. Here too, the TSP is completely free on how to indicate in the certificate that a pseudonym is used. However, if TSPs share a common way to express it, it will be easier to users and Third Parties to identify if the Signatory has used a pseudonym or not. [ETSI EN 319 412] provides a clear way to express that a certificate is a pseudonym certificates thanks to the pseudonym attribute used instead of the above givenName and surname**. Adoption of the [ETSI EN 319 412] way to express the use of pseudonym satisfies this requirement of the Regulation. Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of pseudonym to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.**

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: If the subject field represent a natural person, [ETSI EN 319 412-2] § 5.2.6 allows the use of the pseudonym attributes instead of the givenName and surname. This dedicated attributes indicates therefore the use of a pseudonym in a clear way, and thus, satisfies the requirement of the regulation.

(*d)electronic signature validation data that corresponds to the electronic signature creation data;*

GUIDANCE:

It is an industry standard to use cryptographic key pair. Key pair are composed of

- **a private key, that is used as electronic signature creation data;**
- **a public key, that is used as electronic signature validation data;**

A certificate compliant with [ETSI EN 319 412] contains the public key, *i.e.,* the electronic signature validation data. Thus, TSPs may use [ETSI EN 319 412] compliant certificates to satisfy this requirement of the Regulation.
Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the electronic signature validation data to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: Certificates compliant with [ETSI EN 319 412] shall include a SUBJECT PUBLIC KEY INFO field. This field is a container for the pubic key, *i.e.,* the electronic signature validation data.

Details

Information of this container is satisfying requirements of [IETF 5280]. Therefore, the field SUBJECT PUBLIC KEY INFO, included in such certificates, as defined in [IETF 5280] § 4.1.2.7, contains:

- a *public key*
- information *identify the algorithm with which the key is used (e.g., RSA, DSA, or Diffie-Hellman)*

The public key of a cryptographic key pair represents *electronic signature validation data*, allowing verifying electronic signatures generated by the corresponding private key, which represents *electronic signature creation data* in the asymmetric key cryptographic model.

Moreover, as mentioned in [ETSI EN 319 412]§5.2.7.

> *The subject public key shall be selected according to ETSI TS 119 312 (…).*

[ETSI TS 119 312] specifies set of state of art algorithms that shall be used in [ETSI EN 319 412] certificates for the cryptographic key pair.

(e)details of the beginning and end of the certificate's period of validity;

GUIDANCE:

Certificates should not be valid indefinitely. Cryptographic algorithm may be broken in the future or may be not enough secured for qualified certificates. Moreover information included in a certificate may change over time. Therefore, a generally adopted good practice is to issue certificates for a limited period of time, generally one to three years. For that, beginning and end of validity period shall be indicated in the certificate.
X.509 certificates syntax provides attributes to define this validity period. However, there exists several ways to encode a date (*e.g.* UTC time, generalized time). Therefore, to enhance interoperability, TSPs should share the same practice for encoding the validity period. [ETSI EN 319 412] requires the use of the validity date attributes and requires a date encoding format, so a certificate compliant with [ETSI EN 319 412] satisfies this requirement of the Regulation.
Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the validity period and date format to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a

convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.
Summary: **[ETSI EN 319 412] requires the inclusion of the** validity **field that contains a representation of the validity period of the certificate.**

Details:
Certificates compliant with [ETSI EN 319 412] shall be compliant with [IETF RFC 5280].
Certificates compliant with [IETF RFC 5280] shall include a VALIDITY field representing the certificate validity period defined as follows:

> *The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a SEQUENCE of two dates: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter). Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime.*

The rules regarding the use of UTC or Generalized time is explicitly provided further in [IETF RFC 5280].

> *CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime.*

Thus, certificates compliant with [ETSI EN 319 412] satisfies the requirement of providing *beginning and end of the certificate's period of validity*

(f)*the certificate identity code, which must be unique for the qualified trust service provider;*

GUIDANCE:

In the purpose of non-ambiguous identification of any issued certificate, it is a good practice, widely spread in the industry, to use identity code in certificate. That allows, for example, identifying without ambiguity a certificate to be revoked. Regulation provides no technical constraint on how to introduce that identity code within the certificate. X509 certificates have a serial Number field that may be used by TSP to provide the identity code in a common way. This generally industry accepted way to provide identification numbers is mandatory in **[ETSI EN 319 412]. Moreover, [ETSI EN 319 412] provides rules for encoding the serial number. Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identity code of a legal person to ensure their compliance with the Regulation. Furthermore, this guidance**

facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.
Summary: **[ETSI EN 319 412] requires the inclusion of the** `serial Number` **field that contains an identity code of the certificate.**

Details

[IETF RFC 5280] 4.1.2.2. states that compliant certificates SHALL contain a serial number that satisfied the following:

> *The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the serialNumber to be a non-negative integer.*

This serial number is a certificate *identity code* which *is unique for the qualified trust service provider*, thanks to the above [IETF RFC 5280] requirement. Therefore the requirement of Regulation is satisfied by certificates compliant with [ETSI EN 319 412].

Additional Guidance:
Compliance with [ETSI EN 319 412] ensure the uniqueness of identify code for a given CA, i.e., a given qualified service issuing certificates. If a TSP owns several qualified services issuing certificates, it must ensure uniqueness among all its services. Therefore, it is recommended that the serial number is composed of two elements:

- a fixed prefix specific to the trusted service
- a unique identifier among the certificates issued by the service.

(g)the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

GUIDANCE:

The role of the certificate is to link signature validation data, typically a public key, with the identity of the legal or natural person that owned the signature creation data. The Regulation specifies that this must be done through an advanced electronic signature or advanced electronic seal of the qualified trust service provider, and that signature must be included in the issued certificate, such that the validity of the certificate may be checked by Third Parties and validation services. X.509 certificate format provides a `signatureValue` **field aiming at containing the signature information of the issuer . In practice, this field is widely used for that purpose in the industry . Within [ETSI EN 319 412] certificates, this field is mandatory and shall contains an advanced signature format. Therefore, the use of a certificate compliant with [ETSI EN 319 412] satisfies this requirement of the Regulation.**

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of a legal person to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.
Summary: **[ETSI EN 319 412] requires the inclusion of the signatureValue field that contains an Advanced Electronic Seal of the TSP.**

Details:
Certificates compliant with [ETSI EN 319 412] must satisfy the requirements of [IETF RFC 5280]. [IETF RFC 5280]§4.1.1 specifies the mandatory certificates field as *a `SEQUENCE` of three required fields.*
One of these three fields is the `signatureValue` field, that contains a *digital signature* computed by the CA. [IETF RFC 5280]§4.1.1.3 states that:

> *By generating this signature, a CA certifies the validity of the information in the tbsCertificate field. In particular, the CA certifies the binding between the public key material and the subject of the certificate.*

This signature is an advanced signature as defined in Article 26 of the regulation since it is

- (a) *it is uniquely linked to the creator of the seal,* as stated in [IETF RFC 5280]§4.1.1.3
- (b) *it is capable of identifying the creator of the seal*; since the creator of the seal is identified in the ISSUER field of the certificate, as explained in the guidance of Annex 1 clause (b).
- (c) *it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation*; Since the certificate is issued by a CA in conformity with [ETSI EN 319 411-2], the electronic seal creation data are operated in condition described in [ETSI EN 319 411-2]§6.4 and §6.5 that can be can be reasonably considered as conditions allowing a *high level of confidence* on the control on the key
- (d) *it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable*. Regarding that specific point, [ETSI EN 419412-2] specifies that : *Signature algorithm shall be selected according to ETSI TS 119 312.*

  [ETSI TS 119312] specifies state-of-art algorithm to be used for the signature. Therefore, this signature *is linked to the data to which it relates in such a way that any subsequent change in the data is detectable*.

Since clause (a), (b), (c) and (d) of Article 36 are satisfied, the CA signature encompassed in [ETSI EN 319 412] issued by CAs compliant with in [ETSI EN 319 411-2] are Advanced Electronic Signatures, and thus, are satisfying Annex 1 (g) og the Regulation

(*h)the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;*

GUIDANCE:

Users and Third Parties shall be able to verify the generated Advanced Electronic Signature and Advanced Electronic Seal.
For that, the Regulation requires the following elements:

i. **A certificate allowing third parties to verify the advanced signature or the advanced seal contained within the Qualified Certificate**
ii. **A location, where the certificate is available free of charge**

iii. **Within the Qualified Certificate, an indication of that location**

X.509 Format provides an authority access extension designed to provide indication of the location (iii), therefore, TSP may use that extension to provide that required information. [ETSI EN 319 412] requires this extension

a. **to be present and,**
b. **the location to be public.**

Therefore, a certificate compliant with [ETSI EN 319 412] provides the elements (ii) and (iii).

However, [ETSI EN 319 411] allows the TSP to provide the signature validation data in a format that may not be a certificate (use of certificate is only recommended). Therefore, to be compliant with the Regulation, TSPs must follow the recommendation of [ETSI EN 319 411] and provide the signature verification data as a certificate, and thus, provide by this way element (i). It is important to notice that providing a CA certificate publicly is a common practice within the industry.

Therefore, the use of a certificate compliant with [ETSI EN 319 412] satisfies this requirement of the Regulation as long as the signature validation data provided by the TSP is a certificate.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of a legal person to ensure their compliance with the Regulation, as long as they provide the certificate of the CA (notice that it is a common practice within the industry). Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: **[ETSI EN 319 412] requires the inclusion of a** *authority information access extension* that provides the public URL of the certificate.

Details:

[IETF RFC 5280] defines a non-mandatory *authority information access extension [that] indicates how to access information and services for the issuer of the certificate in which the extension appears.*

Within [ETSI EN 319 412-2]§5.5.1, this extension became mandatory for compliance and ensures that at least one access location is standard HTTP URL.

Therefore, certificates compliant with [ETSI EN 319 412] provides *the location* of the certificate. The location shall be a public URL, the certificate is thus *available free of charge*.

These points lead to the satisfaction of the requirements of the regulation.

Additional Guidance

[ETSI EN 319 411] allows the TSP to provide the signature validation data in a format that may not be a certificate. Using a certificate is only a recommendation and alternative methods are authorized, such as providing only the public key instead of the certificate. To be compliant with the Regulation, TSP must provide the public key within a certificate.

(i)the location of the services that can be used to enquire about the validity status of the qualified certificate;

GUIDANCE:

For verification purpose, it is necessary to be able to verify if the status has been revoked. Extensions exists

in X.509 certificates syntax to provide the location of the validity status service. TSP may use these extensions to meet this requirement. [ETSI EN 319 412] requires the use of at least one of these extension, therefore, the use of a certificate compliant with [ETSI EN 319 412] satisfies this requirement of the Regulation.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the location of the validity status services to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary

[ETSI EN 319 412] requires certificates to provide at least an extension indicating a CRL distribution point or the address of a OCSP responder. At least one service must be publicly available and access protocol are standard.

Details

[ETSI EN 319 412]§5.4.14 states that the certificate shall contain at least one of these two:

- a *CRL distribution point* extension that
  - shall *include at least one reference to a publicly available CRL*
  - shall at least use one of the commonly used scheme
    - http [IETF RFC 2616]
    - ldap [IETF RFC 2255]
- An authority information access extention (defined in [ETSI EN 319 412-2]§5.5.1) that points an *publicly available OCSP responder*.

Therefore, certificates compliant with [ETSI EN 319 412-2] provide *the location of the services that can be used to enquire about the validity status of the qualified certificate*.

(j)where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

GUIDANCE:

When receiving a certificate and an electronic signature, it is important for Users and Third Parties to easily identify if this certificate is qualified or not, i.e. (clause a) but also if the electronic signature creation data is located in a qualified electronic creation device. Therefore, it is mandatory for TSP to provide this information.

The regulation let the TSP to freely choose the way to indicate that as long as the form is suitable for an automated process. However, to enhance the interoperability between the TSP, adoption of a common way to provide this indication is recommended, since multiple mechanisms for indicating the use of a qualified electronic signature creation device, means more complexity for any service providers, users or Third Parties for verifying the signatures. [ETSI EN 319 412-5] provides certificate extension, suitable for an automated process, that complies with this requirement of the Regulation.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding Signature Creation Device to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: [ETSI EN 319 412-5] provides a specific QCStatement attribute to claim that the private key resides in a QSCD. TSP may use this attribute to fulfills the Regulation Requirement.

Details:[ETSI EN 319 412-5]§4.2.2 specifies a *QCStatement* attributes claiming *that the private key related to the certified public key resides in a QSCD*.
More specifically, setting this specific attributes means that either:

> *the private key related to the certified public key resides in a Qualified Signature/Seal Creation Device (QSCD) according to the Regulation (EU) No 910/2014*

or resides in

> *a secure signature creation device as defined in the Directive 1999/93/EC [i.3]*

Since this attribute is encoded in the industry widely used ASN.1 format, it is suitable for automated process.

ARTICLE 38

Art.38.1 Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.

GUIDANCE :

Guidance related to Annex 3 is provided further in this document.

Art. 38.2. Qualified certificates for electronic seals shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex III.

No specific guidance given at this time.

Art. 38.3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.

GUIDANCE:

Certificates format allows to add, within the certificate, non-mandatory specific attributes, expressing, for example, the locality of the organization or the Organizational Unit..We provide example of non-mandatory additional specific attributes that may affect or may not affect the interoperability.

*Examples of non-mandatory additional specific attributes that **do not affect** the interoperability may include:*

- *Any additional standard attributes in Subject or Issuer field such as:*
  - *Organizational Unit*
  - *State or Province Name*
  - *Locality*

- *Additional extensions such as*
    - *Subject Key Identifier*
    - *Authority Key Identifier*
    - *Certificate policies extension*
    - *Extended key usages*

Examples of non-mandatory additional specific attributes that <u>may affect</u> the interoperability may include:

- *Any extended key usage extension or proprietary extension set as critical in the certificate.*
- *For a legal person, the use of surname and givenName, or any attributes commonly related to a natural person should not be used. Then adding such attributes, the certificate may be considered by users as a natural person certificate, and the may affect interoperability.*
-

Art 38.4. If a qualified certificate for electronic seals has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

No specific guidance given at this time.

Art 38.5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic seals:

GUIDANCE :

Due to the actual state of art of the industry regarding the verification of signature, and particularly the fact that the majority of verification tools are unable to verify the validity of a signature generated by a certificate that has been temporarily suspended, it is recommended that each Member State forbids the practice of temporary suspension of a qualified certificate for electronic signature. However, if Members States still lay down national rules on temporary suspension, we suggest that verification mechanisms able to handle the suspension are provided together with the authorization to suspend qualified certificates.

(a)if a qualified certificate for electronic seal has been temporarily suspended that certificate shall lose its validity for the period of suspension;

No specific guidance given at this time.

(b)the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

No specific guidance given at this time.

Art. 38.6. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seal. Compliance with the requirements laid down in Annex III shall be

presumed where a qualified certificate for electronic seal meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

No specific guidance given at this time.

ANNEXE III

GUIDANCE:

Annex 3 provides a list of ten requirements that shall be fulfilled by the Qualified TSP. There are divergent ways for a TSP to fulfil these requirements. The purpose of this guidance is to allow TSP that want to use convergent implementations of these requirements to do so. For each requirement, this guidance includes:

- Contextual information about the requirement (aim, scope, mandatory elements, optional elements)
- The technical elements that have to be included to be compliant to the requirement
- The standards that exist and can be applied to ensure compliance to the requirement and to maximize interoperability
- A rationale explaining how these standards meet the requirement.
- When applicable, additional guidance on how to apply the standard in conformance with the regulation.

This guidance targets three different objectives:

- automatic legal compliance to eIDAS Regulation for TSPs choosing to follow the guidance;
- largest possible certificates uses for TSPs choosing to follow the guidance;
- maximized usage of European certificates for users and third parties, thanks to TSPs convergent implementations.

Qualified certificates for electronic seals shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic seal;

GUIDANCE :

When receiving a certificate and an electronic seal, it is important for Users and Third Parties to easily identify if this certificate is qualified or not. Therefore, it is mandatory for TSP to provide, within the certificate, if it is qualified or not.

The regulation let the TSP to freely choose the way to indicate if a certificate is qualified or not, as long as the form is suitable for an automated process. However, to enhance the interoperability between the TSP, adoption of a common way to provide this indication is recommended, since multiple mechanisms for indicating the qualification of a certificate means more complexity for any service provider for verifying the signatures. [ETSI EN 319 412-5] provides certificate extension, suitable for an automated process, that complies with this requirement of the Regulation. A TSP issuing qualified certificates compliant with [ETSI EN 319 412-5] fulfils this requirement of the regulation and issues certificates that may be more easily be accepted by the industry.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding information about the qualification of the certificate, to ensure their compliance with the Regulation. Furthermore, this guidance facilitates

adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary:

[ETSI EN 319 412-5] specifies the qcStatements certificate extension, that provide the information that the certificate is issued as qualified.

Details:

ETSI EN 319 412-5 provides the definition of the *qcStatements* certificate extensions. These extensions have been designed in the aim of being « *a declaration that the certificate fulfils specific legal requirements for qualified certificates according to a defined legal framework* » (ETSI EN 319 412-5 § Introduction).

ETSI EN 319 412-5 § 4.2.2 specifies a *qcStatements* that specifies the type of the certificate. This extension may be used to express that the certificate is a:

- *Certificate for electronic signatures as defined in Regulation (EU) No 910/2014*
- ***Certificate for electronic seals as defined in Regulation (EU) No 910/2014***
- *Certificate for website authentication as defined in Regulation (EU) No 910/2014*

The indication is suitable for automated processing, since it is compliant with the ASN.1 format that is industry commonly used data structure.

Therefore, a certificate that is compliant with ETSI EN 319 412-5 is then compliant with the clause (a) of Annexe 3.

(b)a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established

GUIDANCE :

The Regulation specifies that a set of data, within the certificate, shall contain:

- **a non-ambiguous identification of the Qualified Trust Service;**
- **a non-ambiguous identification of the Member State, in which that provider is established.**

The Regulation puts no more constraint on how a TSP must achieve this. TSP are free to specify this information by any set of data, as long as it is non-ambiguous. However, in x509 certificate, the most widely used certificate format, a specific set of data, the `issuer` field is designed to handle such identification and this practice is commonly spread in the industry. Therefore, it is recommended, for

interoperability reasons, to identify the Qualified Service and the TSP.

Since the issuer field provides lots of flexibility, there's several ways to encode the TSP in that field. Therefore, interoperability will be enhanced if all the TSPs share a common way to identify themselves in the certificate. [ETSI EN 319 412] specified a standardized way to identify the service issuing the qualified certificates and the information (including the Member State, in which that provider is established) regarding the TSP. Adoption of this method of encoding by a TSP is not mandatory, but will help Users and Third Parties to identify more easily the Qualified Service and the Qualified Service Provider.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the representation of the Qualified Trust Service Provider within the certificate to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary:

[ETSI EN 319 412-2] specifies a set of attributes, within the issuer field of the certificate that identifies the issuer of the qualified certificates.

Details:

[ETSI EN 319 412-2] § 5.2.4.1 states that:

> *« The identity of the issuer, when the issuer is a legal person, shall contain at least the following attributes (…) :*
>
> *– countryName;*
>
> *– organizationName;*
>
> *– organizationIdentifier; and*
>
> *– commonName.*

When issued in compliance with [ETSI EN 319 412-2], the certificate shall contain a countryName attribute that identifies *the Member State in which that provider is established*.

> *The countryName attribute shall specify the country in which the issuer of the certificate is established.*

Therefore, such a certificate meets the requirement of the Regulation.

The fields organizationName, organizationIdentifier, and commonName are designed to identify the TSP in a non-ambiguous way. Especially, the organizationName attribute shall contain the name of the TSP, as stated in [ETSI EN 319 412-2] § 5.2.4.1

> *The organizationName attribute shall contain the full registered name of the certificate issuing organization.*

The commonName attribute also identifies the organization but may contains an alternative name, e.g. a commercial name, as stated in the standard:

> *The commonName attribute value shall contain a name commonly used by the subject to represent itself. This name need not be an exact match of the fully registered organization name.*

These two attributes may not be sufficient to identify an organization, since several organizations may share the same registered name. Therefore, another attribute is mandatory within the issuer field as stated in [ETSI EN 319 412-1] § 5.1.4. This clause explicitly describes that any Legal Person Identifier, such as the issuer field, SHALL include an organizationIdentifier attribute. This organization identifier contains a structured set of data that identifies the trusted service provider and the member state in a non-ambiguous way. This structured set includes:

- the information of the type of reference that is used to identify the organization. It can be either
  - a *3 character legal person identity type reference*, such as a VAT number or a national registration number ;
  - *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)*.
- the country in which the identification number shall be interpreted. The country is encoded in a non-ambiguous way, based on a *2 character ISO 3166 (…) country code*;
- the *identifier (according to country and identity type reference)* already defined above.

Example :

if the attribute contains the "VATBE-0876866142", it shall be interpreted as follows :

- the provider is established is Belgium (BE)
- it is uniquely identified by its Belgian VAT number 0876866142

This triple constitutes a unique identifier that TSPs may use to identify themselves. By this way, they meet the requirement of the Regulation to provide *a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established*

It is important to notice that [ETSI EN 319 412] allows physical person to identify themselves as issuer of the certificate. This shall obviously be not used for Qualified certificates, since in the Regulation, TSP are legal person and not physical person.

Therefore, a certificate with a format including a legal person issuer field conform with ETSI EN 319 412-2 § 5.2.4.1 and ETSI EN 319 412-1 § 5.1.4 satisfies this part of the requirement (b) of Annex 3.

and:

— for a legal person: the name and, where applicable, registration number as stated in the official records,

GUIDANCE :

It is crucial that a qualified certificate identifies a legal person issuing certificate without any ambiguity. Therefore name of the legal person and a registration number are needed. Regulation does not require a way to identify the subject of the certificate, but Industry common practice use the Subject field of the certificate to identify the legal person. There is several ways for TSP to encore the legal name and registration number of the subject within the Subject field. However, interoperability and ease of use for Certificates Users and Third parties will be enhanced if the

Subject **field is encoded in in the same way by all the TSPs. [ETSI EN 319 412] provides a way for** Subject **field encoding that satisfies this requirement of the Regulation. Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of a legal person to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.**

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: Certificates compliant with [ETSI EN 319 412] issued to legal person shall include a Subject field that contains:

- the legal person name, within the organizationName attribute;
- the registration number of the legal person, within the organizationIdentifier attribute.

Details:

ETSI EN 319 412 provide a Subject field that may represent either a legal or a natural person. In case of a legal person, ETSI EN 319 412-3 § 4.2.1 states that the structure of the Subject shall be as follow :

> *The subject field shall include at least the following (…):*
>
> *countryName*
>
> *organizationName;*
>
> *organizationIdentifier ; and*
>
> *commonName.*

The rules applying to these attributes and the associated semantics are the same than the ones of the issuer field (see the preceding requirement).

Therefore, *name* and *identification number* of the legal person are provided within the certificate. Then, [**E**TSI EN 319 412] certificates issued to legal person are compliant with this requirement of the Regulation.

—for a natural person: the person's name;

GUIDANCE :

According to the Regulation, certificate issued by a natural person shall include its name. As for legal person, the subject field is the most common way to identify the subject of the certificate. In the scope of the Regulation, TSPs are free to use another way to identify the natural person, and, if they choose the common practice of the subject, the certificate syntax offers many ways to do it.

[ETSI EN 319 412] proposes a way to encode names in the subject field that is widely used by the industry and will enhance interoperability.

A certificate issued to a physical person compliant with [ETSI EN 319 412] with the choice of including givenName and surname instead of pseudonym satisfies this clause of the EU Regulation.

TSP may use other ways to encode person names. However, lot of widely used software use the

commonName **attribute of the certificate to identify the certificate holder. Even if it is not an obligation of the Regulation, it seems therefore to be a good practice to include such an attribute.**

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of a natural person to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: **[ETSI EN 319 412] requires the inclusion of the fields** givenName and surname, **that are used to represent the person's name.**

Details:
If the subject field represent a natural person, ETSI EN 319 412-2 § 5.2.6 states that

> *The subject field shall include the following attributes (…) :*
>
> *– countryName;*
>
> *– choice of (givenName and surname) or pseudonym; and*
>
> *– commonName.*

A certificate of natural person that includes the givenName and surname, provides a non-ambiguous identification of *the person's name*.

(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;

GUIDANCE :

Regulation requires that an identification of the creator of the seal is provided. The TSP is completely free on how to provide this information within the certificate. However, if TSPs share a common way to express it, it will be easier to users and Third Parties to identify if the Creator of the seal. [ETSI EN 319 412] provides a clear way to express this, thanks to the subject field that may be used to identify a legal person. Adoption of the [ETSI EN 319 412] way to identify a legal person satisfies this requirement of the Regulation. Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification legal to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: If the subject field represent a legal person, [ETSI EN 319 412-2] § 5.2.6 allows the use of the same identification structure than the one of the issuer filed (see clause b)

(d)electronic seal validation data that corresponds to the electronic seal creation data;

GUIDANCE:

It is an industry standard to use cryptographic key pair. Key pair are composed of

- **a private key, that is used as electronic signature creation data;**
- **a public key, that is used as electronic signature validation data;**

A certificate compliant with [ETSI EN 319 412] contains the public key, *i.e.,* the electronic seal validation data. Thus, TSPs may use [ETSI EN 319 412] compliant certificates to satisfy this requirement of the Regulation.
Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the electronic seal validation data to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: Certificates compliant with [ETSI EN 319 412] shall include a SUBJECT PUBLIC KEY INFO field. This field is a container for the pubic key, *i.e.,* the electronic seal validation data.

Details

Information of this container is satisfying requirements of [IETF 5280]. Therefore, the field SUBJECT PUBLIC KEY INFO, included in such certificates, as defined in [IETF 5280] § 4.1.2.7, contains:

- a *public key*
- information *identify the algorithm with which the key is used (e.g., RSA, DSA, or Diffie-Hellman)*

The public key of a cryptographic key pair represents *electronic seal validation data*, allowing verifying electronic seal generated by the corresponding private key, which represents *electronic seal creation data* in the asymmetric key cryptographic model.

Moreover, as mentioned in [ETSI EN 319 412]§5.2.7.

> *The subject public key shall be selected according to ETSI TS 119 312 (…).*

[ETSI TS 119 312] specifies set of state of art algorithms that shall be used in [ETSI EN 319 412] certificates for the cryptographic key pair.

(e)details of the beginning and end of the certificate's period of validity;

GUIDANCE:

Certificates should not be valid indefinitely. Cryptographic algorithm may be broken in the future or may be not enough secured for qualified certificates. Moreover information included in a certificate may change over time. Therefore, a generally adopted good practice is to issue certificates for a limited period of time, generally one to three years. For that, beginning and end of validity period shall be indicated in the certificate.
X.509 certificates syntax provides attributes to define this validity period. However, there exists several ways to encode a date (*e.g.* UTC time, generalized time). Therefore, to enhance interoperability, TSPs should share the same practice for encoding the validity period. [ETSI EN 319 412] requires the use of the validity date attributes and requires a date encoding format, so a certificate compliant with [ETSI EN 319 412] satisfies this requirement of the Regulation.
Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the validity period and date format to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a

convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.
Summary: **[ETSI EN 319 412] requires the inclusion of the** validity **field that contains a representation of the validity period of the certificate.**

Details:
Certificates compliant with [ETSI EN 319 412] shall be compliant with [IETF RFC 5280].
Certificates compliant with [IETF RFC 5280] shall include a VALIDITY field representing the certificate validity period defined as follows:

> *The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. The field is represented as a SEQUENCE of two dates: the date on which the certificate validity period begins (notBefore) and the date on which the certificate validity period ends (notAfter). Both notBefore and notAfter may be encoded as UTCTime or GeneralizedTime.*

The rules regarding the use of UTC or Generalized time is explicitly provided further in [IETF RFC 5280].

> *CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime.*

Thus, certificates compliant with [ETSI EN 319 412] satisfies the requirement of providing *beginning and end of the certificate's period of validity*

(f)*the certificate identity code, which must be unique for the qualified trust service provider;*

GUIDANCE:

In the purpose of non-ambiguous identification of any issued certificate, it is a good practice, widely spread in the industry, to use identity code in certificate. That allows, for example, identifying without ambiguity a certificate to be revoked. Regulation provides no technical constraint on how to introduce that identity code within the certificate. X509 certificates have a serial Number field that may be used by TSP to provide the identity code in a common way. This generally industry accepted way to provide identification numbers is mandatory in **[ETSI EN 319 412]. Moreover, [ETSI EN 319 412] provides rules for encoding the serial number. Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identity code of a legal person to ensure their compliance with the Regulation. Furthermore, this guidance**

facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.
Summary: **[ETSI EN 319 412] requires the inclusion of the** serial Number **field that contains an identity code of the certificate.**

Details

[IETF RFC 5280] 4.1.2.2. states that compliant certificates SHALL contain a serial number that satisfied the following:

> *The serial number MUST be a positive integer assigned by the CA to each certificate. It MUST be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the serialNumber to be a non-negative integer.*

This serial number is a certificate *identity code* which *is unique for the qualified trust service provider*, thanks to the above [IETF RFC 5280] requirement. Therefore the requirement of Regulation is satisfied by certificates compliant with [ETSI EN 319 412].

Additional Guidance:
Compliance wih [ETSI EN 319 412] ensure the uniqueness of identify code for a given CA, i.e., a given qualified service issuing certificates. If a TSP owns several qualified services issuing certificates, it must ensure uniqueness among all its services. Therefore, it is recommended that the serial number is composed of two elements:

- a fixed prefix specific to the trusted service
- a unique identifier among the certificates issued by the service.

(g)the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;

GUIDANCE:

The role of the certificate is to link signature validation data, typically a public key, with the identity of the legal or natural person that owned the signature creation data. The Regulation specifies that this must be done through an advanced electronic signature or advanced electronic seal of the qualified trust service provider, and that signature must be included in the issued certificate, such that the validity of the certificate may be checked by Third Parties and validation services. X.509 certificate format provides a `signatureValue` **field aiming at containing the signature information of the issuer . In practice, this field is widely used for that purpose in the industry . Within [ETSI EN 319 412] certificates, this field is mandatory and shall contains an advanced signature format. Therefore, the use of a certificate compliant with [ETSI EN 319 412] satisfies this requirement of the Regulation.**

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of a legal person to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.
Summary: **[ETSI EN 319 412] requires the inclusion of the signatureValue field that contains an Advanced Electronic Seal of the TSP.**

Details:
Certificates compliant with [ETSI EN 319 412] must satisfy the requirements of [IETF RFC 5280]. [IETF RFC 5280]§4.1.1 specifies the mandatory certificates field as *a `SEQUENCE` of three required fields.*
One of these three fields is the `signatureValue` field, that contains a *digital signature* computed by the CA. [IETF RFC 5280]§4.1.1.3 states that:

> *By generating this signature, a CA certifies the validity of the information in the tbsCertificate field. In particular, the CA certifies the binding between the public key material and the subject of the certificate.*

This signature is an advanced signature as defined in Article 26 of the regulation since it is

- (a) *it is uniquely linked to the creator of the seal,* as stated in [IETF RFC 5280]§4.1.1.3
- (b) *it is capable of identifying the creator of the seal*; since the creator of the seal is identified in the ISSUER field of the certificate, as explained in the guidance of Annex 3 clause (b).
- (c) *it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation*; Since the certificate is issued by a CA in conformity with [ETSI EN 319 411-2], the electronic seal creation data are operated in condition described in [ETSI EN 319 411-2]§6.4 and §6.5 that can be can be reasonably considered as conditions allowing a *high level of confidence* on the control on the key
- (d) *it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable*. Regarding that specific point, [ETSI EN 419412-2] specifies that : *Signature algorithm shall be selected according to ETSI TS 119 312.*

  [ETSI TS 119312] specifies state-of-art algorithm to be used for the signature. Therefore, this signature *is linked to the data to which it relates in such a way that any subsequent change in the data is detectable*.

Since clause (a), (b), (c) and (d) of Article 36 are satisfied, the CA signature encompassed in [ETSI EN 319 412] issued by CAs compliant with in [ETSI EN 319 411-2] are Advanced Electronic Signatures, and thus, are satisfying Annex 3 (g) og the Regulation

(*h)the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;*

GUIDANCE:

Users and Third Parties shall be able to verify the generated Advanced Electronic Signature and Advanced Electronic Seal.
For that, the Regulation requires the following elements:

- **iv. A certificate allowing third parties to verify the advanced signature or the advanced seal contained within the Qualified Certificate**
- **v. A location, where the certificate is available free of charge**

vi. Within the Qualified Certificate, an indication of that location

X.509 Format provides an authority access extension designed to provide indication of the location (iii), therefore, TSP may use that extension to provide that required information. [ETSI EN 319 412] requires this extension

- **c. to be present and,**
- **d. the location to be public.**

Therefore, a certificate compliant with [ETSI EN 319 412] provides the elements (ii) and (iii).

However, [ETSI EN 319 411] allows the TSP to provide the signature validation data in a format that may not be a certificate (use of certificate is only recommended). Therefore, to be compliant with the Regulation, TSPs must follow the recommendation of [ETSI EN 319 411] and provide the signature verification data as a certificate, and thus, provide by this way element (i). It is important to notice that providing a CA certificate publicly is a common practice within the industry.

Therefore, the use of a certificate compliant with [ETSI EN 319 412] satisfies this requirement of the Regulation as long as the signature validation data provided by the TSP is a certificate.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the identification of a legal person to ensure their compliance with the Regulation, as long as they provide the certificate of the CA (notice that it is a common practice within the industry). Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: **[ETSI EN 319 412] requires the inclusion of a** *authority information access extension* that provides the public URL of the certificate.

Details:

[IETF RFC 5280] defines a non-mandatory *authority information access extension [that] indicates how to access information and services for the issuer of the certificate in which the extension appears.*

Within [ETSI EN 319 412-2]§5.5.1, this extension became mandatory for compliance and ensures that at least one access location is standard HTTP URL.

Therefore, certificates compliant with [ETSI EN 319 412] provides *the location* of the certificate. The location shall be a public URL, the certificate is thus *available free of charge*.

These points lead to the satisfaction of the requirements of the regulation.

Additional Guidance

[ETSI EN 319 411] allows the TSP to provide the signature validation data in a format that may not be a certificate. Using a certificate is only a recommendation and alternative methods are authorized, such as providing only the public key instead of the certificate. To be compliant with the Regulation, TSP must provide the public key within a certificate.

(i)the location of the services that can be used to enquire about the validity status of the qualified certificate;

GUIDANCE:

For verification purpose, it is necessary to be able to verify if the status has been revoked. Extensions exists

in X.509 certificates syntax to provide the location of the validity status service. TSP may use these extensions to meet this requirement. [ETSI EN 319 412] requires the use of at least one of these extension, therefore, the use of a certificate compliant with [ETSI EN 319 412] satisfies this requirement of the Regulation.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding the location of the validity status services to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary

[ETSI EN 319 412] requires certificates to provide at least an extension indicating a CRL distribution point or the address of a OCSP responder. At least one service must be publicly available and access protocol are standard.

Details

[ETSI EN 319 412]§5.4.14 states that the certificate shall contain at least one of these two:

- a *CRL distribution point* extension that
  - shall *include at least one reference to a publicly available CRL*
  - shall at least use one of the commonly used scheme
    - http [IETF RFC 2616]
    - ldap [IETF RFC 2255]
- An authority information access extension (defined in [ETSI EN 319 412-2]§5.5.1) that points an *publicly available OCSP responder*.

Therefore, certificates compliant with [ETSI EN 319 412-2] provide *the location of the services that can be used to enquire about the validity status of the qualified certificate*.

(j)where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

GUIDANCE:

When receiving a certificate and an electronic signature, it is important for Users and Third Parties to easily identify if this certificate is qualified or not, i.e. (clause a) but also if the electronic signature creation data is located in a qualified electronic creation device. Therefore, it is mandatory for TSP to provide this information.

The regulation let the TSP to freely choose the way to indicate that as long as the form is suitable for an automated process. However, to enhance the interoperability between the TSP, adoption of a common way to provide this indication is recommended, since multiple mechanisms for indicating the use of a qualified electronic signature creation device, means more complexity for any service providers, users or Third Parties for verifying the signatures. [ETSI EN 319 412-5] provides certificate extension, suitable for an automated process, that complies with this requirement of the Regulation.

Thus, TSP may follow the proposition of [ETSI EN 319 412] regarding Signature Creation Device to ensure their compliance with the Regulation. Furthermore, this guidance facilitates adoption of a convergent format that is used and recognized by most Users all across Europe, and prevents divergent implementations that lead to absence of interoperability.

Rationale on how [ETSI EN 319 412] satisfies that requirement.

Summary: [ETSI EN 319 412-5] provides a specific QCStatement attribute to claim that the private key resides in a QSCD. TSP may use this attribute to fulfils the Regulation Requirement.

Details:[ETSI EN 319 412-5]§4.2.2 specifies a *QCStatement* attributes claiming *that the private key related to the certified public key resides in a QSCD*.
More specifically, setting this specific attributes means that either:

> *the private key related to the certified public key resides in a Qualified Signature/Seal Creation Device (QSCD) according to the Regulation (EU) No 910/2014*

or resides in

> *a secure signature creation device as defined in the Directive 1999/93/EC [i.3]*

Since this attribute is encoded in the industry widely used ASN.1 format, it is suitable for automated process.

ANNEX A: CERTIFICATE PROFILES

We provide a proposition of certificate profile satisfying the requirements of the Regulation

ANNEX A.1: CERTIFICATE PROFILE FOR NATURAL PERSON

BASIC FIELDS

<table>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>Version</td><td>2 (=version 3)</td></tr>
<tr><td>Serial number</td><td>Unique for each certificate issued by the TSP</td></tr>
<tr><td>Key Size</td><td>Any key size in conformance with [ETSI TS 119 312]</td></tr>
<tr><td>Issuer DN</td><td>
<table>
<tr><td>Attribute</td><td>Value</td></tr>
<tr><td>countryName</td><td>Country where the TSP is established</td></tr>
<tr><td>organizationName</td><td>full registered name of the TSP</td></tr>
<tr><td>organizationIdentifier</td><td>Unique identifier of the TSP in conformance with [ETSI EN 319 412-1]§ 5.1.4</td></tr>
<tr><td>commonName</td><td>Common name of the TSP or the service</td></tr>
</table>
</td></tr>
<tr><td>Subject DN</td><td>
<table>
<tr><td>Attribute</td><td>Value</td></tr>
<tr><td>countryName</td><td>Country defining the general context of the issuance</td></tr>
<tr><td>givenName</td><td>Given name of the natural person</td></tr>
<tr><td>surname</td><td>Surname of the natural person</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Field</th><th>Value</th></tr>
<tr><td></td><td>
<table>
<tr><td>commonName</td><td>Name of the natural person (presentation format). TSP may impose the format.</td></tr>
</table>

Or for pseudonym certificate
<table>
<tr><td>Attribute</td><td>Value</td></tr>
<tr><td>countryName</td><td>Country defining the general context of the issuance</td></tr>
<tr><td>pseudonym</td><td>pseudonym of the natural person</td></tr>
<tr><td>commonName</td><td>pseudonym of the natural person (presentation format)</td></tr>
</table>

Notice the the attribute SerialNumber may be used to ensure the unicity of the DN.
</td></tr>
<tr><td>NotBefore</td><td>Begining of validity of the certificate encoded in conformance with [RFC5280]</td></tr>
<tr><td>NotAfter</td><td>Begining of validity of the certificate encoded in conformance with [RFC5280]</td></tr>
<tr><td>Public Key Algorithm</td><td>In conformance with [ETSI TS 119 312]</td></tr>
<tr><td>Signature Algorithm</td><td>In conformance with [ETSI TS 119 312]</td></tr>
</table>

EXTENSIONS

Extensions standards	Mandatory	Critical	Value
Authority Key Identifier	**yes**	**FALSE**	Key identifier for the issuing CA's public key
Basic Constraint	**yes**	**TRUE**	CA shall be set to false
Certificate Policies	**yes**	**FALSE**	The certificate policies extension shall contain the identifier of at least - one certificate policy which reflects the practices and procedures undertaken by the CA and/or - one of the identifier defined in [ETSI EN 319 411-2]§5.2 It is recommended to implement the first case.
Authority Information Access	**yes**		- the Authority Information Access extension shall include an accessMethod OID, id-ad-calIssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA At least one access location should use the http scheme.

<table>
<tr><th>Extensions standards</th><th>Mandatory</th><th>Critical</th><th>Value</th></tr>
<tr><td></td><td></td><td></td><td>- the Authority Information Access extension may include an accessMethod OID, id-ad-ocsp, with an accessLocation value specifying at least one access location of an publicly available OCSP. This is mandatory is no public CRL Distribution point is defined.</td></tr>
<tr><td>CRL Distribution Points</td><td>conditional</td><td>FALSE</td><td>If no public OCSP location is defined within the certificate.

- CRL Distribution point is mandatory
- CRL Distribution point shall include a reference to a publicly available CRL
- At least one reference to a publicly available CRL shall use http or ldap protocol.</td></tr>
<tr><td>Key Usage</td><td>yes</td><td>TRUE</td><td>In conformance with [ETSI TS 119 312-2]§5.3.4</td></tr>
<tr><td>Subject Key Identifier</td><td>no</td><td>FALSE</td><td>[RFC 5280] recommends the inclusion of this extension.</td></tr>
<tr><td>QCStatements</td><td>X</td><td>FALSE</td><td>This extension shall be set in conformance with [EN 319 312-5]
<table>
<tr><th>Extension</th><th>included</th><th>comments</th></tr>
<tr><td>esi4-qcStatement-1</td><td>yes</td><td>Identifies the certificate as qualified</td></tr>
<tr><td>esi4-qcStatement-2</td><td>Cond.</td><td>Included if a limit of transaction want to be set</td></tr>
<tr><td>esi4-qcStatement-3</td><td>Cond.</td><td>Included if a retention perioed want to be set</td></tr>
<tr><td>esi4-qcStatement-4</td><td>Cond.</td><td>Included if the private key is in a QSCD</td></tr>
<tr><td>esi4-qcStatement-5</td><td>yes</td><td>Shall contain a reference to the PKI disclosure agreement</td></tr>
<tr><td>esi4-qcStatement-6</td><td>yes</td><td>Value shall be id-etsi-qct-esign</td></tr>
</table></td></tr>
</table>

Notice that we propose a minimal list of attributes. However the use of non-critical extra attributes in conformity with RFC 5280 is authorized.

ANNEX A.2: CERTIFICATE PROFILE FOR LEGAL PERSON

<table>
<tr><th>Field</th><th>Value</th></tr>
<tr><td>Version</td><td>2 (=version 3)</td></tr>
<tr><td>Serial number</td><td>Unique for each certificate issued by the TSP</td></tr>
<tr><td>Key Size</td><td>Any key size in conformance with [ETSI TS 119 312]</td></tr>
<tr><td>Issuer DN</td><td>
<table>
<tr><td>Attribute</td><td>Value</td></tr>
<tr><td>countryName</td><td>Country where the TSP is established</td></tr>
<tr><td>organizationName</td><td>full registered name of the TSP</td></tr>
<tr><td>organizationIdentifier</td><td>Unique identifier of the TSP in conformance with [ETSI EN 319 412-1]§ 5.1.4</td></tr>
<tr><td>commonName</td><td>Common name of the TSP or the service</td></tr>
</table>
</td></tr>
<tr><td>Subject DN</td><td>
<table>
<tr><td>Attribute</td><td>Value</td></tr>
<tr><td>countryName</td><td>Country where the Legal Person is established</td></tr>
<tr><td>organizationName</td><td>full registered name of the legal person</td></tr>
<tr><td>organizationIdentifier</td><td>Unique identifier of the legal person in conformance with [ETSI EN 319 412-1]§ 5.1.4</td></tr>
<tr><td>commonName</td><td>Common name of the Legal Person</td></tr>
</table>
</td></tr>
<tr><td>NotBefore</td><td>Begining of validity of the certificate encoded in conformance with [RFC5280]</td></tr>
</table>

Field	Value
NotAfter	Begining of validity of the certificate encoded in conformance with [RFC5280]
Public Key Algorithm	In conformance with [ETSI TS 119 312]
Signature Algorithm	In conformance with [ETSI TS 119 312]

EXTENSIONS

Extensions standards	Mandatory	Critical	Value
Authority Key Identifier	**yes**	**FALSE**	Key identifier for the issuing CA's public key
Basic Constraint	**yes**	**TRUE**	CA shall be set to false
Certificate Policies	**yes**	**FALSE**	The certificate policies extension shall contain the identifier of at least - one certificate policy which reflects the practices and procedures undertaken by the CA and/or - one of the identifier defined in [ETSI EN 319 411-2]§5.2 It is recommended to implement the first case.
Authority Information Access	**yes**		- the Authority Information Access extension shall include an accessMethod OID, id-ad-calssuers, with an accessLocation value specifying at least one access location of a valid CA certificate of the issuing CA At least one access location should use the http scheme. - the Authority Information Access extension may include an accessMethod OID, id-ad-ocsp, with anaccessLocation value specifying at least one access location of an publicly available OCSP. This is mandatory is no public CRL Distribution point is defined.
CRL Distribution Points	**conditional**	**FALSE**	If no public OCSP location is defined within the certificate. - CRL Distribution point is mandatory - CRL Distribution point shall include a reference to a publicly available CRL - At least one reference to a publicly available CRL shall use http or ldap protocol.
Key Usage	**yes**	**TRUE**	In conformance with [ETSI TS 119 312-2]§5.3.4
Subject Key Identifier	**no**	**FALSE**	[RFC 5280] recommends the inclusion of this extension.
QCStatements	**X**	**FALSE**	This extension shall be set in conformance with [EN 319 312-5] Extension / included / comments esi4-qcStatement-1 / no / Identifies the certificate

Extensions standards	Mandatory	Critical	Value		
					as qualified
			esi4-qcStatement-2	Cond.	Included if a limit of transaction want to be set
			esi4-qcStatement-3	Cond.	Included if a retention perioed want to be set
			esi4-qcStatement-4	Cond.	Included if the private key is in a QSCD
			esi4-qcStatement-5	yes	Shall contain a reference to the PKI disclosure agreement
			esi4-qcStatement-6	yes	Value shall be id-etsi-qct-eseal

Notice that we propose a minimal list of attributes. However the use of non-critical extra attributes in conformity with RFC 5280 is authorized.