Guidance for Requirements for qualified trust service providers: trustworthy systems and products

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 24.2.(E)

Art.24.2 A qualified trust service provider providing qualified trust services shall:
(…)
(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;

GUIDANCE:

Article 19.1 obliges TSP to setup measures to manage the risk posed to the security of the trust services. This Clause of Article 24.2. is more specific and **only applicable to qualified services**.

Without any implementation act referencing a specific standard to be met, the type and the appropriate level of security of a trustworthy system or product is subject to interpretation. Divergent interpretation of what an appropriate system or product is may lead to:

- Inadequate level of security for trust services
    - that may cause security breaches, if the security level is too low regarding the legal impact of the service
    - that may cause economic issues to providers setting up unnecessary costly material.

The purpose of this guidance is to allow TSPs that want to use convergent type of material with adequate security level to do so. For that, this guidance provides, when possible, for each type of trust service, a link to the applicable security standards.

1. APPLICABLE SCOPE

Article 24.2 specifies that the scope is *qualified trust service providers.* This specifies that the article is applicable to any provider that delivers at least one qualified trust service as defined in the Regulation (Article 3.16):

- qualified services issuing qualified certificates for electronic signatures, electronic seals and certificates for website authentication;
- qualified timestamping services;
- qualified validation services for qualified electronic signatures and qualified electronic seals;
- qualified preservation services for qualified electronic signatures and qualified electronic seals;
- qualified electronic registered delivery services.

As mentioned in Art. 24.2 (f) , the *system and product* to be use by the provider to

- *protected against modification*
- *ensure the technical security*

- *ensure the reliability of the processes supported by them;*

It is important to notice, that, even if it is not mandatory to use *trustworthy systems and products* for non-qualified trust service, non-qualified trusted service provided may also use such product.

2. SECURITY PRODUCT REFERENCE STANDARDS

To be compliant with the Regulation, TSPs shall use *trustworthy systems and products* to ensure the security of their qualified service. Therefore, it is a challenge for TSP to:

- Assert the security level of the systems and service
- To ensure, even if the security level of the product is in adequation with the service, that the TSP is using it in a propor and secure way. Even the most secured product may offer no protection if it is not used in a proposer manner. For example, smartcard proposes a very high security level offering protection against various and high level attacks. However, if the PIN code is written on the card, all these state-of-the-art security measures implemented on the smartcard are useless.

Product security and trustworthyness is not only boilt down to its capability to resists to attacks but need also to take into account :

- The way the product has been designed : bad design of the product may lead to inadequate functionnality or security measures.
- The way the product has been implemented and tested : incorect implementation of a secured design may lead to an insecured product. In the same way, if the product has not been properly tested, we have no evidence that it works with an appropriate behavior.
- The way the product may be identified. If a vendor produces secured and non-secured system, it is needed to identified secured ones in a non ambiguous way.
- The life cycle of the product. If the product is designed, produced or delivered in an insecure way, this may induce security threat. For example, the product may be substitute by a less secured one or may be modified before being delivered to TSP.
- The way the product shall be setup and used. To be used in a secured way, product shall generally been intiated in a specific manner and shall be used under specific constraint. For example, products are generally provided with default credentials that shall be changed before being used in production. It is commonly easy to take control of a system with default credential since these values are generally public or easy to find. Therefore, adequate and clear guidances on how to install and use the product or system shall be provided by vendors.

Since TSP are using generally third parties systems and products, it may be complicated for them to provide evidence of certain of the above aspects. Especially the ones that completely within the vendor scope (such as product development, implementation or design) and out of the scope of the TSP.

Moreover, it may be difficult to evaluate the level of security measure that should be associated to each of these aspects.

Finally, by evaluating itself the security of the used product, TSPs won't be able to ensure the impartiality of the evaluation.

Therefore, industry have created Security Standard for products and the associated evaluation scheme. These standards proposes a commonly accepted methodology and evaluation criteria. The two most commons are :

- Common Criteria (ISO- 15408), which is an international norm for security products
- FIPS 140-2, which is an NIST norm for cryptographic products

Notice that with the general availability of devices which meet ISO/IEC 15408, it is expected that FIPS 140-2 evaluation scheme (or ISO/IEC 19790 scheme) will no longer be acceptable.Therefore, Common Criteria (ISO-15408) standard and evaluation scheme is strongly recommended.

Common criteria evaluation methodology, for example, covers all the product security aspect mentioned above together with a evaluation methodology, based on independant and accredited evaluation Labs and a certification body, that ensure a impartiality of the evaluation.

Therefore, a TSP using a product that have been evaluated against one of these methodology will easily provide evidence of the trustworthiness ot the used products. **Consequently, it is recommended to qualified TSP to implement evaluated trust system when possible** (when an evaluation scheme and the associated protection profile exists typically).

Evaluating a product against a security standard may not be sufficient. Security products may offer several functionalities, some may be evaluated and some may not. **Therefore, a TSP should ensure that the product has been evaluated, but also that precisiely the functionnality needed for providing its qualified service have been evaluated and that they met the adequate security level.**

To ease the work of the Secure product user, and to provide product with comparable security functionalities, methodology such as Common Criteria proposes so called Protection Profiles. These protection profile, mostly considered as industry standard, are templates specifying, particularly :

- A set of security requirements and functionalities that a product shall met for ensuring a specific purpose.
- A security level to be reached.

TSP using products that are compliant with such Protection Profiles will have stronger evidence that they meet the industry standard.

3. PROTECTION PROFILES AND APPLICABLE STANDARDS FOR TRUST SERVICES

Since Trust Service Providers may provide several Qualified Trusted Services, the underlying products and services used to operate these services may have differents functionnalities. Therefore, threats against these products and system may differ from one service to another.

It is important for a TSP to identify which product may be used to operate the service in a secure manner. For that, it is recommended to refer to security standards that are commonly accepted by industry. A list of such standard is maintained by SOG-IS[1].

We provide, for each type of qualified trusted services, guidelines for the standards thay may be applied.

A. TRUSTWORTHY SYSTEM FOR TSP ISSUING CERTIFICATES

For a TSP issuing qualified certificates, it is crucial that the private key used to sign (*i.e*. certify) the subject public key is protected in an adequate manner. EN 319-411 part2 is a European Norm provides a list of requirements considered by industry as sufficient to issue Qualified Certificates. § 6.5.2 defines requirements related to *Private Key Protection and Cryptographic Module Engineering Controls.* This section refers to another related norm EN 319-411 part1 § 6.5.2

[1] https://www.sogis.org/uk/pp_en.html

EN 319-411 part1 § 6.5.2 states that for Key Generation:

> *(…) the following particular requirements apply:*
>
> *a) CA key generation shall be carried out within a secure cryptographic device which:*
>
> *i) meets the requirements identified in ISO/IEC 19790 [3]; or*
>
> *NOTE 1: Demonstrated conformance to FIPS PUB 140-2 [i.13], level 3 is considered as fulfilment of this requirement.*
>
> *NOTE 2: Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO/IEC 15408 [1], are currently under development within CEN as CEN EN 419 221-2 [i.17] orCEN EN 419 221-3 [i.18], CEN EN 419 221-4 [i.19], or CEN EN 419 221-5 [i.20].*
>
> *ii) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], orequivalent national or internationally recognized evaluation criteria for IT security. This shall be to asecurity target or protection profile which meets the requirements of the present document, based on arisk analysis and taking into account physical and other non-technical security measures. NOTE 3: This applies also to key generation even if carried out in a separate system.*

EN 319-411 part1 § 6.5.2 states that for the use of the signature:

> *The CA private signing key shall be held and used within a secure cryptographic device which:*
>
> *i) meets the requirements identified in ISO/IEC 19790 [3], or*
>
> *NOTE 4: Demonstrated conformance to FIPS PUB 140-2 [i.13], level 3 is considered as fulfilment of this requirement.*
>
> *NOTE 5: Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO/IEC 15408 [1], are currently under development within CEN as CEN EN 419 221-2 [i.17] or CEN EN 419 221-3 [i.18], CEN EN 419 221-4 [i.19] or CEN EN 419 221-5 [i.20].*
>
> *ii) is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.*

Therefore, it is important to notice that the norm recommends several solutions for an adequate protection of the keys. A TSP that would like to provide evidence that it uses a trustworthy system may choose among one of these solutions.

The following table provide the synthesis of the possibilities secure cryptographic device.

#	Security Level	Elements to provide	Comment
1	**Conformance with Common Criteria ISO/IEC 15408 and in conformity with one of these protection profile :** **1. EN 419 221-2** **2. EN 419 221-3** **3. EN 419 221-4** **4. EN 419 221-5**	Certificate of the conformity	List of certified products may be found on Common Criteria Portal[2]. It is necessary to verify both the evaluation and the conformity to the protection profile.
2	**Conformance with Common Criteria ISO/IEC 15408 at EAL 4**	Certificate of the conformity of the product + Risk analysis + demonstration of coverage or the requirement.	The conformance to Common Criteria without conformance to protection profile will need extra demonstration by the TSP.
3	**National or internationally recognized evaluation criteria for IT security that is equivalent to Common Criteria ISO/IEC 15408**	Certificate of the conformity of the product to evaluation + Risk analysis + demonstration of coverage or the requirement + evidence of the equivalence of the evaluation criteria to ISO/IEC 15408	TSP shall provide all elements of case 3 and shall also provide evidence that its evaluation scheme is equivalent to ISO/IEC 15408.
4	**Conformity with FIPS PUB 140-2 level 3**	Certificate of the conformity	NIST provides a list of certified cryptographic modules on its website[3]. It is important to notice that FIPS evaluation allow to meet partially the level 3 (e.g. some evaluation unit may be at level 3 and others at level 2). To meet this requirement, overall level 2 shall be met. Vendor may also provide the certificate of conformity
5	**Conformity to the requirements identified in ISO/IEC 19790**	Demonstration of conformity	TSP shall provide a demonstration of conformity to the requirements. This may be done, for example, by using a products that meet partially the two above requirements and demonstrating that non-covered requirements are not necessary to meet ISO/IEC 19790 requirements.

Solution 1 and 2 provides an easy way for TSP to claim its conformance to the EN 319-411 part1 § 6.5.2 requirement, since it is boiled down to the choice of a product that have already been performed and the

[2] https://www.commoncriteriaportal.org/products/

[3] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

capability to provide a certificate of conformance that can be easily checked. A TSP that uses such product will then use the industry standard and demonstrating its conformance to Article 24.2 (e) is therefore easier.

Notice that ETSI standard states also that:

> *NOTE 2 : With the general availability of devices which meet ISO/IEC 15408 [1], it is expected that ISO/IEC 19790 [3] or FIPS 140-2 [12] level 3 will no longer* be acceptable."

This shall be taken into account in the choice of the system and Common Criteria (*ISO/IEC 15408) should be preferred.*

TSP may also adopt other solutions, but demonstration may be more complicated to produce and may need more effort for the TSP.

It is important to notice that a TSP may use the same Trustworthy system for generating its keys and to use theses keys but may also use different Trustworthy system to perform each of these operations.

If different systems are used for these operations, this means that the keys shall be exported from the Trustworthy system that have generated the keys and then imported in the Signing trustworthy system. This transfer shall be performed in a secure way. EN 319-411 recommends that

> *c) [CONDITIONAL]: When outside the secure cryptographic device (see item b) above) the CA private signing key shall be protected in a way that ensures the same level of protection as provided by the signature creation device.*
>
> *d) The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 6.4.2). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.*

Regarding the management of the product, the following recommendation applies.

> *g) The secure cryptographic device shall not be tampered with during shipment.*
>
> *h) The secure cryptographic device shall not be tampered with while stored.*
>
> *i) The secure cryptographic device shall be functioning correctly.*

Moreover CA service may not only use a cryptographic module to protect the CA keys and the signature process, but may also use a system to manage and produce the certificates. For that *EN 419 261 Security requirements for trustworthy systems managing certificates for electronic signature* provides a set security requirements for a software interacting with the above cryptographic module and handling a set of functionalities for generating and managing certificates.

A TSP that use a system that has been evaluated in conformity with the list of requirement **of** *EN 419 261* or that can demonstrate its conformity to these requirements *w*ill provide strong evidence of its conformity to Article 24.2 (e).

B. TRUSTWORTHY SYSTEM FOR TSP ISSUING TIMESTAMPS

EN 319-421 is a European Norm providing a list of requirements considered by industry as sufficient for a TSP to issue Time Stamps.

Concerning the protection of the keys and the cryptographic module, §7.6.2 states that

> *The generation of the TSU's signing key(s) shall be carried out within a cryptographic module(s) which either:*
>
> *- meets the requirements identified in ISO/IEC 19790 [2], level 3 or higher; or*
>
> *NOTE 1: Demonstrated conformance to FIPS PUB 140-2 [i.9], level 3 is considered as fulfilment of this requirement.*
>
> *- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [3]; or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.*
>
> *NOTE 2: Standards specifying common criteria protection profiles for TSP cryptographic modules, in accordance with ISO 15408 [3], are currently under development within CEN as CEN EN 419 221-2 [i.14] or CEN EN 419 221-3 [i.15], CEN EN 419 221-4 [i.16], or CEN EN 419 221-5 [i.17].*

The following table summarizes the possibility recommended to the TSP.

#	Type of compliance	**Evidence to be provided**	**Comment/useful information**
1	**Conformance with Common Criteria ISO/IEC 15408 and in conformity with one of these protection profile :** **1. EN 419 221-2** **2. EN 419 221-3** **3. EN 419 221-4** **4. EN 419 221-5**	Certificate of the conformity	List of certified products may be found on Common Criteria Portal[4]. It is necessary to verify both the evaluation and the conformity to the protection profile.
2	**Conformance with Common Criteria ISO/IEC 15408 at EAL 4**	Certificate of the conformity of the product + Risk analysis + demonstration of coverage or the requirement.	The conformance to Common Criteria without conformance to protection profile will need extra demonstration by the TSP.
3	**Conformity with FIPS PUB 140-2 level 3**	Certificate of the conformity	NIST provides a list of certified cryptographic modules on its website[5]. It is important to notice that FIPS evaluation allow to meet partially the level 3 (e.g. some evaluation unit may be at

[4] https://www.commoncriteriaportal.org/products/

[5] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

			level 3 and others at level 2). To meet this requirement, overall level 2 shall be met. Vendor may also provide the certificate of conformity
4	**Conformity to the requirements identified in ISO/IEC 19790**	Demonstration of conformity	TSP shall provide a demonstration of conformity to the requirements. This may be done, for example, by using a product that meet partially the two above requirements and demonstrating that non-covered requirements are not necessary to meet ISO/IEC 19790 requirements.

Solution 1 provides an easy way for TSP to claim its conformance to the EN 319-421 part1 §7.6.2 and §7.6.3 requirements, since it is boiled down to the choice of a product that have already been performed and the capability to provide a certificate of conformance that can be easily checked. A TSP that uses such product will then use the industry standard and demonstrating its conformance to Article 24.2 (e) is therefore easier.

Notice that ETSI standard states also that:

> *NOTE 2 : With the general availability of devices which meet ISO/IEC 15408 [1], it is expected that ISO/IEC 19790 [3] or FIPS 140-2 [12] level 3 will no longer* be acceptable."

This shall be taken into account in the choice of the system and Common Criteria (*ISO/IEC 15408) should be preferred.*

TSP may also adopt the third solution or demonstrate the conformance to Article 24 this method of its choice; however, in that case demonstration may be more complicated to produce and may need more effort for the TSP.

Moreover, Time-stamping service may not only use a cryptographic module to protect the TSU keys and the signature process, but may also use a system to manage and produce the time-stamp, and to ensure the accuracy of the date. For that the future EN 419 231 (Security requirements for trustworthy systems supporting time-stamping) is planned to cover this scope. This document, still currently under development by CEN, will be a Common Criteria Protection Profile defining security requirements for software interacting with the above cryptographic module and handling a set of functionalities for generating and managing time-stamps.

A TSP that uses a time-stamping system that has been evaluated in conformity with this protection profile using Common Criteria ISO/IEC 15408 evaluation scheme will provide strong evidence that it meets the requirement of Article 24.2.

C. TRUSTWORTHY SYSTEM FOR TSP PROVIDING VALIDATION SERVICES

EN 119 101 is a European Norm based on ETSI technical specification TS 119 101 providing a list of requirements considered by industry as state of art of signature creation services and signature validation services. ETSI TS 119 101 § 4.2 deal with the use of trustworthy system

> *In the case where a Protection Profile (PP) for signature creation application and signature validation application is needed, the CEN document "Protection Profiles for Signature Creation & Validation Applications" (…) should be considered. The decision to conform to this PP depends on the business requirements.*

The cited CEN document *"Protection Profiles for Signature Creation & Validation Applications"* is a reference to the following document:

- ETSI EN 419 111: "Electronic Signatures and Infrastructures (ESI); Protection Profiles for Signature Creation & Validation Applications"

This norm proposes a set of requirements for Signature Creation Application or Signature Validation Application. In particular, EN 419111-4 proposes a Common Criteria protection profile for Signature Verification Application

A TSP that uses a signature validation system that has been evaluated in conformity with the above protection profile using Common Criteria ISO/IEC 15408 evaluation scheme will provide strong evidence that it meets the requirement of Article 24.2. Therefore, a TSP adopting such signature validation system may demonstrate its compliance with Article 24.2 requirement in an easier way than with alternative solution.

The demonstration of the conformity can also be supported by the application of the ETSI TS 119 441 standard (currently in draft version).

D. TRUSTWORTHY SYSTEM FOR TSP PROVIDING SIGNATURE SERVICES

For a TSP providing a Signature service, the service has to ensure

1. ensure the *technical security and reliability of the processes* of signature, that may include steps like
    a. Visualisation of the data to be signed
    b. Capture of the Signatory agreement to sign
    c. Appropriate selection of the signer certificate
    d. Appropriate selection of the type of signature and signature attributes
    e. Appropriate creations of the signature envelop.
2. In the specific case where the TSP operates the Signatory private key within a server signing, the TSP should also *ensure the technical security and reliability* of this process

We provide recommendation for these two processes.

RECOMMENDATIONS FOR SIGNATURE PROCESS

EN 119 101 is a European Norm based on ETSI technical specification TS 119 101 providing a list of requirements considered by industry as state of art of signature creation services and signature validation services. ETSI TS 119 101 § 4.2 deal with the use of trustworthy system:

> *In the case where a Protection Profile (PP) for signature creation application and signature validation application is needed, the CEN document "Protection Profiles for Signature Creation & Validation Applications" (…) should be considered. The decision to conform to this PP depends on the business requirements.*

The cited CEN document *"Protection Profiles for Signature Creation & Validation Applications"* is a reference to the following document :

- ETSI EN 419 111 "Electronic Signatures and Infrastructures (ESI); Protection Profiles for Signature Creation & Validation Applications"

This document proposes a set of requirements for Signature Creation Application or Signature Validation Application. In particular, EN 419111-2 proposes a Common Criteria protection profile for Signature Creation Application and EN 419111-3 proposes extension of this protection profile

A TSP that uses a signature creation system that has been evaluated in conformity with the above protection profile using Common Criteria ISO/IEC 15408 evaluation scheme will provide strong evidence that it meets the requirement of Article 24.2. Therefore, a TSP adopting such signature validation system may demonstrate its compliance with Article 24.2 requirement in an easier way than with alternative solutions.

It is important to notice that the use of a certified signature creation application should only stay a good practice and should not be an obligation, as mentioned in Recital 56:

the scope of the certification obligation should exclude signature creation applications

RECOMMENDATION FOR SERVER SIGNING

For TSP operating a server signing, this server signing system should be considered as a *qualified electronic signature creation devices* (see Article 29 of the regulation). Therefore, it *shall meet the requirements laid down in Annex II* of the Regulation.

There is actually no published norm describing technical requirements what are considered by industry as sufficient to meet requirements of Annex II. However:

- EN 419 241 Security requirements for trustworthy systems supporting server signing document *specifies security requirements and recommendations for Trustworthy System Supporting Server Signing (TW4S) that generate advanced electronic signatures*. Current version of EN 419 241 contains only requirements for *advanced electronic signatures* and not requirements for Qualified Electronic Signatures. Therefore, requirements defined in current version of EN 419 241 may not be sufficient for Qualified Electronic Signature. However, according to eIDAS Regulation, a Qualified Signature is an Advanced Electronic Signature. Therefore a Trustworthy System providing Qualified Electronic Signature should be able to generate Advanced Electronic Signatures. Thus, such Trustworthy System should at least cover the requirements described in current version of EN 419 241.
- A new version of EN 419 241 is planned to cover this subject. This document is is composed of 3 parts :
    - EN 419 241 part 1 should be an updated version of the current version of EN 419 241 including adaptation to the Regulation
    - EN 419 241 part 2 should define a protection profile (PP-SAP/SAD) dealing with Server Signing system. It will specifically define requirement on the authentication protocol that authenticates the Signatory and that activates the signature on the server part and the protection of the key management and the authorization to use the keys.

  Since these documents have been publicly reviewed, requirements of these documents should be taken into account for server signing design.
- Concerning the operation of the QSCD, new standards are currently being developed at ETSI:
    - TS 119 431-1: Policy and security requirements for TSP service components operating a remote QSCD / SCD

- TS 119 431-2: Policy and security requirements for TSP service components supporting AdES digital signature creation
- TS 119 432: Protocols for remote digital signature creation

Moreover, since Server Signing System operates private keys, TSP should use Trustworthy System to protect these keys. For that, a TSP which wants to meet the same level of protection than the other qualified services may use one of these solutions:

- A cryptographic module in evaluated conformity with Common Criteria ISO/IEC 15408 and in conformity with one of these protection profile :
  - EN 419 221-2
  - EN 419 221-3
  - EN 419 221-4
  - EN 419 221-5
- A cryptographic module in evaluated conformity with FIPS PUB 140-2 level 3

As mentioned before, since ETSI standards states that:

> - *NOTE 2 : With the general availability of devices which meet ISO/IEC 15408 [1], it is expected that ISO/IEC 19790 [3] or FIPS 140-2 [12] level 3 will no longer* be acceptable."

This shall be taken into account in the choice of the system and Common Criteria (*ISO/IEC 15408)* should be preferred.

It is important to notice that, regarding Server Signing, some member states have proposed alternative certification scheme[6].

E. TRUSTWORTHY SYSTEM FOR TSP PROVIDING SIGNATURE PRESERVATION SERVICES

There is actually no published standard covering requirements for preservation services. These requirements may be covered by these futures standard to be defined by ETSI:

- TS 119 511 Policy & security requirements for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques
- TS 119 512 Protocols for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques EN 319 521 Policy and security requirements for data preservation service providers

F. TRUSTWORTHY SYSTEM FOR TSP PROVIDING EDELIVERY SERVICES.

[6] https://ec.europa.eu/futurium/en/content/list-alternative-processes-notified-commission-accordance-article-303b-and-392-eidas

There is actually no published standard covering requirements for eDelivery services. ETSI EN 319 521 and ETSI EN 319 531 (Policy and security requirements for registered electronic mail (REM) service providers) is planned to cover this scope and are actually available in stable draft version.