# Analysis of standards related to Trust Service Providers

## Mapping of requirements of eIDAS to existing standards

VERSION 1.1

JUNE 2016

# About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

## Authors

Iñigo Barreira, Izenpe
Jerome Bordier, SEALWeb
Olivier Delos, SEALED
Arno Fiedler, Nimbus Technologieberatung GmbH
Tomasz Mielnicki, Gemalto
Artur Miękina, Polish Security Printing Works
Jon Shamah, EJ Consultants
Clemens Wanko, TUV Informationstechnik GmbH
Clara Galan Manso, ENISA
Sławomir Górniak, ENISA

## Contact

For contacting the authors please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

## Acknowledgements

ENISA would like to thank the numerous experts from governmental entities, industry, foundations and trust service providers who reviewed this paper for their contributions.

ISBN 978-92-9204-153-3 DOI 10.2824/540231

# Table of Contents

# Executive Summary

Pursuant to 15 years of implementation of Directive 1999/93/EC[1] on a Community framework for electronic signatures, the lack of trust and in particular the perceived lack of legal certainty have made consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new digital services.

Re-building trust in the online environment has been perceived as key to economic and social development by the European legislator. Regulation (EU) No 910/2014[2] (hereafter the eIDAS Regulation) adopted last year and repealing Directive 1999/93/EC on 1 July 2016 clearly aims to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

In order to ensure uniform conditions for its implementation, the Regulation confers implementing powers to the Commission, to promulgate implementation specifications or to reference standards the use of which would raise a presumption of compliance with select requirements laid down in the eIDAS Regulation. When adopting delegated or implementing acts, the Commission needs to take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular ETSI, CEN, ISO and ITU.

Already in 2009, the European Commission issued Standardisation Mandate 460 to CEN, CENELEC and ETSI to update the existing eSignature standardisation deliverables in view of establishing a fully rationalised framework, which would solve the issues raised in actual use of eSignatures in the EU. These issues were about, notably, the mutual recognition and cross-border interoperability of eSignatures, the multiplicity of standardization documents and the lack of usage guidelines, and different technical implementations.

This report on one hand analyses the eIDAS requirements with regard to the standards, on the other analyses currently available standards and compares the results of both analyses. Such a mapping is oriented at the requirements specified in the various eIDAS articles. Pursuant to this mapping it can be concluded that usually the analysed standards usually cover some requirements in part or whole.

Existing standards can be endorsed for being used within the frames of eIDAS Regulation, to the extent as presented in the previous sections. The analysis presented in this report led, however, to a shortlist of gaps, where specific eIDAS requirements have yet to be addressed in EU standards (ETSI/CEN/CENELEC) nor international ones.

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. OJ L 13, 19.1.2000, p. 12–20.
[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.

# 1. Introduction[3]

Pursuant to 15 years of implementation of Directive 1999/93/EC[4] on a Community framework for electronic signatures, the lack of trust and in particular the perceived lack of legal certainty have made consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new digital services.

Re-building trust in the online environment is still seen as key to economic and social development by the European legislator. Regulation (EU) No 910/2014[5] (hereafter the eIDAS Regulation) adopted last year and repealing Directive 1999/93/EC on 1 July 2016 clearly aims to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

In addition to a set of provisions addressing the mutual recognition and equivalence over the EU of national electronic identification schemes notified against a common assurance level scheme, the eIDAS Regulation is setting legal provisions for cross-border recognition and EU harmonised legal effects for a much broader range of trust services than Directive 1999/93/EC that was a mere framework-setting instrument. Furthermore, the notions of qualified trust services and qualified trust service provider have been introduced with a view to indicating requirements and obligations that ensure high-level security of qualified trust services and products are used or provided. While Directive 1999/93/EC was purposefully aimed at (a) provisions on non repudiation addressed by means of issuing qualified certificates and (b) the automatic cross-border recognition of "qualified electronic signatures" as equivalent to hand written signature, the eIDAS Regulation also addresses other types of qualified trust services. Such services aim at the protection and adoption of electronic services (e.g. eGovernment and eCommerce transactions etc.) in the digital market, including qualified electronic time stamps, qualified electronic seals, qualified validation and preservation of qualified electronic signatures/seals, qualified electronic registered delivery services and qualified website authentication.

These qualified trust services are clearly "marketed" by the Regulation to enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products.

As illustrated in Figure 1 below, through its set of (qualified) trust services related provisions and articles, it is actually a complete pyramid of trust that the eIDAS Regulation is setting up. The most visible part is the

[3] Sources:
- Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market. SMART 2012/0001. Deliverable 2.1. Recommendations for implementing acts on establishment and supervision of TSPs. DLA Piper, SEALED et al.;
- Study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market. SMART 2012/0001. Deliverable 5. Report on the follow-up of mandate m460 - Gap Analysis. DLA Piper, SEALED et al.

[4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. OJ L 13, 19.1.2000, p. 12–20.

[5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014, p. 73–114.

"EU trust mark for qualified trust services", which each qualified trust service provider may use to brand and promote the quality and trustworthiness of the qualified trust services it provides.

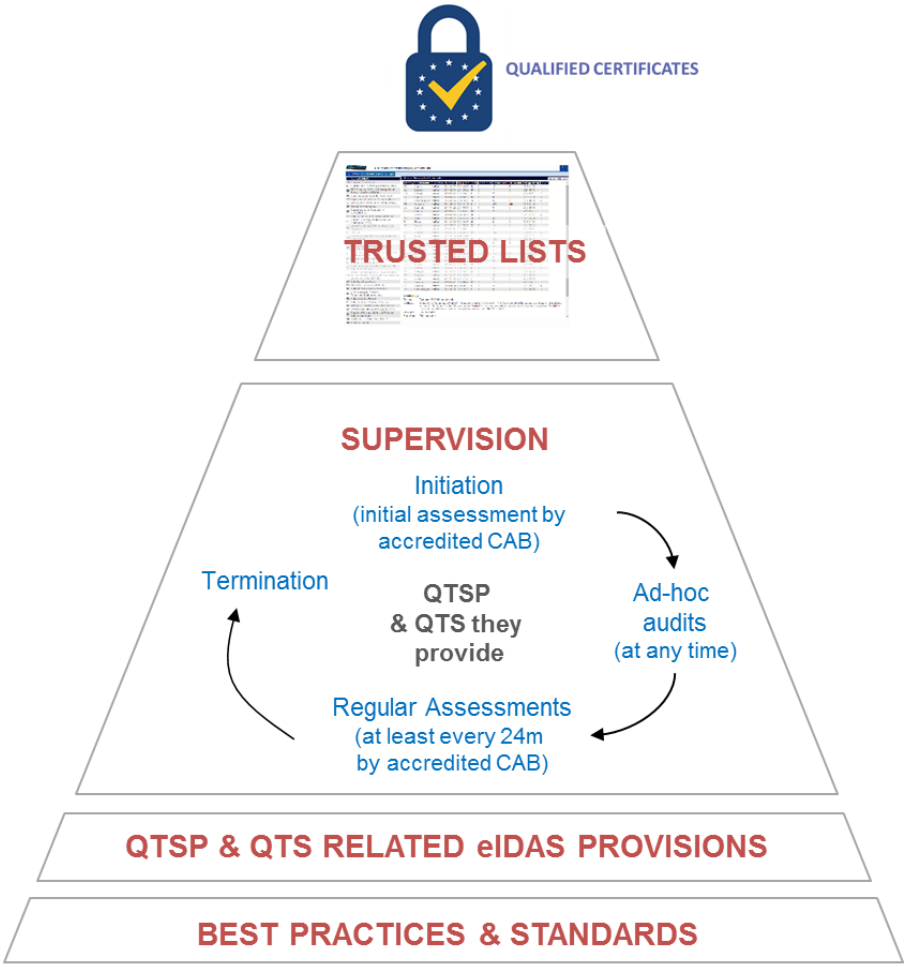



**Figure 1**: eIDAS Regulation building trust in the online environment – Supervision

(Source: IAS² study)

This trust mark introduced by the eIDAS Regulation and further defined by Commission Implementing Regulation (EU) 2015/806[6] is expected to be the convenient distinctive mark for online services users to identify qualified trust services provided by qualified trust service provider and gain confidence in such services to secure online service they are using or about to use. By clearly differentiating high quality and trustworthy qualified trust services from other services, using a trust mark, it is expected that transparency in the market will improve. The users will be helped to fully benefit and consciously rely on electronic services supported by qualified trust services and hence to contribute to the development of the digital market.

The adoption of a trust mark, its credibility, and trustworthiness require a legal basis (as per Art.23 of the Regulation) and a suitable set of procedural, quality and security requirements to comply with.

[6] Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services. OJ L 128, 23.05.2015, p13-15.

Additionally a mechanism is needed to notify the market that qualified trust service providers meet such requirements and obligations so that users of such services can make informed decisions.

As illustrated in the above Figure 1, the eIDAS Regulation explicitly sets up a consistent set of quality andsecurity requirements and obligations for qualified trust services (QTSs) and qualified trust service providers (QTSPs). These requirements aim to enhance the trust of consumers and enterprises, in particular SMEs, in the internal (electronic) market and to promote the use of such qualified trust services and products.

Through ex-ante and ex-post supervisory activities the eIDAS Regulation sets up a supervisory regime upon these quality and security requirements and obligations for QTSs and QTSPs. The eIDAS Regulation aims to ensure that, from before providing qualified services up to terminating such services, the QTSPs indeed meet these requirements. This supervisory regime for QTS' and QTSPs is enforced in each EU Member State (MS), through a national supervisory body to ensure a comparable security level of QTSs over the EU.

The supervisory regime covers the entire life-cycle of the QTSP and their QTSs and in specific:

- It relies on a pre-authorisation mechanisms obliging trust service providers intending to provide QTS to notify the competent supervisory body of their intention together with a conformity assessment report (CAR) issued by an accredited conformity assessment body (CAB) attesting that the QTSP and the QTSs it intends to provide meet the requirements laid down in the Regulation.
- Once qualified status is granted, it obliges, QTSPs to re-affirm attestations, as above, each two years.
- It allows competent supervisory bodies, at their own discretion and at any time, to audit themselves or to request an accredited CAB to perform a conformity assessment of a QTSP/QTS and to produce a CAR confirming that the QTSP and the QTSs it provides meet the requirements laid down in the Regulation.
- It foresees rules to be followed by QTSP and supervisory activities to be performed in cases where the QTSP changes or terminates the provisioning of a QTS, or risk ceasing operating.

The decisions to grant or withdraw qualified status to trust services and trust service providers, resulting from the above described supervisory activities, are taken by the national supervisory bodies .

All associated decisions are published in electronically signed or sealed national trusted lists. Such national trusted lists are established, maintained and published to disseminate in a trustworthy manner information related to the qualified trust service providers for which a Member State is responsible, together with information related to the qualified trust services provided by them, including the whole history of the qualified status they have been granted.

The mandatory EU MS national trusted lists are published at least in a form suitable for automated processing. In practice these are XML files. The voluntary "EU trust mark for qualified trust services", aims to make any such qualification visible to the consumer. The eIDAS Regulation obliges QTSPs using such a trust mark to provide, close to it, a link to the corresponding trusted list allowing for verification.

The pyramid of trust further relies on and is strengthened by the use of best practices and standards. In order to ensure uniformity the Regulation confers implementing powers on the Commission, with regard to specifications and standards referencing (Recital (71)).

When adopting delegated or implementing acts, the Commission typically takes account of standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications

Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services (Recital (72)).

Seven implementing acts are foreseen by the Regulation to support implementation of eIDAS, as illustrated in Figure 2. Two mandatory implementing acts have to be laid down respectively on trust marks[7] and trusted lists[8], three optional implementing acts supporting the supervisory regime, respectively on conformity assessment bodies, QTSP initiation and supervisory body yearly activities reports, and two optional implementing acts on common provisions respectively on TSPs and on QTSPs.

Additional implementing acts are foreseen on specific provisions per type of (qualified) trust service and trust service provider.

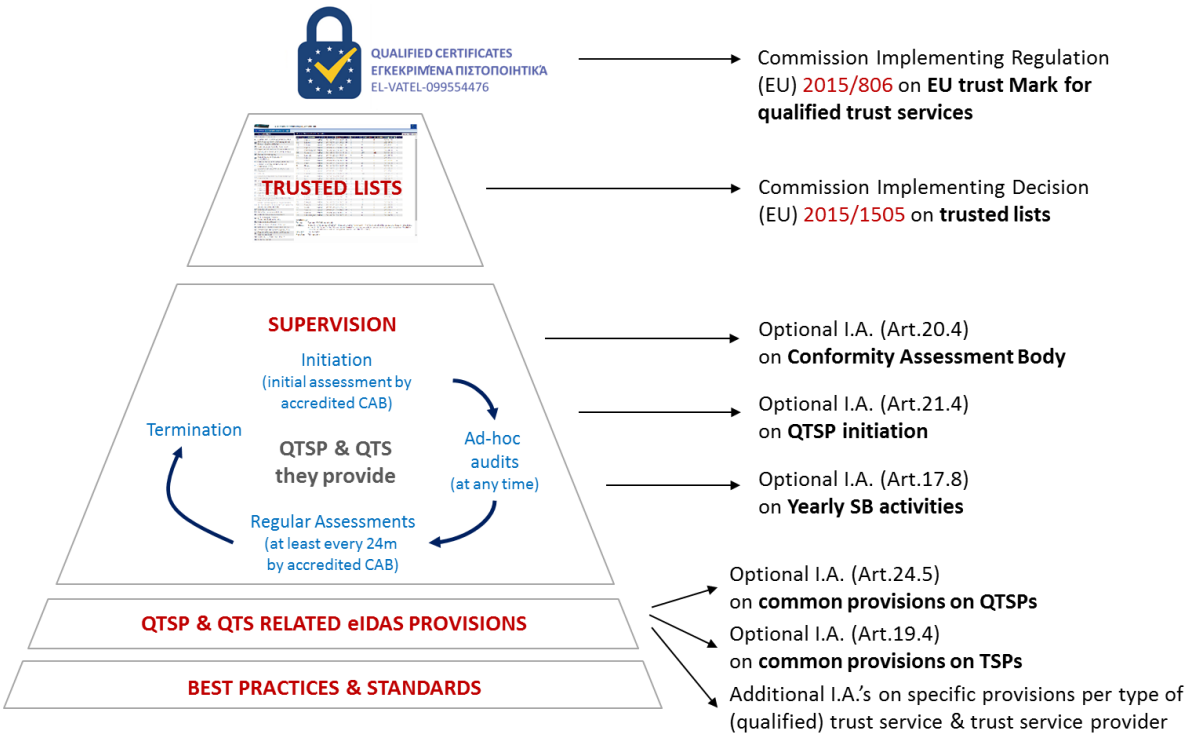



**Figure 2**: Implementing acts foreseen to support the Regulation in implementing provisions on supervision.

(Source: IAS² study)

[7] Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services. OJ L 128, 23.05.2015, p13-15.
[8] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p26-36.

These implementing acts can also be split in terms of type of the legislative power conferred to the Commission:

- Implementing acts for which the EC is empowered to define the technical requirements and specifications that when met will grant presumption of compliance with the corresponding legal provisions:
    - Art.17(8) - defines formats and procedures for the annual report supervisory bodies submit to the Commission about its previous calendar year's main activities along with a summary of breach notifications received from trust service providers.
    - Art.19(4)a - specifies the technical and organisational measures TSPs implement to manage risks posed to the security of the trust services they provide (Art.19(1)).
    - Art.19(4)b - defines formats, procedures and deadlines, applicable for the purpose of security and personal data breach notifications by TSPs and QTSPs (Art.19(2)).
    - Art.21(4) - defines formats and procedures for the purpose of Art.21(1) (notification by TSPs of their intention to start providing QTSs together with a conformity assessment report issued by a conformity assessment body) and of Art.21(2) (verification by supervisory body of compliance with Regulation requirements).
    - Art.22(5) - defines the technical specifications and formats for trusted lists and corresponding notification from EUMS to the European Commission (Art.22(1)to(4)). Adopted as CID 2015/1505/EU.
    - Art.23(3) – contains specifications with regard to the form, such as presentation, composition, size and design of the EU trust mark for qualified trust services. Adopted as CIR 2015/806/EU.
    - Art.27(5) - defines reference formats of advanced electronic signatures in public services or reference methods where alternative formats are used. Adopted as CID 2015/1506/EU[9].
    - Art.31(3) - defines formats and procedures applicable for the purpose of the notification by Member States to the European Commission of information on qualified electronic signature creation devices that have been certified by their designated bodies and information on electronic signature creation devices that are no longer certified (Art.31(1)).
    - Art.37(5) - defines reference formats of advanced electronic seals in public services or reference methods where alternative formats are used. Adopted as CID 2015/1506/EU.
    - Art.39(3) - defines formats and procedures applicable for the purpose the notification by Member States to the Commission of information on qualified electronic seal creation devices that have been certified by their designated bodies and information on electronic seal creation devices that are no longer certified (Art.31(1)).
- Implementing acts for which the Commission establishes reference numbers of standards but is not empowered to determinate directly their content:
    - Art.20(4) establishes reference number of the following standards:
        (a) accreditation of the conformity assessment bodies and for the conformity assessment report referred to in Art.20(1);

[9] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced electronic seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p37-41.

(b) auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in Art.20(1).

- Art.24(5) - reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of Art.24.
- Art.27(4) - reference numbers of standards for advanced electronic signatures (in public services).
- Art.28(6) - reference numbers of standards for qualified certificates for electronic signatures.
- Art.29(2) - reference numbers of standards for qualified electronic signature creation devices.
- Art.30(3) - a list of standards for the security assessment of information technology products included in the list of qualified electronic signature creation devices whose conformity with the requirements laid down in Annex II of the Regulation has been certified by appropriate public or private bodies designated by Member States.
- Art.32(3) - reference numbers of standards for the validation of qualified electronic signatures.
- Art.33(2) - reference numbers of standards for qualified validation service for qualified electronic signatures (Art.33(1)).
- Art.34(2) - reference numbers of standards for the qualified preservation service for qualified electronic signatures (Art.34(1)).
- Art.37(4) - reference numbers of standards for advanced electronic seals (in public services).
- Art.38(6) - reference numbers of standards for qualified certificates for electronic seals.
- Art.39(1) - reference numbers of standards for qualified electronic seal creation devices.
- Art.39(2) - a list of standards for the security assessment of information technology products included in the list of qualified electronic seal creation devices whose conformity with the requirements laid down in Annex II of the Regulation has been certified by appropriate public or private bodies designated by Member States.
- Art.40 - reference numbers of standards for the validation of qualified electronic seals.
- Art.40 - reference numbers of standards for qualified validation service for qualified electronic seals.
- Art.40 - reference numbers of standards for the qualified preservation service for qualified electronic seals.
- Art.42(2) - reference numbers of standards for the binding of date and time to data and for accurate time sources in the context of qualified electronic time stamps (Art.42(1)).
- Art.44(2) - reference numbers of standards for processes implemented by qualified electronic registered delivery service for sending and receiving data (Art.44(1)).
- Art.45(2) - reference numbers of standards for qualified certificates for website authentication.

- Art.30(4) delegated acts concerning the establishment of specific criteria to be met by the designated bodies certifying the conformity of qualified electronic signature creation devices with the requirements laid down in Annex II.

Amongst the above list of secondary legislative acts, only four implementing acts are mandatory, timed and adopted (trust mark, trusted lists and electronic signatures/seals format in public services and standards for the security assessment of information technology products under article 30.3) For the rest

of implementing acts, it is clearly expected that industry will self-regulate as much as possible within the legal and supervisory framework provided by the Regulation.

When the European Commission is empowered to draft secondary legislation it:

- Produces drafts of sets of rules published as a delegated or an implementing act; in this case there would be no (EU) standard, but a piece of secondary legislation to be approved according to article 48.2 of the Regulation.
- Issues a Mandate to European Standardisation Organisations to produce a standard that will be referenced by a delegated or implementing act. Such standards should clearly separate the purely technical (industry) part and the eventual regulatory part that implements or specifies a specific aspect of the Regulation.

Currently, an informal expert group has been set up by the Commission, composed of MS experts to draw up a compilation of mandatory Implementing Acts in 2015 and will do the same for non mandatory ones as well.

# 2. Requirements of eIDAS

## 2.1 Supervision and conformity assessment requirements

### 2.1.1 Conformity assessment bodies accreditation & conformity assessment rules

The ex ante and ex post supervisory regime covering the entire life-cycle of the QTSP and the QTSs they provide relies on conformity assessment reports issued by a conformity assessment body (initiation of a QTS, two-yearly assessment, ad hoc assessment at discretion of supervisory body).

As per Art.3.(18) a 'conformity assessment body' refers to 'a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008 [7], which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides'.

The European co-operation for Accreditation (EA - www.european-accreditation.org) is the body established under Regulation (EC) No 765/2008 to define the accreditation schemes used by national accreditation bodies (NAB) to accredit CABs in a specific context like the one defined by the eIDAS Regulation.

EA and CEN/ETSI have already set up discussions to establish, under Regulation (EC) No 765/2008, the scheme under which national accreditation bodies (NABs) shall accredit, in accordance with Regulation (EU) No 910/2014, conformity assessment bodies (CABs), as competent to carry out conformity assessments referred to in its Art.20.1 and whose purpose is '*to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation*'.

That accreditation scheme is organised as follows:

- The retained scheme relies on ISO/IEC 17065 (Internal & External Services), as the general framework for accrediting the competency of CABs to assess products, processes and services, and within this framework requires to demonstrate their:
  - competency to carry out specific ISO/IEC 17021 -based assessments,
  - competency to carry out specific ISO/IEC 27006 -based assessments (Information Security Management Systems - ISMS).

Note: Beyond ISO/IEC 17065, no additional accreditation is further required according to ISO/IEC 17021 and ISO/IEC 27006

- The scheme also defines a "sectoral" specific framework, to further accredit the competency of CABs to carry out assessments of qualified trust service providers (QTSPs) and qualified trust services (QTSs) they provide. This specific framework builds on EN 319 403 to specify the general requirements for CABs and the general auditing rules under which CABs will carry out their conformity assessments of QTSPs and their QTSs.
- In order to be complete, the accreditation scheme requires the identification of a specific set of "TSP audit criteria", as defined in EN 319 403, against which the competences of CABs to assess the QTSPs/QTSs will be accredited and against which the conformity assessment of QTSPs/QTSs will be conducted by the accredited CAB's. EN 319 403 allow these "TSP audit criteria" to:

- take into account specificities of the type of trusted service to be assessed;
- ensure that all aspects of the TSP activity are fully covered; and
- be based on standards, publicly available specifications and/or regulatory requirements.

Leveraging on such an accreditation scheme, the competence of accredited CABs would be recognised to cover not only the conduction of Art.20.1 two-yearly conformity assessments but also the initial conformity assessments referred to in Art.21, as well as ad-hoc assessments referred to in Art.20.2. These assessments can perfectly result in conformity assessment reports based on the same set of QTSP/QTS audit criteria as used for two-yearly conformity assessments (Art.20.1).

### 2.1.2 CAB as certification bodies

It should be noted as well that this accreditation scheme requires CABs to be certification bodies, and not simply inspection bodies or laboratories, as CABs are required to certify the conformity of TSPs against the identified TSP audit criteria against which the assessment is conducted.

*'EA members unanimously selected ISO 17065[10] as the best option as basis for the accreditation of CABs in the context of conformity assessments of TSPs and trust services they provide, and in particular assessment of QTSPs/QTSs. EA experience is that ISO 17020[11] is not considered appropriate to assessment of conformance of requirements for the management system of the TSP, and it is considered that review of the security management system of TSP provides an important part of a TSP audit.*

*Also, 17020 does not impose a continued assessment by following deviations of the use of certification brands. Inspection processes tend to review the status of the items being inspected at a point in time whereas the requirements for a TSP need a more long term, continuous assessment as provided by a certification scheme. The issue of certification includes requirements for regular surveillance activities as well as specific requirements for ongoing quality and service improvement.*

*On their own ISO 27006[12] and 17021[13] are not considered sufficient to cover assessment of specific service requirements. However, ISO 17065 was specifically designed to be extended to incorporate requirements from 17021, but the opposite is not true as ISO 17065 requirements do not fit well into ISO 17021.*

*The industry requirement for public trust services, such as reflected in the CA Browser Forum guidelines and for other national schemes for non-qualified trust services, is for a clear indication of the technical compliance to industry good practice. The aim of the EN 319 403 conformity assessment is also to allow assessment of conformance to industry good practices as well as that the technical requirements of the Regulation are met. ETSI/CEN consider that any scheme which falls short of assessment against industry good practice will bring the acceptability of qualified trust services into question.*

*Furthermore, there seem to be a market requirement for a clear statement in the international context where an independent non-governmental statement of conformance.'*[14]

[10] http://www.iso.org/iso/catalogue_detail?csnumber=46568
[11] http://www.iso.org/iso/catalogue_detail?csnumber=52994
[12] http://www.iso.org/iso/catalogue_detail.htm?csnumber=62313
[13] http://www.iso.org/iso/catalogue_detail?csnumber=61651
[14] EA/ETSI disposition on comments made during the approval process of EN 319 403

The certification decision of the CAB as to whether QTSP/QTS assessed (technically, operationally and procedurally) meet the requirements of the eIDAS Regulation addressed in Art.20.1 with regards to two-yearly assessments. Same decisions are required in the context of initial assessments (Art.21) and of ad hoc assessments (Art.20.2) conducted by accredited CABs.

Certification decisions of the CABs do not automatically entail an obligation for the Supervisory Body to align its decision as to whether to grant a qualified status to the trust service provider and the trust service it provides. With regards to supervision of QTSPs/QTSs, Regulation 910/2014/EU gives an exclusive legal competence for the national Supervisory Body (SB) in granting the qualified status to trust service providers and the trust services they provide (see Art.17.4.g, Art.20.3 and Art.21.2).

### 2.1.3 "TSP audit criteria" in the context of eIDAS Regulation

In any other context than Regulation (EU) No 910/2014, having a specific technical standard such as "TSP audit criteria" allows TSPs to demonstrate conformity against such a standard to interested parties benefiting from the certification issued by the accredited CAB as a result of a successful conformity assessment. For example, TSPs being certified by an accredited CAB against EN 319 411-1 ("Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements") would likely be entitled to be accepted by CA/Browser Forum members for inclusion of their CA root certificates in the corresponding CA root certificates trust stores of these members.

However in the context of Regulation (EU) No 910/2014, limiting the "TSP audit criteria" to one or more specific technical standards raise some issues:

- **Expected purpose**: As per Art.20.1 of the Regulation, the expected purpose of conformity assessment reports from accredited CAB on QTSPs/QTSs is "*to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation*". These eIDAS conformity assessment reports (initial, two-yearly and ad hoc[15]) must confirm that the QTSP/QTS meet all the applicable requirements of the eIDAS Regulation. Their purpose is not to confirm the conformity of the QTSP/QTS to a specific technical standard addressed to TSPs.

None of the CEN/ETSI standards cover all requirements of the Regulation applicable to the addressed (Q)TSP/(Q)TS. They only cover the technical counterparts of an important but limited set of legal provisions laid down in the Regulation.

The "TSP audit criteria against which the competences of CABs to assess the QTSPs/QTSs will be accredited and against which the conformity assessment of QTSPs/QTSs will be conducted by the accredited CAB's" (hereafter called "QTSP/QTS audit criteria") should allow accredited CABs to assess whether QTSPs/QTSs meet the requirements of the Regulation not how they meet them.

- **De facto mandatory TSP standards**: Assuming that one or more CEN/ETSI standards would address and cover all requirements applicable to a specific type of QTSP/QTS, having such standards as the "QTSP/QTS audit criteria" would make them de facto obligatory for QTSPs and the QTSs they provide. Indeed as QTSPs must be assessed by accredited CABs, when CABs

[15] Standards mentioned require annual surveillance of TSPs, but from the eIDAS Regulation, there is no such recurrence needed, as there is a continuous supervision from the Supervisory Body that is entitled to conduct an ad-hoc audit or request an ad-hoc assessment from an accredited CAB.

are accredited only against such standards, there is no other choice for QTSPs to comply with such standards; otherwise they could not be assessed by an accredited CAB.

The eIDAS Regulation is intimately associated to an implementing technical layer that will mainly rely on standards adopted by standardisation bodies (as per articles 2(1) , (8), (9) and (10) as well as Annex I of Regulation 1025/2012/EC) and technical specifications. Such a technical layer could be used by stakeholders on a voluntary basis as one manner to implement the requirements of the Regulation. It would not be acceptable that a standard became de facto mandatory.

The implementation of the eIDAS accreditation scheme should target the same approach with regards to the QTSPs/QTSs, allowing them to implement any method, standardised or not, to meet the applicable requirements of the Regulation.

Furthermore, Art.20.4 implementing acts are addressing CABs *and not QTSPs* with regards to the referencing of standards, in particular on their accreditation, conformity assessment reports, and auditing rules under which they will carry out their conformity assessment of the qualified trust service providers.

- **Incomplete standard referencing scheme in the eIDAS Regulation with regards to QTSP/QTS obligations**: The eIDAS Regulation allows, through the adoption of secondary legislation, to establish reference numbers of standards, which when they are met will provide legal presumption of conformity to the corresponding legal provisions. However it should be clearly noted that not all the requirements applicable to a specific type of QTSP/QTS are covered by such a referencing mechanism. E.g. from Art.24 on requirements for QTSPs, only Art.24.(2).e and Art.24.(2).f requirements benefit from such a referencing.

It is not possible to establish a list of standards applicable to QTSPs/QTSs that will provide presumption of conformity with the Regulation.

- **IA foreseen in Art.20.4 are optional**: It should be noted that the implementing acts foreseen in Art.20.4 are not mandatory but optional. There is no obligation for the European Commission to establish such acts. The provisions of the eIDAS Regulation are supposed self-sufficient in order to ensure the applicability of the legal framework. As for all optional implementing acts, these Art.20.4 acts are deemed related to non-essential elements of the Regulation that are not substantial for the Regulation to work. The need to adopt them must be assessed on a case-by-case basis in the light of several principles including
    - **The eIDAS framework consistency:** in the present case adopting Art.20.4 implementing acts would require to ensure its consistency with other implementing acts granting QTSPs/QTSs with presumption of compliance with some legal provisions.
    - **Taking into account stakeholders/market needs**: evaluating stakeholders / market's demands and needs, potential barriers hamper eIDAS adoption and take-up
    - **Favouring non-regulatory approach, co-regulatory approach and development under other regulatory frameworks**: In this case, as the implementation of an eIDAS accreditation scheme may be ensured under the framework of Regulation 765/2008/EC, as being set up by EA, the implementing act foreseen in art.20.4 may not be needed. Furthermore adopting a secondary act means codifying a given technological approach that may quickly become obsolete, requiring a revision of the adopted act.

- **Availability and adequacy of standards**: Following the availability of a standard, the Commission may assess whether to list it in an implementing act.
- **Availability of QTSPs/QTSs standards is important but not required**: Considering the current status of the European (ETSI, CEN/CENELEC) standardisation framework, it is unlikely that all types of QTSPs/QTS will be addressed by technical specifications and standards
- **Outcome based "QTSP/QTS audit criteria" in the context of eIDAS Regulation:** For all the above-stated reasons, in the eIDAS accreditation scheme being set up by EA under Regulation 765/2008/EC, the "QTSPs/QTSs audit criteria"[16] should be designed in such a way that:
    - The resulting conformity assessment reports issued by accredited CABs aim to confirm that the qualified trust service providers and the qualified trust services provided by them meet the requirements laid down in the eIDAS Regulation.
    - It consists of one or more separate standards, outcome based, mapping audit criteria built as control objectives and controls, against the requirements of the Regulation per type of qualified trust service. These criteria shall be used by accredited CABs as a basis for establishing the conformity assessment report to be issued by them confirming QTSP/QTS they assess meet all applicable requirements from the Regulation.
      These criteria defined in an "outcome based" approach could leverage on the check lists specified by or in the context of relevant available standards (e.g. the check list from ETSI draft EN 319 411-2 with regards to QTSPs issuing qualified certificates); it should however be clear that these criteria are for use by CABs as a method to produce a conformity assessment report on the conformity of the audited QTSPs/QTSs and shall not presuppose or require QTSPs/QTSs to comply with the standards from which they are derived. QTSPs/QTSs are free to implement such standards, any other standard or no standard at all. Current CEN/ETSI standards addressing QTSP and QTS related specifications, including the ETSI EN 319 4x1 series and any other relevant standards, can be used by TSPs on a voluntary basis but cannot be made (de facto) mandatory.
    - Whenever compliance with part of the applicable eIDAS requirements would be deemed satisfied by compliance with a referenced standard, this would be acknowledged provided the conformity with such a referenced standard has been assessed and confirmed by an eIDAS accredited CABs.

Currently no such QTSPs/QTSs audit criteria standard exists and the European Commission should ask CEN/ETSI to prepare it as matter of priority.

This does not prevent the accreditation scheme being set up by EA and CEN/ETSI to allow accreditation of CABs against specific set of TSP oriented standards so that TSPs/TSs and/or QTSPs/QTSs can benefit from certification of conformity against any of such specific standards. This can be used to certify compliance with standards for use outside the context of the eIDAS Regulation (e.g. CA/Browser Forum and the associated industry) but also for attesting compliance with standards possibly referenced in eIDAS secondary legislation.

[16] i.e. TSP audit criteria against which the competences of CABs to assess the QTSPs/QTSs will be accredited and against which the conformity assessment of QTSPs/QTSs will be conducted by the accredited CAB's.

## 2.2 Requirements that TSPs should put in place in order to provide certain services

### 2.2.1 Requirements common to all TSPs

- **Data processing and protection** (Art.5)
    - *Art.5.1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.*
    - *Art.5.2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.*
- **Liability and burden of the proof** (Art.13)
    - (Art.13.1) TSP liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation
        - Burden of proving intention/negligence of non-qualified TSP is on claiming party
        - Intention or negligence of a QTSP shall be presumed, unless proven otherwise by QTSP
    - (Art.13.2) When TSP informed customer in advance on limitations on the use of their services, & when such limitations are recognisable to third parties, TSP not liable when limitations have been exceeded.
    - (Art.13.3) In accordance with national rules on liability.
- **Accessibility for person with disabilities** (Art.15) – where feasible
- **Due diligence** (Art.19.1)
    - shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.
    - Having regard to the latest technological developments, these measures shall ensure that the level of security is commensurate to the degree of risk
    - measures shall be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents
- **Security & personal data breach notification** (Art.19.2)
    - shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein
    - shall also notify the [likely adversely affected] natural or legal [customer] of the breach of security or loss of integrity without undue delay
    - May be required by the supervisory body to inform the public, when it is in the public interest

The Commission may, by means of implementing acts, further specifies measures & procedures for these due diligence and security/personal data breach notification provisions. In this context however, the initiative of ENISA on security breach notifications (SBN) may make the adoption of the related implementing act under art.19.4 of eIDAS Regulation unnecessary. Building upon the experience on SBN gained while working on the implementation of article 13a of the e-communication Framework Directive, ENISA is currently developing technical guidelines to facilitate the implementation of article 19 of the eIDAS Regulation. Such guidelines will be developed in close cooperation with all stakeholders (in particular national supervisory bodies and TSPs) and focus on appropriate technical and operational solutions to comply with article 19 of the eIDAS Regulation. Once completed, these guidelines would be available to stakeholders for voluntary adoption, and be subject to regular revision (as it has been the case of these related to article 13a of the e-communication Framework Directive).

Furthermore it is recommended to the TSPs to prepare procedures to be used in case of and to support supervision of their SB according to article 17.3. This may be done in co-operation with the responsible SB.

### 2.2.2 Requirements common to all QTSPs

Requirements common to all QTSPs are these requirements applicable to all TSPs (see section 2.2.1) together with the following requirements laid down in Art.24.2 of the eIDAS Regulation:

(a) Inform SB of any change in QTS provisioning and of intention to cease (new provision compared to that of Directive 1999/93/EC);
(b) Requirements on staff (similar to Annex II.e of Directive 1999/93/EC);
(c) Sufficient financial resources and/or liability insurance, in accordance with national law (similar to Annex II.h of Directive 1999/93/EC);
(d) Consumer information on terms and conditions, incl. limitations on use (similar to Annex.II.k);
(e) use trustworthy systems and products (similar to Annex.II.f + reliability of supported processes);
(f) use trustworthy systems to store (personal) data (new provision compared to that of Directive 1999/93/EC);
(g) take appropriate measures against forgery and theft of data (generalisation of Annex.II.g);
(h) Record and keep accessible activities related data, issued and received (generalisation of Annex.II.i), even after cessation (new);
(i) Up-to-date termination plan (agreed with SB) to ensure continuity of service (new provision compared to that of Directive 1999/93/EC);
(j) ensure lawful processing of personal data in accordance with Directive 95/46/EC (similar to Art.8 of Directive 1999/93/EC).

(Art.24.5) The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products, which comply with the requirements

- under Art.24.2.(e) - trustworthy systems and products
- under Art.24.2.(f) - trustworthy systems for data storage

Compliance with the requirements laid down in these articles Art.24.2.(e) and (f) shall be presumed where trustworthy systems and products meet these standards.

### 2.2.3 Requirements for QTSPs issuing qualified certificates

Requirements for QTSPs issuing qualified certificates are these requirements applicable to all TSPs, these requirements common to all QTSPs, and the following requirements laid down in:

- Art.24.1:

1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

a) by the physical presence of the natural person or of an authorised representative of the legal person; or

b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or

c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

- Art.24.2.(k) on establishing and keeping updated a certificate database;
- Art.24.3: If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.
- Art24.4: With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

OCSP does not necessarily provide more up to date information than a CRL. In practice, the two last requirements do not require the implementation of OCSP based certificate validity status information services. It would be advised to provide both types of such services for efficiency reasons, provided adequate profiling of the corresponding standards are specified. Anticipating the termination, expected or unexpected, may also have a considerable influence in selecting implementation of both types of services.

- Content of qualified certificates:
  - As per Annex I for qualified certificate for electronic signatures (Art.28.1)
  - As per Annex III for qualified certificate for electronic seals (Art.38.1)
  - As per Annex IV for qualified certificate for website authentication (Art.45.1)
- May include non-mandatory attributes, not affecting interoperability or recognition (Art.28.3, Art. 38.3, also applying to QC for WSA when special case of QC for electronic seals – Recital (65))
- Revocation of qualified certificates is definitive (Art.28.4, Art. 38.4, also applying to QC for WSA when special case of QC for electronic seals – Recital (65))

- Temporary suspension of QC for electronic seals and for electronic signatures may be specified on a national basis (Art.28.5, Art.38.5)
    - With obliteration?
    - Without obliteration?

In case the QTSP issues qualified electronic signature creation devices (QSCD), the following requirements apply:

- Characteristics of QSCD:
    - As per Annex II for qualified electronic signature creation devices (Art.29.1)
- Certification of the QSCD by appropriate bodies (Art.30.1) whereas the certification is based upon an security evaluation process according to Art. 30.3, and where the European Commission shall, by means of implementing acts, establish list of standards for the security assessment of information technology products.

Instead of issuing a new QSCD, the QTSP might want to certify public keys originating from QSCD already in the hand of a user. In such a case the QTSP has to ensure by appropriate means that the key is truly originating from a QSCD, before issuing the certificate (Art.3(12)).

With regard to the requirements of art. 24.1.(b), on issuing remotely a qualified certificate, the identity verification process is in fact more strict than identity proofing process at the issuance of electronic means of identification of the level of assurance 'high'[17]. Therefore to be compliant with art. 24.1.(b) it is (explicitly) mandatory to use electronic identification means for which physical presence was performed at issuance, regardless it represents level 'substantial' or 'high'.

### 2.2.4 Requirements for QTSPs providing qualified validation services for QESig / QESeal

Requirements for QTSPs providing validation services for QESig / QESeal[18] (referring to Art.33 / Art.40) are these requirements applicable to all TSPs, these requirements common to all QTSPs, and the following requirements laid down in:

- Art.33.1(a) with regard to the validation process to be provided in compliance with Art.32.1. (alinea (a) to (h)).
- Art.33.1(b) for the provision of the validation result in an automated manner that needs:
    - to provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues (in conjunction of Art.32.2);
    - to be reliable and efficient; and
    - to bear the advanced electronic signature or advanced electronic seal of the QTSP providing the qualified validation service.

[17] According to CIR (EU) 2015/1502 on setting out the minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p7-20.

[18] Art.40 for validation of QESeals refers back to Art. 32 and 33

As foreseen in Art.32.3, the Commission may, by means of implementing acts, establish reference numbers of standards for the validation of qualified electronic signatures and as foreseen in Art.33.2 the Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service as required by Art.33.1.

As the relative vagueness of provisions stipulated in Art.32 on the requirements for the validation of qualified electronic signatures may lead to varying implementation measures , adopting such implementing acts would be recommended.

### 2.2.5 Requirements for QTSPs providing preservation service for QESig/ QESeal

Requirements for QTSPs providing preservation services for QESig / QESeal[19] (referring to (Art.34 / Art.40) are these requirements applicable to all TSPs, these requirements common to all QTSPs, and the following requirements laid down in:

- Art.34.1 for making use of procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

Where, according to Art.34.2 the Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures and seals.

### 2.2.6 Requirements for QTSPs issuing qualified electronic time stamps

Requirements for QTSPs issuing qualified electronic time stamps (referring to Art.42) are these requirements applicable to all TSPs, these requirements common to all QTSPs, and the following requirements laid down in:

- Art.42.1 for qualified electronic time stamps:
    - to bind the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
    - to be based on an accurate time source linked to Coordinated Universal Time; and
    - to be signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method

As of Art.42.2 the Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources.

### 2.2.7 Requirements for QTSPs providing qualified electronic registered delivery service

Requirements for QTSPs providing qualified electronic registered delivery service (referring to Art.44) are these requirements applicable to all TSPs, these requirements common to all QTSPs, and the following requirements laid down in:

- Art.44.1 on the definition of the qualified electronic registered delivery service which may be offered by one or more QTSP.

[19] Art.40 for preservation of QSeals refers back to Art. 34

As of Art.44.2 the Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data.

## 2.3 Technical requirements for signatures, seals, certificates and their validation

In this context, Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced electronic seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market has been published in the Official Journal of the EU[20].

The eIDAS Regulation specifies other electronic signatures, electronic seals and related certificates requirements set directly in the annexes to the regulation; other requirements are stipulated as follows, by establishing reference numbers of standards for:[21]

- Art.24(5) - trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of Art.24.
- Art.27(4) - advanced electronic signatures in public services.
- Art.28(6) - qualified certificates for electronic signatures.
- Art.29(2) - qualified electronic signature creation devices.
- Art.32(3) - the validation of qualified electronic signatures.
- Art.34(2) - qualified preservation service for qualified electronic signatures
- Art.37(4) - advanced electronic seals in public services.
- Art.38(6) - qualified certificates for electronic seals.
- Art.39(1) - qualified electronic seal creation devices.
- Art.40 - the validation of qualified electronic seals.
- Art.42(2) - the binding of date and time to data and for accurate time sources in the context of qualified electronic time stamps (Art.42(1)).
- Art.45(2) - qualified certificates for website authentication.

The following direct requirements are specified with ANNEX I to IV to the eIDAS-Regulation:

- ANNEX I – Requirements for qualified certificates for electronic signatures:
  Specifies the minimum data contents of the certificate and requires, that the certificate supporting advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider must be available free of charge, ANNEX I (h),
- ANNEX II – Requirements for qualified electronic signature creation devices:
  Specifies minimum requirements to be met by a QSCD and requires that electronic signature creation data may only be managed on behalf of the signatory by a qualified trust service provider. In addition, requirements for the duplication of a signatory's electronic signature creation data are specified ANNEX II, 4.
- ANNEX III – Requirements for qualified certificates for electronic seals:
  Specifies the minimum data contents of the certificate and requires, that the certificate supporting advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider must be available free of charge, ANNEX III (h),

[20] OJ L 235, 9.9.2015, p37-41.
[21] The approach of the Commission in this regard is expressed in section 2.1.3.

- ANNEX IV – Requirements for qualified certificates for website authentication:
  Specifies the minimum data contents of the certificate and requires, that the certificate supporting advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider must be available free of charge, ANNEX IV (i).

# 3. Inventory of standards

## 3.1 Overview

In late 2009, the European Commission issued Standardisation Mandate 460[22] to CEN, CENELEC and ETSI to update the existing eSignature standardisation deliverables in view of establishing a fully rationalised framework, which would solve the issues raised in actual use of eSignatures in the EU. These issues were about, notably, the mutual recognition and cross-border interoperability of eSignatures, the multiplicity of standardization documents and the lack of usage guidelines, the difficulty of access, the lack of business orientation, the numerous options and latitude for divergent interpretations and different technical implementations.

Other standardisation bodies such as ISO, IETF, OASIS, UPU, ITU and national accreditation or supervisory bodies are also defining "standards" or "local rules" that apply to Trust Services and Trust Service Provider.

The main objective of this section is to have an overview of involved parties and existing standards at the time of writing. Annex A of this document provides a table of all identified standards.

## 3.2 ETSI/CEN framework for standardization of signatures

One of the first tasks in the context of Mandate 460 was to establish a rationalized framework for signature standardization to overcome the reported issues within the context of the eSignature Directive, taking into account possible revisions to this Directive. In August 2014, the European Commission published Regulation 910/2014/EU aiming to repeal that Directive as from 1/7/2016. That Regulation extends the scope of the Directive with additional services for identification and authentication alongside an extended range of signature related trust services and defines additional forms of qualified certificates.

A work programme has been established and will be maintained to address any elements identified as missing in the framework for standardization of signatures. All documents of the framework intend to cover digital signatures supported by PKI and public key certificates, and aim to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from the EU legislation. Digital signatures as data appended to, or being a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, can support, when appropriately supported themselves by relevant trust services, implementation of electronic signatures and electronic seals as they are defined in the applicable European legislation.

ETSI technical report TR 119 000 describes the general structure for ETSI/CEN digital signature standardization outlining existing and potential standards for such signatures, hereafter referred to as the ETSI/CEN framework for standardization of signatures. This framework identifies six areas of standardization with a list of existing and potential future standards in each area:

1. **Signature creation and validation:** focusing on standards related to the creation and validation of digital signatures, covering:
    - i) the policy and security requirements for signature creation applications and signature validation applications;
    - ii) the expression of rules and procedures to be followed at creation, verification and for preservation of digital signatures for long term;

[22] http://www.etsi.org/images/files/ECMandates/m460.pdf

iii) signature format, packaging of signatures and signed documents; and
iv) protection profiles, according to Common Criteria for signature creation/verification applications.

2. **Signature creation and other related devices:** focusing on standards related to secure signature creation devices as defined in Directive 1999/93/EC, on signature creation devices used by trust service providers as well as other types of devices supporting digital signatures and related services such as authentication.
3. **Cryptographic suites:** covering standardisation aspects related to the use of signature cryptographic suites, i.e. the suite of digital signature related algorithms including key generation algorithms, signing algorithms with parameters and padding method, verification algorithms, and hash functions.
4. **Trust service providers supporting digital signatures and related services:** covering TSPs issuing qualified certificates, TSPs issuing public key certificates other than qualified certificates, including web server certificates, time-stamping services providers, TSPs offering signature validation services, TSPs offering remote signature creation services (also called signing servers).
5. **Trust application service providers:** covering trust service providers offering value added services applying digital signatures and that relies on the generation/validation of electronic signatures in normal operation. This includes namely registered mail and other e-delivery services, as well as data preservation (long term archiving) services.
6. **Trust service status (list) provider:** covering standards related to the provision of trusted lists as defined by CD 2009/767/EC as amended and by CD 2015/1505/EU.

Up to five types of documents may be associated with each area:

- Guidance documents
- Policy and Security Requirements
- Technical Specifications
- Conformance Assessment Guidance
- Compliance and Interoperability Testing

The next subsections describe shortly these different areas and their constitutive documents. The descriptive text regarding each listed document is minimised as an extended version can be found in TR 119 000. An overview of the effective availability of the documents is also provided.

The total number of expected documents for the whole framework is 59 multipart documents and more than a hundred (107) when counting each part separately. This also explains the need for guidance documents from different sources of interest in eSignatures (business, security, etc.). The bulk of these are technical specification documents. Thanks to ETSI Plug-Test programs, the “Compliance and Interoperability Testing” documents for electronic signatures/seals are also available.

### 3.2.1 Introductory documents

An additional area (Area 0) is grouping TR 119 000, the document presenting the general structure of the CEN/ETSI framework for standardization of signatures, as well as studies and other introductory deliverables related to the structure of the framework.

This general purpose Area 0 includes the documents listed in Table 1 below. This table and the other tables listing the existing document of the ETSI/CEN framework indicate the new numbering of each standard as it appears in the framework, its title, the type of document, the number(s) of the document(s) it replaces, and the effective or expected publication date (for information and subject to changes).

| | | | | | | Introductory documents of the framework for signature standardisation | Replaces | Expected publication |
|---|---|---|---|---|---|---|---|---|
| | | | | Sub-areas | | | | |
| | | | | | Guidance | | | |
| TR | 1 | 19 | 0 | 0 | 0 | The framework for standardisation of signatures: overview | SR 001604 v1.1.1 | published |
| TR | 4 | 19 | 0 | 1 | 0 | The framework for standardisation of signatures: Extended structure including electronic identification and authentication | (new) | Feb. 2016 (hand over to CEN) |
| SR | 0 | 19 | 0 | 2 | 0 | The framework for standardisation of signatures: Standards for AdES digital signatures in mobile environments | (new) | Nov. 2015 |
| TR | 4 | 19 | 0 | 3 | 0 | The framework for standardisation of signatures: Best practices for SMEs | CWA 14365 | Dec. 2015 |
| TR | 4 | 19 | 0 | 4 | 0 | The framework for standardisation of signatures: Guidelines for citizens | CWA 14365 | Dec. 2015 |
| SR | 0 | 19 | 0 | 5 | 0 | Rationalised framework of standards for electronic registered delivery applying electronic signatures | (new) | published |
| | | | | | Policies | | | |
| TR | 1 | 19 | 0 | 0 | 1 | The framework for standardisation of signatures: Definitions and abbreviations | (new) | published |

**Table 1**: Introductory documents of the framework for signature standardization (source ETSI TR 119 000)

No draft is available yet for TR 419 010 that aims to propose an extension of the signature standardisation framework to cover electronic identification, electronic authentication and signatures. Its delivery has been delayed in order to be aligned with Regulation 2014/910/EU and in particular with its secondary legislation on electronic identification means, i.e. CID 2015/1502/EU[23].

The special report SR 019 020 is planned for publication in November 2015. This document recommends:

- The provision of specifications on the framework for standards (including potential architectures and relevant scenarios) required for the creation of advanced AdES in distributed environments (e.g. via new TS 119 152). This is expected to leverage on OASIS DSS and on MCOMM specifications.
- The provision of specifications on the policy requirements for TSPs providing signature generation services (e.g. via new EN 319 431). The operation of the TSP providing such signature generation services needs to be trusted to ensure that the keys held on the server are not open to hostile attack. Support for split keys (e.g. models in use in Poland) is for further study. This document will reference EN 319 401 for general policy requirements on TSPs.
- The provision of specifications to address protocol requirements for use of TSPs to support both local and remote signing (e.g. via new EN 319 432). For local signing both ETSI M-COMM and OASIS DSS are applicable. M-COMM already has a significant installed base and can take advantage of particular features of mobile environment. OASIS DSS has the advantage of being generally applicable to both mobile and of computing environments. For remote signing, OASIS DSS is directly applicable.
- The provision of specifications on the policy requirements for TSPs providing signature validation services (e.g. via new EN 319 441). The operation of the TSP providing such signature validation services needs to be trusted to ensure that the service is not open to hostile attack. This document will reference EN 319 401 for general policy requirements on TSPs.
- The provision of specifications (e.g. via new EN 319 442) to address protocol, formats and procedures requirements for use of signature validation trust service (providers). OASIS DSS is directly applicable although other services may be used to support signature validation (e.g. W3C XML Key Management Specifications, DVCS protocols, SCVP protocols).

[23] CIR (EU) 2015/1502 on setting out the minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. OJ L 235, 9.9.2015, p7-20.

The production of TR 419 030 (Best practices for SMEs) and TR 419 040 (Guidelines for citizens) has been started but no drafts are available yet. These documents aim to provide best practices in the usage of e-signatures within the context of SMEs and consumers. They should answer questions in relation to the use and benefits (ROI) of eSignatures to SMEs / consumers ecosystems. These guides are not meant to be as technically oriented as ETSI documents.

TR 119 001 provides all definitions & abbreviations used in documents of the framework and serve as reference.

SR 019 050 provided a proposal for a rationalized framework of standards for electronic registered delivery services, as defined by the eIDAS Regulation 20914/910/EU; the current structure of the framework documents covering these services is the one published in TR 119 000 (see section 3.2.§ below).

### 3.2.2 Signature Creation and Validation

The standardisation documents for signature creation and validation are summarised in table 2 with further details provided in TR 119 000.

With regards to the validation of digital signatures, it should be noted that procedures for signature validation were previously specified in TS 102 853 - Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies updated in November 2014 to reflect corrections in processing identification of the signer's certificate in XAdES, CAdES and PAdES. EN 319 102 "Procedures for Signature Creation and Validation; Part 1: Signature validation procedures", under EN approval, will further update TS 102 853, in particular to meet the requirements of Regulation 2014/910/EU. It should be noted however that the standardisation work on specifications for a signature validation report (EN 319 102 Part2) has been delayed to the next specialist task force activities waiting for funding from the European Commission.

Significant efforts have been made to standardise requirements for signature creation and/or validation applications. This encompasses specifications for policy and security requirements (TS 119 101), protection profiles (EN 419 111 series) and relevant conformity assessment guidance (TS 119 103). This is believed to be an important contribution to the enhancement of the quality and security of such applications. Appropriate coordination between CEN and ETSI shall be required to properly finalise such efforts. TS 119 101 and TS 119 103 are not yet published while all five parts of the Protection Profiles (PPs) for signature creation and verification application (prCEN/EN 419 111) have been published as CEN enquiry status in 2013-03 hence in the context of Directive 1999/93/EC. These latter PPs may need to be updated for alignment with eIDAS Regulation, upcoming ETSI documents (e.g. TS 119 101) and furthermore Part 2 and Part 4 still need to be evaluated and certified. Evaluation and certification were delayed due to the need to find a new editor.

| Signature creation and validation | | | | | | | | Replaces | Expected publication |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sub-areas | | | | |
| | | | | | Guidance | | | | |
| TR | 1 | 19 | 1 | 0 | 0 | Business driven guidance for implementing digital signature creation and validation | | (new)<br>TR 102 047 | Feb. 2016 |
| | | | | | Policy & Security Requirements | | | | |
| TS | 1 | 19 | 1 | 0 | 1 | Security requirements for signature creation applications and signature validation applications | | (new) | Nov. 2015 |
| EN | 4 | 19 | 1 | 1 | 1 | Protection profiles for signature creation and validation application<br>- Part 1: Introduction to the European Norm<br>- Part 2: Signature creation application - Core PP<br>- Part 3: Signature creation application - Possible Extensions<br>- Part 4: Signature verification application - Core PP<br>- Part 5: Signature verification application - Possible Extensions | | CWA/prEN 14170 | All parts published & to be updated: undefined<br>Part 2 & 4 to be evaluated |
| | | | | | Technical Specifications | | | | |
| EN | 3 | 19 | 1 | 0 | 2 | Procedures for creation and validation of AdES digital signatures<br>- Part 1: Creation and validation<br>- Part 2: Validation report | | TS 102 853,<br>CWA 14170,<br>CWA 14171 | Part 1:<br>- TS: published<br>- EN: Apr. 2016<br>Part 2: undefined |
| EN | 3 | 19 | 1 | 2 | 2 | CAdES digital signatures<br>- Part 1: Building blocks and CAdES baseline signatures<br>- Part 2: Extended CAdES signatures | | TS 101 733,<br>TS 103 173,<br>TS 102 734 | Parts 1 & 2:<br>- TS: published<br>- EN: Apr. 2016 |
| EN | 3 | 19 | 1 | 3 | 2 | XAdES digital signatures<br>- Part 1: Building blocks and XAdES baseline signatures<br>- Part 2: Extended XAdES signatures | | TS 101 903,<br>TS 103 171,<br>TS 102 904 | Parts 1 & 2:<br>- TS: published<br>- EN: Apr. 2017 |
| EN | 3 | 19 | 1 | 4 | 2 | PAdES digital signatures<br>- Part 1: Building blocks and PAdES baseline signatures<br>- Part 2: Additional PAdES signatures profiles<br>- Part 3: Visual representations of digital signatures | | - TS 102 778-1<br>- TS 103 172<br>- TS 102 778-2/5<br>- TS 102 778-6 | Parts 1 & 2:<br>- TS: published<br>- EN: Apr. 2016<br>(Part 3: delayed) |
| TS | 1 | 19 | 1 | 5 | 2 | Architecture for AdES digital signatures in distributed environments | | (new) | Undefined |
| EN | 3 | 19 | 1 | 6 | 2 | Associated Signature Containers (ASiC)<br>- Part 1: Building blocks and ASiC baseline containers<br>- Part 2: Additional ASiC containers | | TS 102 918,<br>TS 103 174 | Parts 1 & 2:<br>- TS: Sep. 2015<br>- EN: July 2016 |
| TS | 1 | 19 | 1 | 7 | 2 | Signature policies<br>- Part 1: Building blocks and table of contents for human readable signature policy documents<br>- Part 2: XML format for signature policies<br>- Part 3: ASN.1 format for signature policies<br>- Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists | | - TR 102 041 / 045<br>- TR 102 038<br>- TR 102 272 | - Part1: published<br>- Other parts: undefined |
| | | | | | Conformity Assessment | | | | |
| TS | 4 | 19 | 1 | 0 | 3 | Conformity assessment for signature creation & validation (applications & procedures) | | (new)<br>(CWA 14172-4 ?) | Feb. 2016<br>(hand over to CEN) |
| | | | | | Testing Conformance & Interoperability | | | | |
| TS | 1 | 19 | 1 | 2 | 4 | CAdES Testing conformance & interoperability | | (new) | April 2016 |
| TS | 1 | 19 | 1 | 3 | 4 | XAdES Testing conformance & interoperability | | (new) | April 2016 |
| TS | 1 | 19 | 1 | 4 | 4 | PAdES Testing conformance & interoperability | | (new) | April 2016 |
| TS | 1 | 19 | 1 | 5 | 4 | Testing conformance & interoperability of AdES in mobile environments | | (new) | April 2017 |
| TS | 1 | 19 | 1 | 6 | 4 | ASiC Testing conformance & interoperability | | (new) | April 2016 |

**Table 2**: Standards for signature creation and validation (source ETSI TR 119 000)

Increased rationalisation and simplification with regards to the specifications of XAdES, CAdES and PAdES signature formats have been implemented, further simplifying and promoting the baseline profiles as the primary specifications while marginalising any additional optional extensions. The same improvements have been done for associated signature containers (ASiC) specifications. All corresponding documents are under EN approval process and are expected to be adopted and published early 2016. It is expected that these specifications could be candidate for being referenced by implementing acts foreseen in Art.27.5 and Art 37.5 of the eIDAS Regulation, when amending CID 2015/1506/EU.

Facilities for testing conformance and interoperability of signatures generated by implementers' signature creation applications are provided under the form of ETSI Plugtests™ and testers. The remote Plugtests™ interoperability events aim to conduct conformance and interoperability testing on X/C/PAdES digital signatures and ASiC containers and provide full test coverage of the specifications including testing signatures evolution, simulating real life situations. The tests include creation, augmentation and verification of signature and are executed according to current version and new draft of applicable standards. They are organised three or four times a year. Outside these events, ETSI is also designing and developing a set of conformance testing tools. ETSI TS 119 1x4 documents aim to help implementers and accelerate the development of C/X/PAdES-ASiC signature creation and validation applications by defining test suites complete sets of test assertions for testing technical conformance of signatures against the relevant technical specifications. The test results can also be used in conformity assessment for signature creation and validation applications (ETSI EN 319 103) with policies requiring conformity to specific ETSI signature formats and procedures.

With regards to signature policies, published part 1 of TS 119 172 lays down the concepts and the specifications for the table of contents of a human readable signature policy while parts 2 & 3 specifying the derived machine processable formats (XML and ASN.1) have been postponed to a future phase of the standardisation work programme. TS 119 172 Part 4 will be dedicated to specify a signature validation policy as aligned to Art.32 of Regulation (EU) 910/2014, i.e. rules for validating digital signatures using EU MS trusted lists in order to indicate whether they are advanced electronic signatures/seals, advanced electronic signatures/seals supported by a qualified certificate or qualified electronic signature/seal in accordance with the applicable EU legislation.

### 3.2.3 Signature creation and other related devices

The standardisation documents for signature creation and other related devices are summarised in table 3 with further details available in TR 119 000.

| | | | | | | | Signature creation and other related devices | Replaces | Expected publication |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Sub-areas | | |
| | | | | | | | Guidance | | |
| TR | 4 | 19 | 2 | 0 | | 0 | Business driven guidance for signature creation and other related devices | (new) | February 2016 |
| | | | | | | | Policy & Security Requirements | | |
| EN | 4 | 19 | 2 | 1 | | 1 | Protection profiles for secure signature creation device<br>- Part 1: Overview<br>- Part 2: Device with key generation<br>- Part 3: Device with key import<br>- Part 4: Extension for device with key generation and trusted communication with certificate generation application<br>- Part 5: Extension for device with key generation and trusted communication with signature creation application<br>- Part 6: Extension for device with key import and trusted communication with signature creation application | <br>- (new part)<br>- prTS 14169-2<br>- prTS 14169-3<br>- prTS 14169-4<br><br>- prEN 14169-5<br><br>- (new part) | published |
| EN | 4 | 19 | 2 | 2 | | 1 | Protection Profiles for TSP cryptographic modules<br>- Part 1: Overview<br>- Part 2: Cryptographic Module for CSP signing operations with backup – Protection Profile (CMCSOB-PP)<br>- Part 3: Cryptographic module for CSP key generation services – Protection Profile (CMCKG-PP)<br>- Part 4: Cryptographic module for CSP signing operations without backup – Protection Profile (CMCSOPP)<br>- Part 5: Cryptographic module for trust services | <br>- (new part)<br>- prTS 14167-2<br>- prTS 14167-3<br>- prTS 14167-4<br>- (new part) | <br>By end 2015<br>By end 2015<br>By end 2015<br>By end 2015<br>In 2016 |
| EN | 4 | 19 | 2 | 3 | | 1 | Protection profile for trustworthy systems supporting time stamping | (new) | In 2016 |
| EN | 4 | 19 | 2 | 4 | | 1 | Security requirements for trustworthy systems supporting server signing<br>- Part 1: Security requirements<br>- Part 2: Protection profile for trustworthy signature creation module (PP-TSCM)<br>- Part 3: Protection profile for signature activation data management and signature activation protocol (PPSAD+SAP) | CWA 14167-5 | <br>- TS published (EN: 2015)<br>- undefined<br>- undefined |
| EN | 4 | 19 | 2 | 5 | | 1 | Security requirements for device for authentication<br>- Part 1: Protection profile for core functionality<br>- Part 2: Protection profile for extension for trusted channel to certificate generation application<br>- Part 3: Additional functionality for security targets | EN 16248 (PP-DAUTH) | published |
| EN | 4 | 19 | 2 | 6 | | 1 | Security requirements for trustworthy systems managing certificates for electronic signatures | prTS 14167-1 | published |
| | | | | | | | Technical Specifications | | |
| EN | 4 | 19 | 2 | 1 | | 2 | Application interfaces for secure elements used as qualified electronic signature (seal-) creation devices<br>- Part 1: Introduction<br>- Part 2: Basic services<br>- Part 3: Device authentication<br>- Part 4: Privacy specific protocols<br>- Part 5: Trusted eServices | EN 14890 | Parts 1 & 2: published<br>Other parts: by end 2015 |
| | | | | | | | Conformity Assessment | | |
| | | | | | | | *no requirement identified* | | |
| | | | | | | | Testing Conformance & Interoperability | | |
| - | | - | - | - | | - | *no requirement identified* | | |

**Table 3**: Standards for signature creation and other related devices (source TR 119 000)

Three new protection profiles (PP) are being developed for server signing:

- Cryptographic modules for Trust Services
  - As new part 5 of EN 419 221 series
  - For TSP operation in secure environment
  - Multipurpose crypto module: protection of signatories keys, authentication mechanisms
- Server signing PPs (as 2 new parts of EN 419 241)
  - Trustworthy Signature Creation Module (TSCM) for TSP

- Sole Control Component (SCC) for Signatory

TSCM and SCC work together to allow only the signatory to securely use his/her private signature key (assurance level substantial or high for authentication). Solutions without SCC might exist that allow the signatory to reliably protect his/her private signature key (under discussion).

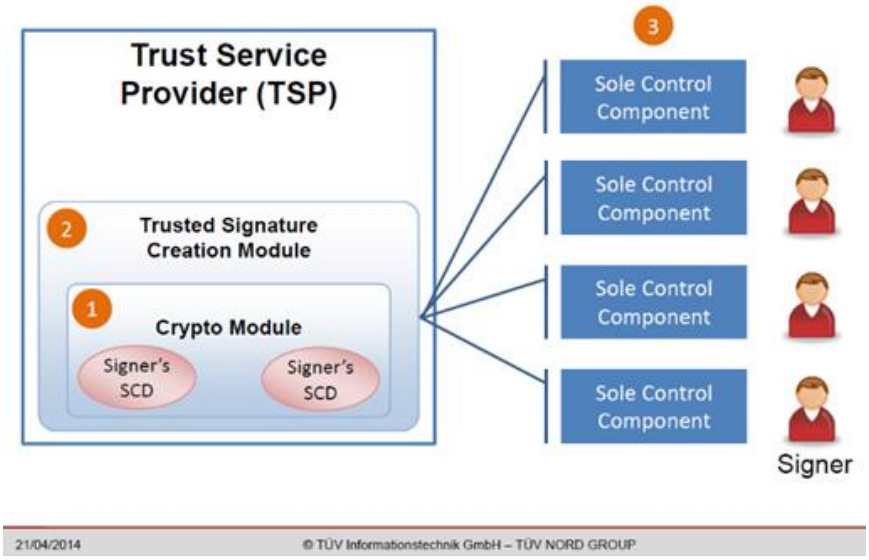



**Figure 3**: Protection Profiles for server signing

prCEN/EN 419 211 (was prEN14169) – Protection Profiles (PP's) for Secure Signature Creation Devices (SSCD): All six parts have been published.

prCEN/EN 419 221 PP's for TSP cryptographic modules: Directive 1999/93/EC oriented PP's corresponding to part 2, part 3 and part 4 have been certified. Part 5 PP for cryptographic modules for TSPs, aimed at being aligned with eIDAS Regulation, supporting electronic signing and sealing, remote server signing and authentication is under formal evaluation and review.

prCEN/EN 419 231 PP for trustworthy systems supporting time stamping is under formal evaluation and review.

prCEN/EN 419 241 security requirements and PP's for trustworthy systems supporting server signing: Part 1 (security requirements) has been published as TS at the beginning of 2014. Conversion to EN is undergoing. Draft is currently discussed, next draft is expected beginning of December for WG17 review. A proposed scope for the PP(s) is still under discussion in WG17, with several drafts proposed by editors.

prCEN/EN 419 251 (was PP-DAUTH) – Security requirements for device for authentication: all 3 parts were published.

prCEN/TS 419 261 (was prTS 419 221-1, was prTS 14167-1) - Security requirements for Trustworthy Systems (incl. Managing Certificates for Electronic Signatures) was published early 2015.

EN 419 212 - Application Interfaces for Secure Signature Creation Devices:

- Part 1 (Introduction) is an introduction to the multi-part document for the application interface and the behaviour of the SSCD in the context of identification, authentication and electronic sig-

nature services. This part provides a tutorial and "how-to" use guide for the following parts of the standard.

- Part 2 (Basic services for electronic signatures) specifies mandatory mechanisms for smart cards and other secure elements to be used as secure signature creation devices covering among other signature creation, user verification, device authentication, and establishment of a secure channel. The specified mechanisms are suitable for other purposes like services in the context of IAS. The group is currently working on the integration of eSeal. It is not clear what are the constraints regarding seal versus signature (where depending on the environment, a device authentication and a secure channel must be established).

- Part 3 (Device authentication) specifies device authentication to be used for SSCDs in various contexts and includes device authentication protocols, data structures, CV-certificates and key management. The device authentication protocols shall apply to sole-control signature as mandated by Directive 1999/93/EC and as mandated by Regulation (EU) No 910/2014.

- Part 4 (Privacy) specifies access to e-services with privacy-oriented protocols. The group is working on the integration of eIDAS token specification.

- Part 5 (Additional services in the context of electronic services) contains Identification, Authentication and Digital Signature (IAS) services in addition to the SSCD mechanisms already described in Part 1 to enable interoperability and usage for IAS services on a national or European level. It also specifies additional mechanisms like key decipherment, Client/Server authentication and identity management.

### 3.2.4 Cryptographic suites

The standardisation documents for cryptographic suites are summarised in table 4 with further details in TR 119 000.

| Cryptographic suites | | | | | | | Replaces | Expected publication |
|---|---|---|---|---|---|---|---|---|
| | | | | | Sub-areas | | | |
| | | | | | Guidance | | | |
| TR | 1 | 19 | 3 | 0 | 0 | Business guidance on cryptographic suites | (new) | published |
| | | | | | Technical Specifications | | | |
| TS | 1 | 19 | 3 | 1 | 2 | Cryptographic suites | TS 102 176-1 | published |
| | | | | | Testing Conformance & Interoperability | | | |
| - | | - | - | - | - | *no requirement identified* | | |

**Table 4**: Standards for cryptographic suites (source TR 119 000)

An updated version of TS 102 176-1 (known as the “Algo paper”) has been published as TS 119 312 v1.1.1 in November 2014.

ETSI TR 119 300 and ETSI TS 119 312 are providing guidance on selection of cryptographic suites with particular emphasis on security. ETSI TS 119 312 identifies a range of different cryptographic suites that can be used corresponding to the appropriate level of security, which meets the security needs identified during the system design; there is no normative requirement on selection among the alternatives but for all alternatives, normative requirements apply to ensure security and interoperability. It is based on various security recommendations given

by other standardization bodies, national security agencies (including but not limited to France[24] and Germany[25]) and supervisory authorities of the Member States. ETSI 119 300 explains the concept of security parameters that helps to choose a proper cryptographic suite for digital signature creation. It also gives an overview how to analyse the business needs on the use of standards for cryptographic suites (in particular for digital signature creation algorithms) and how to select a system that satisfies these needs.

### 3.2.5 TSPs supporting digital signatures and related services

The standardisation documents for TSP supporting digital signatures and related services are summarised in table 5 with further details provided in TR 119 000.

| TSPs supporting digital signatures and related services | | | | | | | | Replaces | Expected publication |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sub-areas | | | | |
| | | | | | Guidance | | | | |
| TR | 1 | 19 | 4 | 0 | 0 | | Business driven guidance for TSPs supporting digital signatures | (new) | Published |
| | | | | | Policy & Security Requirements | | | | |
| EN | 3 | 19 | 4 | 0 | 1 | | General policy requirements for trust service providers | Replacing generic parts of TS 101 456, TS 102 042, (TR 102 040), TS | - TS: July 2015<br>- EN: March 2016 |
| EN | 3 | 19 | 4 | 1 | 1 | | Policy and security requirements for trust service providers issuing certificates<br>- Part 1: General requirements<br>- Part 2: Requirements for TSP issuing EU qualified certificates<br>- Part 3: *To be made historical*<br>- Part 4: Requirements for TSP issuing code signing certificates | - TS 102 042 (EV & BR), EN 319 411-3<br>- TS 101 456 (& TR 102 458), EN 319 411-3<br>- historical<br>- (new) | - TS: July 2015<br>- EN: March 2016<br>- historical<br>- undefined |
| EN | 3 | 19 | 4 | 2 | 1 | | Policy & security requirements for trust service providers issuing time-stamps | TS 102 023 | - TS: July 2015<br>- EN: March 2016 |
| EN | 3 | 19 | 4 | 3 | 1 | | Policy and security requirements for trust service providers providing AdES digital signature generation services | (new) | Undefined |
| EN | 3 | 19 | 4 | 4 | 1 | | Policy and security requirements for trust service providers providing AdES digital signature validation services | (new) | Undefined |
| | | | | | Technical Specifications | | | | |
| EN | 3 | 19 | 4 | 1 | 2 | | Certificate profiles<br>- Part 1: Overview and common data structures<br>- Part 2: Certificate profile for certificates issued to natural persons<br>- Part 3: Certificate profile for certificates issued to legal persons<br>- Part 4: Certifcate profile for web site certificates issued to organisations<br>- Part 5: QCStatements | - (new part)<br>- TS 102 280 & TS 101 862<br>- (new part)<br>- (new part) | All parts:<br>- TS: July 2015<br>- EN: March 2016 |
| EN | 3 | 19 | 4 | 2 | 2 | | Time-stamping protocol and time-stamp profiles | TS 101 861 | - TS: July 2015<br>- EN: March 2016 |
| EN | 3 | 19 | 4 | 3 | 2 | | Protocol profiles for trust service providers providing AdES digital signature generation services | (new) | Undefined |
| EN | 3 | 19 | 4 | 4 | 2 | | Protocol profiles for trust service providers providing AdES digital signature validation services | (new) | Undefined |
| | | | | | Conformity Assessment | | | | |
| EN | 3 | 19 | 4 | 0 | 3 | | Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers | CWA 14172 (2&8), TS 119 403 | - TS: Nov. 2014<br>- EN: end 2015 |
| | | | | | Testing Conformance & Interoperability | | | | |
| - | - | - | - | - | - | | *no requirement identified for such a document* | | |

**Table 5**: Standards for TSPs supporting digital signatures and related services (source TR 119 000)

The above listed documents address four types of trust services provided by trust service providers and their corresponding qualified version:

[24] Agence nationale de la sécurité des systèmes d'information, Référentiel Général de Sécurité version 2.0, 2014-06.
[25] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Übersicht über geeignete Algorithmen, 2014-01

1. Provisioning of certificates,
2. Provisioning of electronic time-stamp,
3. Provisioning of signature generation services, and
4. Provisioning of signature validation services.

Besides the business driven guidance document (TR 119 400), the document entry points for each of the above types of trust service and trust service provider are respectively:

1. EN 319 411 document, respectively Part 1 for general requirements for TSPs issuing certificates and Part 2 for requirements for TSPs issuing qualified certificates;
2. EN 319 421 for the issuance of time-stamps,
3. EN 319 431 for the provisioning of signature generation services, and
4. EN 319 441 for the provisioning of signature validation services.

These documents are highlighted in dark pink in Figure 3 below, together with their interrelations with the other relevant documents of the standardisation area, i.e. indicating which document they require or conditionally require.

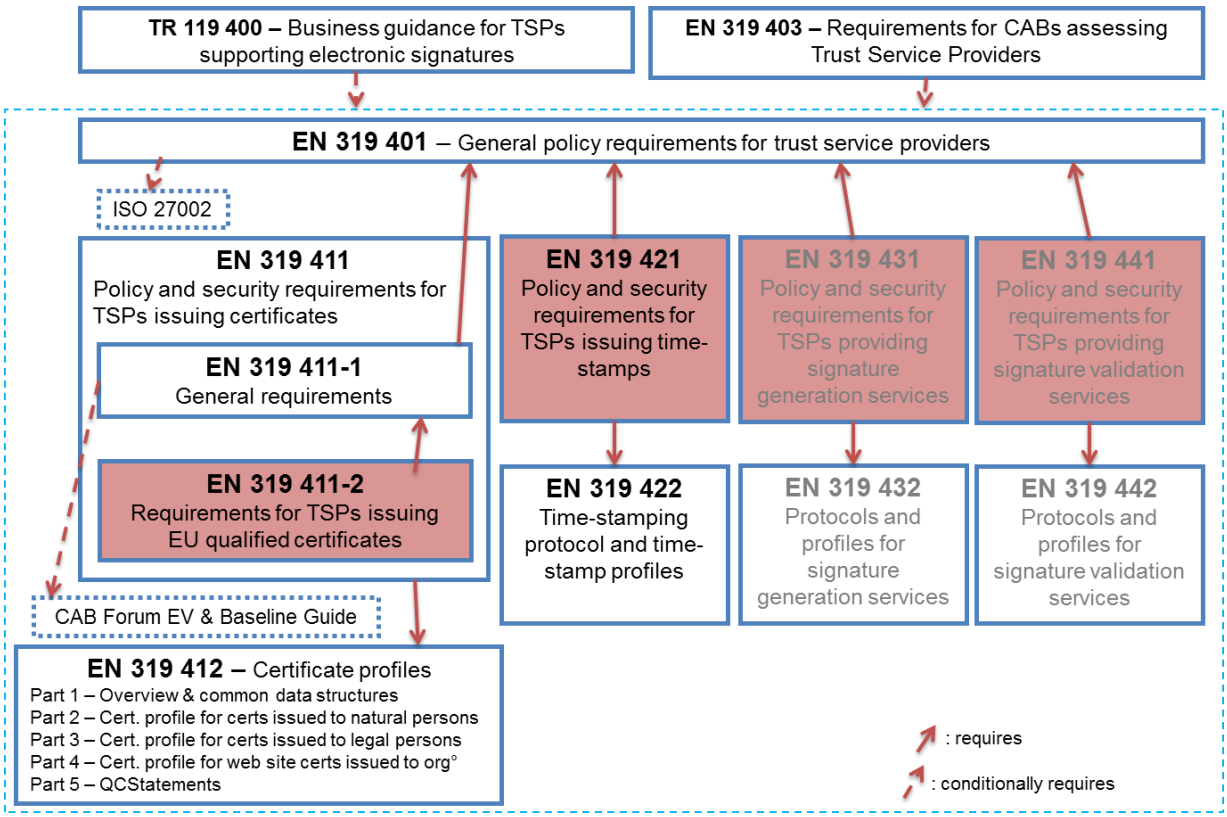



**Figure 3**: Overview the Area 4 documents and their interrelations

It should be noted that production of the documents directly related to the provisioning of signature generation and validation services have been postponed for future standardisation work and they will likely not be available, at least under the form of a European standard (EN) by 1/07/2016.

### 3.2.6 Trust application service providers

The documents for trust application service providers are summarised in table 6 with further details provided in TR 119 000.

| Trust application service providers | | | | | | | | Replaces | Expected publication |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Sub-areas | | | | | |
| | | | | | Guidance | | | | |
| TR | 1 | 19 | 5 | 0 | 0 | | Business driven guidance for trust application service providers | (new) | Undefined |
| SR | 0 | 19 | 5 | 1 | 0 | | Scoping study and framework for standardization of long term data preservation services, including preservation of/with digital signatures | (new) | Undefined |
| | | | | | Policy & Security Requirements | | | | |
| EN | 3 | 19 | 5 | 1 | 1 | | Policy & security requirements for trust service providers providing long term data preservation services, including preservation of/with digital signatures | TS 102 573, TR 102 572 | Undefined |
| EN | 3 | 19 | 5 | 2 | 1 | | Policy & security requirements for electronic registered delivery service providers | (new) | Undefined |
| EN | 3 | 19 | 5 | 3 | 1 | | Policy & security requirements for registered electronic mail (REM) service providers | TS 102 640 | Undefined |
| | | | | | Technical Specifications | | | | |
| EN | 3 | 19 | 5 | 1 | 2 | | Long term data preservation services, including preservation of/with digital signatures | | Undefined |
| EN | 3 | 19 | 5 | 2 | 2 | | Electronic registered delivery services:<br>- Part 1: Framework and architecture<br>- Part 2: Semantic contents<br>- Part 3: Formats<br>- Part 4: Bindings | (new) | Undefined |
| EN | 3 | 19 | 5 | 3 | 2 | | Registered electronic mail (REM) services:<br>- Part 1: Framework and architecture<br>- Part 2: Semantic contents<br>- Part 3: Formats<br>- Part 4: Interoperability profiles | TS 102 640 | Undefined |
| | | | | | Conformity Assessment | | | | |
| - | - | - | - | - | | | *no requirement identified for such a document - relying on TS 119 403 / EN 319 403* | | |
| | | | | | Testing Conformance & Interoperability | | | | |
| TS | 1 | 19 | 5 | 0 | 4 | | General requirements for technical conformance and interoperability testing for trust application service providers and the services they provide | | Undefined |
| TS | 1 | 19 | 5 | 2 | 4 | | Testing conformance and interoperability of electronic registered delivery services:<br>- Part 1: Testing conformance<br>- Part 2: Test suites for interoperability testing of electronic registered delivery service providers | TR 103 071 | Undefined |
| TS | 1 | 19 | 5 | 3 | 4 | | Testing conformance & interoperability of registered electronic mail services.<br>- Part 1: Testing conformance<br>- Part 2: Test suites for interoperability testing of providers using same format and transport protocols<br>- Part 3: Test suites for interoperability testing of providers using different format and transport protocols | | Undefined |

**Table 6**: Standards for trust application service providers

On the subject of trust application service providers (TASP) area, there are no well-established documents besides the existing TS 102 573 (“Policy requirements for trust service providers signing and/or storing data objects”) and the multipart TS 102 640 series (“Registered Electronic Mail (REM)”).

In September 2015, work has been started to address trust service consisting in preservation of (qualified) electronic signatures under the form of a study undertaken to evaluate the needs and scope for such standardisation work. The standardisation work on electronic registered delivery services will leverage on the existing multipart TS 102 640 series addressing standardisation of registered electronic mail (REM) and align these specifications to the requirements of Regulation (EU) No 910/2014 on electronic registered delivery services. Effective production of such REM specifications and more general specifications addressing all other types of electronic registered delivery services has not been planned yet and is likely not to finalised in 2016.

### 3.2.7 Trust service status lists providers

The documents for trust service status lists providers are summarised in table 7 with further details provided in TR 119 000.

| Trust service status lists providers | | | | | | | Replaces | Expected publication |
|---|---|---|---|---|---|---|---|---|
| | | | | Sub-areas | | | | |
| | | | | Guidance | | | | |
| TR | 1 | 19 | 6 | 0 | 0 | Business guidance for trust service status lists providers | new | published |
| | | | | Policy & Security Requirements | | | | |
| TS | 1 | 19 | 6 | 1 | 1 | Policy & security requirements for trusted lists providers | | Undefined |
| | | | | Technical Specifications | | | | |
| TS | 1 | 19 | 6 | 1 | 2 | Trusted lists | TS 102 231 | published |
| | | | | Conformity Assessment | | | | |
| - | - | - | - | - | | *no requirement identified for such a document - relying on TS 119 403 / EN 319 403* | | |
| | | | | Testing Conformance & Interoperability | | | | |
| TS | 1 | 19 | 6 | 1 | 4 | Testing conformance & interoperability of trusted lists:<br>- Part 1: Test suites for testing interoperability of XML representation of trusted lists.<br>- Part 2: Specifications for testing conformance of XML representation of trusted lists | (new) | Undefined |

**Table 7**: Standards for trust service status lists providers

The current technical specifications of the EU Member State national trusted lists are defined by CD 2009/767/EC as amended and currently rely on ETSI TS 119 612 v1.1.1.

The technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 are laid down in Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 (OJ L 235, 9.9.2015, p26-36). CID 2015/1505/EU relies on TS 119 612 v2.1.1 for establishing such specifications.

Work on testing conformance and interoperability of trusted lists is expected to be part of standardisation work programme.

## 3.3 Other standards

The present section identifies standards and publicly available specifications coming from other sources than the CEN/ETSI while addressing the same topics and matters applicable to trust services and trust service providers. These additional sources include other standardisation bodies such as ISO, IETF, ITU, NIST, OASIS, UPU and national accreditation or supervisory bodies.

From all identified documents listed in Annex A, each of the next sub-sections will present these additional standards and publicly available specifications that have been retained as relevant with regards to the addressed topic. Relevance is discussed against the main objective of identifying standards as potential candidates for being referenced by eIDAS Regulation, against the existing ETSI/CEN standards being also candidates. Categories of interesting standards have been added for their connection with trust services and trust service providers even when not addressed directly by the eIDAS Regulation (e.g. cryptographic suites, formats of the document or data that may be required to be signed or sealed).

### 3.3.1 Cryptographic suites

Standards and publicly available specifications related to cryptographic suites can be split into two main categories: the specifications defining specific cryptographic algorithms and their parameters on the one side, and on the other side guidance oriented documents on how to select and implement in practice these algorithms and parameters in a specific context for a specific purpose. These latter guidance can either be defined at a national

level (e.g. BSI in Germany, ANSSI in France, IEEE, NIST or NSA in the US), in a specific domain of application (e.g. biopharma industry, banking industry) or at a more general level (e.g. European standardisation organisation, regional or continental organisation).

Relevant alternatives identified in Annex A are mostly related to the US NIST documents defining and providing guidance on the use of cryptographic suites.

As cryptographic suites and their proper use is a key building blocks for all trust services, it is of utmost importance that appropriate guidance on selection of cryptographic suites that would be applicable for implementation of trust services and in particular qualified trust services under the eIDAS Regulation will be maintained over time to ensure effective and appropriate security of these services.

Different countries set the minimum requirements on the cryptographic suites they recommend to be used. Some examples of what countries like Japan and the U.S. are recommending.

**CRYPTREC** is the **Cryptography Research and Evaluation Committees** set up by the Japanese Government to evaluate and recommend cryptographic techniques for government and industrial use and the **NSA Suite B Cryptography** is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program

Some of the recommended standards are:

- NIST series 800 on computer security such as
    - NIST SP 800- 38, 56, 67, 133, etc.
    - NIST FIPS series such as 140, 180, 197 and 198ISO/IEC 9798RFC 5759, Suite B Certificate and Certificate Revocation List (CRL) Profile
- RFCs:
    - RFC 6239, Suite B Cryptographic Suites for Secure Shell (SSH)
    - RFC 6379, Suite B Cryptographic Suites for IPsec
    - RFC 6460, Suite B Profile for Transport Layer Security (TLS)
- **IEEE (**the Institute of Electrical and Electronics Engineers (IEEE) standardization and the **P1363** project is for public-key cryptography). They´ve developed some standards such as:
    - *1363-- IEEE Standard Specifications for Public-Key Cryptography. 2000.*

As an example, the key length is an important security parameter. There´re recommendations and mathematical formulas to approximate the minimum key size requirement for security. Bluekrypt[26] compares the different approaches and techniques and select the appropriate key length for the desired level of protection.

A list of these documents can be found in annex A.

### 3.3.2 Due diligence – risk analysis – information security management

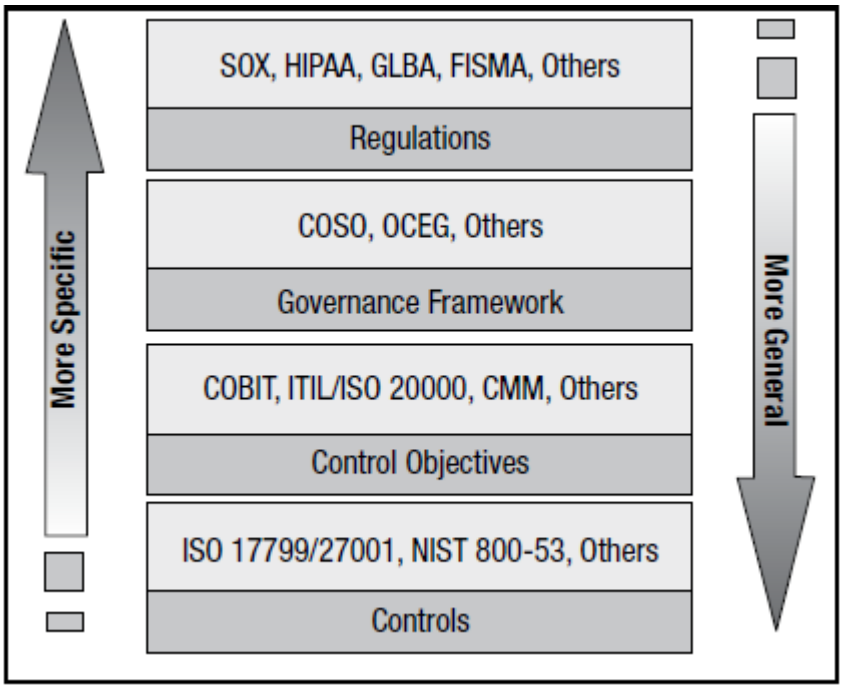
The increasing corporate governance requirements have caused companies to examine and ensure that controls are in place and operating effectively. Organizations are increasingly competing in the global marketplace, which is governed by multiple laws and supported by various best practices and standards (i.e, ITIL, ISO 27000 family, COSO, COBIT).

[26] Bluekrypt (www.keylength.com)

Determination of which standards meet the organization´s needs must be driven by the security policies agreed upon by management. The standards provide the specification of the technology to effectively enable the organization to become successful in meeting the requirements of the policy.

Standards may also refer to guidelines established by standards organizations and accepted by management, including organizations such as NIST, ISO, IEEE, ANSI, NSA and others.

A list of these documents can be found in annex A.




### 3.3.3 Security breach notification

It is crucial to improve the trustworthiness of this ecosystem to provide information to other interested parties on security breaches to avoid or with the goal to learn from incidents and propose alternatives or fixes. This information sharing among interested parties relating to possible enhanced risk from identified individuals, entities, identities, locations, domains, IP addresses, and other data to be determined in order to allow or to determine, whether to undertake additional steps to mitigate or solve.

This notification will consider issues such as legal limitations, privacy concerns, methods for updating or correcting information, and other factors that may arise from such notification of a security breach.

ENISA has developed multiple recommendations in the area of breach notifications (for notifications under Framework Directive Art. 13a, ePrivacy Directive Art.4, eIDAS Art.19).

In areas like cybersecurity, different non-EU governments like the U.S. publish acts on “antitrust policy on sharing cybersecurity information”, which are U.S. related executive orders[27].

[27] Such us https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform , http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

The MITRE Corporation has released the TAXII project. TAXII is not an information sharing initiative or application and does not attempt to define trust agreements, governance, or non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose. Additionally, the MITRE Corporation has also developed an XML schema called STIX.

There´s also, related to cyber threats, an alliance called the Cyber Threat Alliance (CTA), http://cyberthreatalliance.org/ which was founded in 2014, together with Palo Alto Networks, Fortinet, and McAfee and a group of cybersecurity providers, to share threat information to improve defenses against advanced cyber adversaries. The CTA adheres to strict guidelines that protect privacy and anonymize data, while at the same time pooling a broad array of resources to fight cybercriminals.

Also, private companies are working on this notification and have developed some documents, for example, Microsoft, which has announced its strategy publicly[28][29][30].

Some of these initiatives have been adopted by OASIS creating a technical committee on Cyber Threat Intelligence (CTI) taking into account the STIX, TAXII, and CybOX cyber security specifications and will be advanced as international standards by members of the OASIS consortium in a transition headed by the US Department of Homeland Security

### 3.3.4 Issuing digital certificates

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

Standards like IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile and ITU-t X.509 define a digital certificate

Another approach is the ISO/IEC JTC1 SC27 WG4 initiative on TSP practices and its positioning against CEN/ETSI framework documents:

- 14516-1, Guidelines for the use and management of Trust Service Providers – Part 1: Overview and concepts;
- 14516-2, Guidelines for the use and management of Trust Service Providers – Part 2: Guidelines on information security of PKI Trust Service Providers;
- 14516-3, Guidelines for the use and management of Trust Service Providers – Part 3: Guidelines on provision of services by PKI Trust Service Providers

The expected goal of the work made at ISO/SC27is to identify key TSP component services that can be operated by independent service providers for a TSP such as PKI service provider, dissemination service provider, registration service provider, etc.

[28] https://threatpost.com/microsoft-to-preview-interflow-information-sharing-platform/106798
[29] https://msdn.microsoft.com/en-us/library/dn750892.aspx
[30] http://blogs.microsoft.com/firehose/2014/06/23/microsoft-interflow-a-security-and-threat-information-exchange-platform-announced/

Best efforts will be made by editors of these documents to make these standards compatible with the ones from ETSI (for instance including parts equivalent to EN 319 403 using ISO 17065 as the accreditation standard).

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. Initially it was defined in RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP[31] but has been updated to RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP[32]. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Current OCSP/CRL specifications are not sufficient and must be profiled to cover requirements from Art.24.3 and Art.24.4 of eIDAS Regulation.

Another specification of interest in this area is RFC 4806, Online Certificate Status Protocol (OCSP) Extensions to IKEv2[33]

### 3.3.5 Formats of digital/electronic signatures and/or seals

The following ISO standard aims at helping business and governments to guarantee the long-term authenticity of electronic signatures, increasingly used in e-commerce and e-government. It will also ensure the interoperability of electronic signatures when the documents they authenticate are transferred and processed through different information technology systems. The ISO standard is in two parts:

- ISO 14533-1:2012, Processes, data elements and documents in commerce, industry and dministration – Long term signature profiles – Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)
- ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration – Long term signature profiles – Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

Klaus-Dieter Naujok, Chair of ISO technical committee ISO/TC 154 who developed the standard, commented: "ISO 14533-1:2012 and ISO 14533-2:2012 provide a framework complying with the European Commission Mandate M/460, as well as helping the work by UN/CEFACT on its current revision on Recommendation 14 (Authentication of Trade Documents by Means Other than Signature), for guaranteeing interoperability and consumption of messages regardless of the target platform. The new standards provide for long term protection of these document formats that is not currently available."

ISO 14533-1:2012 and ISO 14533-2:2012 were developed by ISO/TC 154, Processes, data elements and documents in commerce, industry and administration.

### 3.3.6 Generation of digital/electronic signatures and/or seals

The OASIS Digital Signature Services (DSS) develops techniques to support the processing of digital signatures, such as an interface for requesting that a web service produce and/or verify a digital signature.

The Digital Signature Services (DSS) specifications describe two XML-based request/response protocols: a signing protocol and a verifying protocol. The DSS Core specifications provide the basic protocols and elements, upon which other services can be built. For instance, the DSS-X Technical Committee has specified several profiles for specific usages.

[31] https://tools.ietf.org/html/rfc2560
[32] https://tools.ietf.org/html/rfc6960
[33] https://tools.ietf.org/html/rfc4806

The OASIS committee on extended services for digital signatures (DSS-X[34]) develops new profiles for digital signature services

### 3.3.7 Validation of digital/electronic signatures and/or seals

The IETF defines other options for a validation services, called Data Validation and Certification Server (DVCS) which is a public key infrastructure or PKI service providing data validation services, asserting correctness of digitally signed documents, validity of public key certificates and possession or existence of data.

A Data Validation and Certification Server (DVCS) is a Trusted Third Party (TTP)[35] providing data validation services, asserting correctness of digitally signed documents, validity of public key certificates, and possession or existence of data.

Services provided by a DVCS do not replace the usage of CRLs and OCSP[36], as mentioned in clause 3.3.4, for public key certificate revocation checking in large open environments, due to concerns about the scalability of the protocol.

RFC 3029 "Internet X.509 Public Key Infrastructure: Data Validation and Certification Server Protocols[37]

### 3.3.8 Preservation of digital/electronic signatures and/or seals

In library and archival science, digital preservation is a formal endeavor to ensure that digital information of continuing value remains accessible and usable. The goal of digital preservation is the accurate rendering of authenticated content over time

To standardize digital preservation practice and provide a set of recommendations for preservation program implementation, the Reference Model for an Open Archival Information System (OAIS) was developed. OAIS is concerned with all technical aspects of a digital object's life cycle: ingest, archival storage, data management, administration, access and preservation planning

- Not only OASIS is developing standards on how to preserve this digital information, there are also other entities promoting other documents such as
- *Design Criteria Standard For Electronic Records Management Software Applications*
- *Electronic archiving - Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation*
- *Space data and information transfer systems - Open archival information system (OAIS) - Reference model*
- *Information and documentation – Records management*
- *PDF/A Specification*
- *Data Preservation Systems Security; Part 1: Requirements for Implementation and Management*
- *Policy requirements for trust service providers signing and/or storing data objects*
- *Spécifications fonctionnelles d'un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps*
- *Evidence Record Syntax*

[34] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss-x
[35] https://en.wikipedia.org/wiki/Trusted_third_party
[36] https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol
[37] http://tools.ietf.org/html/rfc3029

It´s also necessary to assess these services, for what ISO defined an standard on audit and Certification of Trustworthy Digital Repositories (ISO 16363:2012), developed by the Consultative Committee for Space Data Systems (CCSDS), which was approved as a full international standard in March 2012

### 3.3.9 Time stamps and their issuance

A timestamp is the time at which an event is recorded by a computer, not the time of the event itself. In many cases, the difference may be inconsequential: the time at which an event is recorded by a timestamp (e.g., entered into a log file) should be close to the time of the event.

This data is usually presented in a consistent format, allowing for easy comparison of two different records and tracking progress over time; the practice of recording timestamps in a consistent manner along with the actual data is called timestamping. The sequential numbering of events is sometimes called timestamping

ISO 8601 standardizes the representation of dates and times. These standard representations are often used to construct timestamp values.

There are many timestamping schemes with different security goals:

- PKI-based – timestamp token is protected using PKI digital signature.
- Linking-based schemes – timestamp is generated such a way that it is related to other timestamps.
- Distributed schemes – timestamp is generated in cooperation of multiple parties.
- Transient key scheme – variant of PKI with short-living signing keys.
- MAC – simple secret key based scheme, found in ANSI ASC X9.95 Standard.
- Database – document hashes are stored in trusted archive; there is online lookup service for verification.
- Hybrid schemes – the linked and signed method is prevailing, see X9.95

Only the PKI covers the 3 of them, the RFC 3161, X9.95 and ISO/IEC 18014

According to the RFC 3161[38] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), a trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records, …) without the possibility that the owner can backdate the timestamps. Multiple TSAs can be used to increase reliability and reduce vulnerability.

The newer ANSI ASC X9.95 Standard[39] for Trusted Time Stamps augments the RFC 3161 standard with data-level security requirements to ensure data integrity against a reliable time source that is provable to any third party. This standard has been applied to authenticating digitally signed data for regulatory compliance, financial transactions, and legal evidence.

RFC 3628[40] Policy Requirements for Time-Stamping Authorities (TSAs)

### 3.3.10 Electronic delivery services

The delivery of services, whether electronic or not, is one of the key goals of the UPU, the Universal Postal Union (UPU), which is the second oldest international organization worldwide.

[38] https://tools.ietf.org/html/rfc3161
[39] https://en.wikipedia.org/wiki/ANSI_ASC_X9.95_Standard
[40] https://tools.ietf.org/html/rfc3628

The UPU has developed some standards regarding interoperability aspects, the registered electronic mail, in collaboration with CEN, etc.

**S33 Interoperability framework for postal public key infrastructures:**

The objective of this standard is to create a common Postal Public Key Infrastructure (PKI) to provide global certification and security services aimed at globally binding the identity of individuals and organisations with their public key. The framework itself and its first four elements (PKI structure, cryptographic algorithms, data formats and data dissemination protocols) are included.

**S52 Functional specification for postal registered electronic mail:**

This standard defines the functional specification of a secure electronic postal service, referred to as the postal registered electronic mail or PReM service. PReM provides a trusted and certified electronic mail exchange between mailer, designated operators and addressee/mailee. In addition, evidence of corresponding events and operations within the scope of PReM will be generated and archived for future attestation.

### 3.3.11 Supervision of services and certification of products

**Supervision of services**:

Considering the work done by the European cooperation for Accreditation (EA), there is a need to adopt the implementing acts Art.20.4 to support the EA proposed model for CAB accreditation and QTSs/QTSPs evaluation of conformity as well as to cover the missing part to that model i.e. the applicable “QTS/QTSP audit criteria” as discussed in section 2.2.

**Certification of products**:

Security assessment of an IT product is done through the security evaluation of the product. That evaluation should be made by a certification body, itself accredited by some authority. The Common Criteria evaluation scheme (http://www.commoncriteriaportal.org/), for instance, is organized in this way.

ISO 15408 defines a framework for the IT evaluation of IT security products.

Besides the Common Criteria evaluation model, the use of Regulation 765/2008 model should be assessed as well. It is also applicable to the certification of products and a comparable model to the one developed to accredit CABs to certify and confirm compliance of QTS/QTSPs to the provisions laid down in the eIDAS Regulation could be developed similarly for certification of products against appropriate criteria (be it evaluated and certified PPs).

**Criteria for products – Protection profiles**:

TSP and end-users will rely on IT products, either software or hardware (cryptographic modules, USB tokens…) to store, create, validate or preserve (signed or sealed) data. Directive 1999/93/EC mentioned such requirement for “secure signature creation devices”, but the eIDAS Regulation has broadened the concept “qualified signature/seal creation devices”. The eIDAS Regulation allows server (remote) qualified signature, that is in fact a kind of electronic service on-line requiring authentication (use of electronic mean of authentication), as well as remote identity verification using an eID (art. 24.1.(b)). Therefore security assessment of such elements may fall in the scope of interest of QTSP.

It is believed (expected) that CEN PPs developed under the CEN/ETSI framework for standardization of signatures will be natural candidates as criteria for being referenced as criteria against which “qualified signature/seal creation devices” must be certified as compliant with the provisions laid down in the eIDAS Regulation.

### 3.3.12 Formats of documents for which a digital/electronic signature or seal may be required

Protocols and format commonly used for documents include the following:

- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- XML (Extensible Markup Language), and its variant that include:
  - ebXML (electronic business XML)
  - "AS4 Profile of ebMS 3.0" from OASIS submitted to ISO
  - ISO 20022: standard for electronic data interchange between financial institutions (i.e. electronic funds transfers). It describes a metadata repository containing descriptions of messages and business processes, and a maintenance process for the repository content. The repository contains a huge amount of financial services metadata that has been shared and standardized across the industry. The metadata is stored in UML models with a special ISO 20022 UML Profile. Underlying all of this is the ISO 20022 metamodel - a model of the models. The UML (Unified Modeling Language) profile is the metamodel transformed into UML. The metadata is transformed into the syntax of messages used in financial networks. The first syntax supported for messages was XML Schema. ISO 20022 is widely used in financial services and adopted as SEPA format for storing & processing transactions.
- PDF
  - ISO 32000 – Document management – Portable document format
  - SR 003 032 on the Printable Representations of Electronic Signatures

### 3.3.13 Other initiatives

Beyond international standardization committees, there are numerous attempts to implement technical or organisational answers to the need for trust services such as digital identity, signature or transactions. Where no binding legal framework exists, particular requirements and specifications are usually issued by an authoritative body (professional order/association, steering committee, workgroups, etc.) to ensure interoperability of solutions and responsibilities of involved actors.

However, such *ad hoc* solutions tend to be limited to a specific domain and their reusability outside it can be difficult, if not impossible, to assess. The following initiatives were thus selected as they address a sufficiently large scope.

#### 3.3.13.1 xDTM & SafeBiopharma (U.S.)

In the U.S., the xDTM Standard Association[41] (an independent non-profit organization) is on its way to define and advance requirements (the xDTM Standard), and create the framework for an associated certification program to ensure open, secure digital transactions. In the same spirit as the e-IDAS Regulation, the xDTM self-defined objective is to define an interoperable and widely accepted standard. The term Digital Transaction Management (DTM) denotes a category of cloud services that would enable companies to manage their document-based transactions digitally with the same legal value and acknowledgement as they have with paper-based transactions.

First experiments with digital signatures in the U.S. originated in the pharmaceutical industry (http://www.safe-biopharma.org/overview.htm) and has achieved some success in that domain. The xDTM initiative seems to broaden the scope of the project in the same way that the e-IDAS Regulation expanded the 1999/93/EC Directive: digital signatures and identities become means to new digital services (digital transactions).

[41] www.xdtm.org

The xDTM Association has not yet released any standard.

#### 3.3.13.2 e-SENS (Electronic Simple European Networked Services)

e-SENS is a large-scale project to provide an easy access to public European administration and services online, and ensure interoperability across different national systems. Several European projects are part of this initiative:

- SPOCS (Simple Procedures Online for Cross-Border Services, http://www.eu-spocs.eu) uses the solution for the cross border use of natural persons eID developed by STORK. Furthermore it also builds on document transport concepts developed by STORK. It has used the Virtual Company Dossier (VCD) concept of PEPPOL for document containers and has generalized it into a container format for eDocuments (OCD) to package company information for transmission to Points of Single Contact in other countries.

- e-CODEX (e-Justice Communication via Online Data Exchange, http://www.e-codex.eu) will build on and make necessary changes to deliverables from SPOCS and the other pilots in order to meet its objectives of improving the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU.

- PEPPOL (Pan-European Public Procurement Online, http://www.peppol.eu) has developed and implemented technology standards for European governmental public electronic procurement.

- STORK (Secure idenTity acrOss boRders linKed, http://www.eid-stork.eu) aims at establishing a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. This platform allows European citizens to log in to public services of other Member States using the eID technology of their home country.

Currently, STORK 2.0 extends its scope to mandates and representation (e.g. of legal entities) and advances from eGovernment to private sector applications (http://www.eid-stork2.eu).

# 4. Mapping and analysis

## 4.1 Description of methodology

The following section contain mappings between the eIDAS requirements as identified in chapter 2 and the currently available standards as listed in the inventory in chapter 3 of this document. The mapping is oriented at the requirements specified in the different eIDAS articles.

In order to understand the meaning of the mapping and in order to apply the mapped standards in a proper way, the following should to be considered:

- The mapping indicates which standard allows to meet the requirements of the eIDAS Regulation. The mentioned standards usually only cover a part of the eIDAS requirements (the explanation will be given further in the text).
- In some cases the eIDAS Regulation articles laying down requirements for TSPs, TS's, QTSP's or QTS's allows for referencing standards (among other documents), either through direct reference or potentially via specifications established by the European legislator. Compliance with these referenced standards will provide a legal presumption of compliance with the associated legal provisions.
- It should be noted that this legal presumption compliance referencing mechanism is not complete in the Regulation in the sense that it does not cover all the provisions applicable to TSP/TS or QTSP/QTS but to a part of them.
- Furthermore, in practice, it might be rather unlikely at this moment in time, that a standard or a set of standards are available which have been developed especially in order to serve all the different eIDAS articles requirements applicable to all types of TSP/TS or QTSP/QTS. Again, the adequacy of the standards to the articles' requirements can at best be partial.
- Some of the standards content was compiled before the eIDAS Regulation had been released. The content therefore could not cover all of its requirements. In such case, the adequacy of the standards to the articles' requirements can at best be partial.
- In any case, the eIDAS Regulation *"should be technology-neutral"* (recital 27). Thus, even if the hereafter identified standards were to be mentioned in future delegated/implementing acts, compliance with the Regulation could alternatively also be achieved through other implementations, based upon other standards or based upon best practices. In case of a Qualified Service according to the eIDAS requirements, the suitability and coverage of such an alternative solution to meetl the eIDAS requirements will have to be judged by a Conformity Assessment Body (CAB) issuing a corresponding Conformity Assessment Report (CAR).

The Commission may, by means of implementing acts, establish reference number of standards (Art.20.4 (a)) for the accreditation of the conformity assessment bodies and for the conformity assessment report referred to in Art.20.1 and for (Art.20.4.(b)) for auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as referred to in Art.20.1. The standards based accreditation system the European cooperation for accreditation (EA) is currently establishing is however not addressing the standardization of the "QTSP/QTS audit criteria" against which the QTSP/QTS compliance with all the applicable provisions of the eIDAS Regulation will be assessed is missing. This is specifically addressed in section 4.3.

## 4.2 ETSI/CEN Framework - Trust service related standards mapping and analysis

### 4.2.1 Standards covering general TSP operations related requirements

#### 4.2.1.1 Requirements common to all TSPs

Implementing acts foreseen in Art.19(4) do not limit the legislative power of the European Commission to simply refer to standards that would have been assessed as allowing compliant implementations to meet the specific covered requirements and hence granting such compliant implementations a legal presumption of compliance with these requirements. The Commission may through such acts:

- (Art.19(4)a) specify the due diligence technical and organisational measures TSPs must implement to manage the risks posed to the security of the trust services they provide (Art.19(1)).
- (Art.19(4)b) define the formats and procedures, including deadlines, applicable for the purpose of security and personal data breach notifications by TSPs and QTSPs (Art.19(2)).

As already stated in section 2.3.1, the initiative of ENISA on security breach notifications (SBN) may make the adoption of the related implementing act under art.19.4 of eIDAS Regulation unnecessary. ENISA is currently developing technical guidelines to facilitate the implementation of article 19 of eIDAS Regulation. Once completed, these guidelines would be available to stakeholders for voluntary adoption, and be subject to regular revision (as it has been the case of these related to article 13a of the e-communication Framework Directive).

The following table however is analysing the relevance of the ETSI EN 319 4x1 standard in addressing the requirements common to all TSPs as these requirements are identified through the reference to the corresponding article of the eIDAS Regulation (first column). The second column provides, when applicable, a reference to foreseen implementing acts. The third column identifies the standard(s) being candidate for allowing implementer meeting the requirements (or standards referenced by primarily considered standard) for which the publication status is given in the fourth column. The last column provides the results of the assessment/analysis on whether the identified standard actually correctly address the requirement identified in the first column. The content of this last column can be limited to the identification of the standard clause addressing the requirement; when no addition comment is made it is assessed to allow addressing correctly the requirement.

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| 5(1) | - | General Policy Requirements for Trust Service Providers (ETSI TS 119 401/EN 319 401) | EN approval | Clause 7.13(c)<br><br>Note: compliance to EN 319 411-2 (QTSPs issuing QCs) and compliance to EN 391 421 (QTSPs issuing qualified time-stamps) enforce compliance to 319 401 clause 7.13(c). |
| 13(2) | - | General Policy Requirements for Trust Service Providers (ETSI TS 119 401/EN 319 401) | EN approval | Clause 6.2<br><br>Note: compliance to EN 319 411-2 (QTSPs issuing QCs) and compliance to EN 391 421 (QTSPs issuing qualified time-stamps) enforce compliance to 319 401 clause 6.2. |

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| 15 | - | General Policy Requirements for Trust Service Providers (ETSI TS 119 401/EN 319 401) | EN approval | Clause 7.13(b) requires TS's provided and end user products used in the provision of these TS's to be made accessible for persons with disabilities (referring to EN 301 459 for consideration).<br><br>Note: compliance to EN 319 411-2 (QTSPs issuing QCs) and compliance to EN 391 421 (QTSPs issuing qualified time-stamps) enforce compliance to 319 401 clause 7.13.(b). |
| | | Accessibility requirements suitable for public procurement of ICT products and services in Europe (ETSI EN 301 549) | Published | |
| 19(1) | 19(4)<br><br>(indirect) | General Policy Requirements for Trust Service Providers (ETSI TS 119 401/EN 319 401) | EN approval | Clause 5 (Risk assessment): however no strict requirement to implement the selected measures ("select" to become "implement").<br><br>Clause 6.3 (information security policy)<br><br>Clause 7 (excepted 7.1.1 & 7.13)<br><br>The additional requirements stated in clause 6.4 ("facility, management & operational controls) and 6.5 (technical security controls) of EN 319 411-1 are deemed to be required (when generalized for all types of TSPs covered by the eIDAS Regulation) in order to meet the provisions of Art.19(1). For this aim the following is required:<br><br>- compliance with ETSI EN 319 411-1 clauses 6.4 and 6.5, for TSP issuing certificates;<br><br>- compliance with ETSI 319 421 appropriate clauses for TSPs issuing electronic time stamps |

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| | | For TSP issuing certificates: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (ETSI TS 119 411-1/EN 319 411-1) | EN approval | In order to meet Art.19(1) requirements, compliance with ETSI EN 319 411-1 clauses 6.4 and 6.5 would be required for TSP issuing certificates. |
| | | For TSP issuing time stamps: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (ETSI TS 119 421/EN 319 421) | EN approval | In order to meet Art.19(1) requirements, compliance with ETSI EN 319 421 clauses 7.8, 7.9, 7.10, 7.12, and 7.13 would be required for TSP issuing time stamps. |
| 19(2) | 19(4)<br><br>(indirect) | General Policy Requirements for Trust Service Providers (ETSI TS 119 401/EN 319 401) | EN approval | Clause 7.9 (in particular (e) and (f))<br><br>Note: compliance to EN 319 411-2 (QTSPs issuing QCs) and compliance to EN 391 421 (QTSPs issuing qualified time-stamps) enforce compliance to 319 401 clause 7.9. |

There is no specific ETSI standard dedicated to address requirements on due diligence technical and organisational measures that TSPs must implement to manage the risks posed to the security of the trust services they provide or requirements on the formats and procedures, including deadlines, applicable for the purpose of security and personal data breach notifications by TSPs.

Both these types of requirements are however addressed in documents addressing specific types of trust service provider and trust services, requiring any potential referencing process to point to a long list of specific clauses from a combination of specific documents. Furthermore only TSP issuing (qualified) certificates and TSP issuing (qualified) time-stamps related standards are currently available.

#### 4.2.1.2 Requirements common to all QTSPs

Requirements common to all QTSPs are these requirements applicable to all TSPs (see table in section 4.2.1.1) together with the requirements listed in the following table.

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| 20(1) | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Not covered by EN 319 411-2 as it refers to the applicable requirements of EN 319 411-1 that includes no requirements: clause 6.7 of EN 319 411-1 only includes a note referring to EN 319 403 where the requirement is covered (but this document applies to (accredited) conformity assessment bodies.<br><br>Note that remedying any audit failure or non-conformity is not addressed by the above standards.<br><br>Not covered by EN 319 401 |
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Same comment as above |
| 21(1) | 21(4) | No ETSI/CEN standard available or covering specifications for the formats and procedures for the purpose Art.21(1) | | |
| 21(2) | 21(4) | No ETSI/CEN standard available or covering specifications for the formats and procedures for the purpose Art.21(2) | | |
| 24(2).a | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Covered by EN 319 411-2 as it (clause 5.2) refers to the applicable requirements of EN 319 411-1 that in turn (clause 5.2) refers to applicable requirements (clause 6.1) from EN 319 401.<br><br>Note: “coverage” requires “relying party” to be understood as covering competent supervisory body. |
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Covered by EN 319 421 as it (clause 6.2) refers to the applicable requirements (clause 6.1) from EN 319 401.<br><br>Note: “coverage” requires “relying party” to be understood as covering competent supervisory body. |
| 24(2).b | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clause 6.4.4 referring to EN 319 411-1 clause 6.4.4 building on EN 319 401 clause 7.2.<br>Clause 6.9.1 referring to EN 319 411-1 clause 6.9.1 building on EN 319 401 clause 7.1. |

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Clause 7.2 & 7.3 refer to the applicable requirements (respectively clause 7.1 and 7.2) from EN 319 401. |
| 24(2).c | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clause 6.8.2 referring to EN 319 411-1 clause 6.8.2 building on EN 319 401 clause 7.1.1, item c). |
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Clause 7.2 refers to the applicable requirements (clause 7.1 including clause 7.1.1, item c) from EN 319 401. |
| 24(2).d | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clauses 6.1, 6.3.4, 6.3.5 and 6.9.4 respectively referring to EN 319 411-1 clauses 6.1, 6.3.4, 6.3.5 and 6.9.4, that latter building on ETSI EN 319 401, clause 6.2. |
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Clause 6.3 referring to the applicable requirements (clause 6.2) from EN 319 401. |
| 24(2).e & 24(2).f | 24(5) | This is likely to be declined per type of supported process including per type of provided qualified trust service as well as covering Annex II.3 mode of provisioning QSCDs (generating and/or managing signature creation data on behalf of the signatory) e.g. supporting remote or server based creation of (qualified) (advanced) electronic signatures.<br>Candidate standards are:<br>- prCEN/EN 419 221 - PP for TSP cryptographic modules, in particular its Part 5 PP for cryptographic modules for TSPs, aimed at being aligned with eIDAS Regulation.<br>- prCEN/EN 419 231 PP for trustworthy systems supporting time stamping.<br>- prCEN/EN 419 241 security requirements and PP's for trustworthy systems supporting server signing.<br>- prCEN/TS 419 261 (was prTS 419 221-1, was prTS 14167-1) - Security requirements for Trustworthy Systems (incl. Managing Certificates for Electronic Signatures).<br>EN 319 411-2 and EN 319 421 include requirements for corresponding QTSPs to make use of trustworthy systems referred to in Art.24(2).e&f. | | |
| 24(2).g | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clauses 6.4 and 6.5 referring to EN 319 411-1 clauses 6.4 and 6.5 building on EN 319 401. |
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Clauses 6.1, 6.4 & 7 building on EN 319 401. |
| 24(2).h | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clauses 6.2.2, 6.3.4, 6.3.8, 6.4.5, 6.4.6, and 6.4.9 referring to EN 319 411-1 corresponding clauses building on EN 319 401. |

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Clauses 7.6.5, 7.7.2, 7.8 and 7.12 building on EN 319 401. |
| 24(2).i | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clause 6.4.9 referring to EN 319 411-1 clause 6.4.9 building on EN 319 401 clause 7.12. |
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Clause 7.14 building on EN 319 401 clause 7.12. |
| 24(2).j | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clauses 6.8.4 and 6.8.15 referring to EN 319 411-1 clause 6.8.4 and 6.8.15 building on EN 319 401 clause 7.13.a&c. |
| | | TS 119 421/EN 319 421 (QTSPs issuing time stamps) | EN approval | Clause 7.15 building on EN 319 401 clause 7.13. |

#### 4.2.1.3 Requirements for QTSPs issuing qualified certificates

Requirements applicable to QTSPs issuing QCs are these requirements applicable to all TSPs (see table in section 4.2.1.1), together with all the requirements applicable to all QTSPs (see table in section 4.2.1.2) and together with the requirements listed in the following table.

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| 24(1) | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clauses 6.2.2 and 6.2.3 referring to EN 319 411-1 corresponding clauses 6.2.2 and 6.2.3.<br><br>N*ote: To be compliant with art. 24.1.(b) it is (explicitly) mandatory to use electronic identification means for which physical presence was performed at issuance, regardless it represents level 'substantial' or 'high'.* |
| 24(2).k | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clause 6.1 referring to EN 319 411-1 corresponding clause 6.1. |
| 24.3 | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clause 6.2.4 referring to EN 319 411-1 corresponding clause 6.2.4. |
| 24.4 | | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clause 6.3.10 referring to EN 319 411-1 corresponding clause 6.3.10. Note: the "free of charge" aspect is not covered by EN 319 411-2 as deemed to be out of scope of the standard. |

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| Note: With regards to compliance with Art.24.3 and Art.24.4, it is believed that EN 319 411-2 does not include sufficient provisions with regards to the CRL and OCSP profile and creation process in order to meet the requirements of these articles. | | | | |
| 28(1) & Annex I<br><br>38(1) & Annex III<br><br>28(3) & 38(3)<br><br>28(4) & 38(4)<br><br>45(1) & Annex IV | 28(6)<br><br>38(6)<br><br>28(6)<br>38(6)<br><br>28(6)<br>38(6)<br><br>45(2) | TS 119 411-2/EN 319 411-2 (QTSPs issuing QCs) | EN approval | Clause 6.6.1 referring to EN 319 411-1 corresponding clause 6.6.1 and requiring compliance with EN 319 412 series in function of the type of QC.<br><br>Clause 6.3.9 referring to EN 319 411-1 corresponding clause 6.3.9.<br><br>*Note: Instead of issuing a new QSCD, the QTSP might want to certify public keys originating from QSCD already in the hand of a user or operated I accordance with Annex II.3. In such a case the QTSP has to ensure by appropriate means that the public key corresponds to a private key that is truly residing in a certified QSCD, before issuing the certificate (Art.3(12)). This is expected to be covered by EN 319 411-2 clauses 6.5.1(c), 6.5.2(a), 6.3.5(b), and 6.3.12* |
| 28(5)<br><br>38(5) | 28(6)<br><br>38(6) | | | Temporary suspension of QC for electronic seals and for electronic signatures may be specified on a national basis: Assessment to be made on an ad-hoc national basis. |
| 38(3) | | | | *Note: Also applying to QC for WSA when special case of QC for electronic seals – Recital (65)* |
| 38(4) | | | | *Note: Also applying to QC for WSA when special case of QC for electronic seals – Recital (65)* |

ETSI EN 319 412 is expected to cover sufficient requirements to ensure QTSPs issuing QCs to meet the applicable requirements of the eIDAS Regulation. However with regards to compliance with Art.24.3 and Art.24.4, it is believed that EN 319 411-2 does not include sufficient provisions with regards to the CRL and OCSP profile and creation process in order to meet the requirements of these articles. This gap should be covered by additional standardisation work.

#### 4.2.1.4 Requirements for QTSPs providing qualified validation services for QESig / QESeal (Art.33 / Art.40)

| Article | I.A. ref. | Standard | Status | Comment |
|---|---|---|---|---|
| 32(1) | 32(3) | TS 119 172-4 | - | Under drafting process |
| | | EN 319 102-1 | EN approval | |
| | | EN 319 102-2 | - | Standardisation work not started |
| 32(2) | - | TS 119 101 | Under approval | - |
| 33(1) | 33(2) | Procedures for electronic signature verification (CWA CWA 14171) | Published | Technical process description<br>Note: outdated by EN 319 102-1 |
| | | Signature validation procedures and policies (ETSI TS 102 853) | Published | Technical process description<br>Note: outdated by EN 319 102-1 |
| | | Policy and security requirements for TSPs providing signature validation services (ETSI EN 319 441) | - | Standardisation work not started |
| | | General requirements on testing compliance and interoperability of signature creation and validation (ETSI TS 119 104) | - | |
| | | EN 319 102-1 | EN approval | |
| | | EN 319 102-2 | - | Standardisation work not started |

#### 4.2.1.5 Requirements for QTSPs providing preservation service for QESig/ QESeal (Art.34 / Art.40)

| Article | Standard | Status | Comment |
|---|---|---|---|
| 34(2) | PDF/A Specification (ISO 19005-1, Adobe) | Published | See below |
| 34(2) | Audit and Certification of Trustworthy Digital Repositories (ISO 16363:2012, CCSDS) | Published | See below |
| 34(2) | Storage of electronic invoices (CWA CWA 15580) | Published | See below |

| Article | Standard | Status | Comment |
|---|---|---|---|
| 34(2) | Design Criteria Standard For Electronic Records Management Software Applications (DoD DoD 5015.2) | Published | See below |
| 34(2) | Conformity assessment of data preservation service providers (ETSI EN 319 523) | - | (missing) |
| 34(2) | Data preservation services through signing (ETSI EN 319 522) | - | (missing) |
| 34(2) | Policy and security requirements for data preservation service providers (ETSI EN 319 521) | - | (missing) |
| 34(2) | Data Preservation Systems Security; Parts 1-2 (ETSI/ TS 101 533) | Published | See below |
| 34(2) | Policy requirements for trust service providers signing and/or storing data objects (ETSI/CEN TS 102 573) | Published | See below |
| 34(2) | Evidence Record Syntax (ERS)(IETF RFC 4998) | Published | See below |
| 34(2) | Electronic archiving - Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation (ISO/IEC ISO 14641-1:2012) | Published | See below |
| 34(2) | Information and documentation – Records management (ISO/IEC ISO 15489-1:2001) | Published | See below |
| 34(2) | Information technology – Metadata registries (MDR)(ISO/IEC ISO/IEC 11179) | Published | See below |
| 34(2) | Space data and information transfer systems - Open archival information system (OAIS) - Reference model (ISO/IEC ISO 14721:2012) | Published | See below |
| 34(2) | Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents | Published | See below |
| 34(2) | International Standard for Archival Description (General)( ISAD(G) ) | Published | See below |

The eIDAS regulation has no specific requirement on the « procedures and technologies » that can be used to « [extend] the trustworthiness of the qualified electronic signature beyond the technological validity period ». Thus, no assessment of the coverage of the Regulation is possible.

In September 2015, ETSI work started to address trust service consisting in preservation of (qualified) electronic signatures under the form of a study undertaken to evaluate the needs and scope for such standardisation work.

#### 4.2.1.6 Requirements for QTSPs issuing qualified electronic time stamps (Art.42)

| Article | Standard | Status | Comment |
|---|---|---|---|
| 42(2) | Time-stamping System (CC3.1) (ANSSI DCSSI-PP 2008/07) | Published | TST trustworthy product |
| 42(2) | Politique d'Horodatage Type (ANSSI RGS A5) | Published | Assessment |
| 42(2) | EESSI Conformity Assessment Guidance - Part 8 - Time-stamping Authority services and processes (CEN CWA 14172-8) | Published | Assessment |
| 42(2) | Policy and security requirements for TSPs providing time-stamping services (ETSI EN 319 421) | EN approval | Assessment, trustworthy systems, time management |
| 42(2) | Profiles for TSPs providing time-stamping services (ETSI EN 319 422) | EN approval | Assessment, trustworthy systems |
| 42(2) | Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (ETSI TS 119 421) | Published | Replaced by EN 319 421 under the M460 |
| 42(2) | Time-stamping protocol and time-stamp profiles (ETSI TS 119 422) | Published | Replaced by EN 319 422 under the M460 |
| 42(2) | Policy requirements for time-stamping authorities(ETSI TS 102 023) | Published | Replaced EN 319 421-422 under the M460 |
| 42(2) | Time-stamping Protection Profile (prCEN/TS 419231) | DRAFT | |

Conforming to the expected standards must ensure the binding of the date and time to data (42(1)(a)) and an accurate time source (42(1)(b)). The *ETSI/CEN TS 102 023* standard, which is currently used for the certification of timestamping authorities, was updated under the M460 mandate, and split in two standards.

- *ETSI EN 319 421* is a natural candidate for enforcing good security practices and correct time-management of a timestamping authority ; *ANSSI RGS A5* strengthens it but contains some French-specific requirements that may not be compatible with the actual practices in other countries.
- Conforming to the *ETSI EN 319 422* ensures the binding of the date and time to data in the produced timestamps.

ANSSI DCSSI-PP 2008/07 is currently the only evaluated Common Criteria protection profile for a timestamping system. The prCEN/TS 419231 protection profile is currently under evaluation.

#### 4.2.1.7 Requirements for QTSPs providing qualified electronic registered delivery service (Art.44)

| Article | Standard | Status | Comment |
|---|---|---|---|
| 44(2) | Registered Electronic Mail (REM) (ETSI/CEN TS 102 640 (5 parts document)) | Published | Partial coverage of the eIDAS requirements |
| 44(2) | Functional specification for postal registered electronic mail (UPU S52-2) | Published | Partial coverage of the eIDAS requirements |
| 44(2) | Secured electronic postal services (SePS) interface specification (Parts A& B, (UPU S43a-4 & S43b-4)) | Draft | Partial coverage of the eIDAS requirements |
| 44(2) | Conformity assessment for REM service providers (ETSI EN 319 513) | (M460) | Missing |
| 44(2) | Policy and security requirements for registered electronic mail (REM) service providers (ETSI EN 319 511) | (M460) | Missing |
| 44(2) | Registered electronic mail (REM) services (ETSI EN 319 512) | (M460) | Missing |
| 44(2) | Testing compliance and interoperability of REM service providers (ETSI TS 119 514) | (M460) | Missing |

Article 44 of the eIDAS Regulation requires the following on qualified electronic registered delivery services:

*(a) they are provided by one or more qualified trust service provider(s);*

*ETSI TS 102 640 :* That point is not addressed in the standards. Moreover, REM systems may forward messages to "regular e-mail" services, hence "unqualified" services providers.

*UPU :* That point is not addressed in the standards. In particular, issues regarding "cross-border scenarios" are explicitely not covered.

*(b) they ensure with a high level of confidence the identification of the sender;*

*ETSI/CEN TS 102 640 :* In the standards, "choice of the authentication mechanism is left to the [trust service provider]". Specific requirements must hence be added to correctly reflect these of the eIDAS Regulation.

*UPU :* Same situation ("The act of physically authenticating individual calls to a SePS is outside the scope of this specification").

*(c) they ensure the identification of the addressee before the delivery of the data;*

*ETSI/CEN TS 102 640 :* That point is covered in the functional working of the protocol.

*UPU :* idem.

*(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;*

*ETSI/CEN TS 102 640 :* the standards only "assume the usage of at least an Advanced Electronic Signature […] issued with a Secure Signature Creation Device", in the sense of the EU Directive 1999/93/EC. Hence, this standard does not require such a signature, strictly speaking.

*UPU :* The standards contain no requirement on the level of the signatures.

*(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;*

*ETSI/CEN TS 102 640 :* That point is not addressed in the standards.

*UPU :* idem.

However, that point could be deemed unapplicable to these standards, which do not consider that one could alter the sent data in any way.

*(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.*

*ETSI/CEN TS 102 640 :* That point is not addressed in the standards.

*UPU :* The electronic PostMark is a "superset of a standard timestamp", and several European post services are already providing ETSI 102 023-certified services.

Overall, the existing standards are technical and were written before any existing regulation. It is not surprising, then, that they do not try to strongly enforce specific properties. In particular, they contain very few strict requirements on the services.

Future ETSI standardisation work on electronic registered delivery services will leverage on the existing multipart TS 102 640 series addressing standardisation of registered electronic mail (REM) and align these specifications to the requirements of Regulation (EU) No 910/2014 on electronic registered delivery services. Effective production of such REM specifications and more general specifications addressing all other types of electronic registered delivery services has not been planned yet and is likely not to finalised in 2016.

The standards could be used as a basis for a technical definition of the qualified electronic registered delivery services, under additional requirements (service profiles) covering the above elements. For instance, the requirement that sent data must be signed/sealed according to (d).

#### 4.2.1.8 Requirements for QTSPs providing qualified certificates for website authentication

| Article | Standard | Status | Comment |
|---|---|---|---|
| 45(2) | Baseline requirements for the issuance and management of publicly-trusted certificates (CAB Forum CAB BR) | Published | Partial (see below) |
| 45(2) | EV SSL certificate guidelines (CAB Forum CAB EVSSL) | Published | Partial (see below) |
| 45(2) | Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates (ETSI TR 103 123) | Published | Guidance document for auditors (but much lower Assurance scope than expected in eIDAS |

| Article | Standard | Status | Comment |
|---|---|---|---|
| 45(2) | Technical report TR 101 564 on guidance on ETSI TS 102 042 for issuing EV certificates for auditors and CSPs | Published | Intended to be used by auditors as a guidance to assess the compliance of a CA according to TS 102 042 and for the CA to clarify the requirements |

Partial coverage: The CAB Forum documents are an industrial standard on the Internet, used by all the mainstream web browsers, but their requirements, which aim at strongly ensuring a site's identity and that of its owner, do not fully match these of a « qualified certificate for website authentication », as defined in the eIDAS Regulation.

ETSI EN 319 412-4 ("Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates") is an expected candidate for referencing by Art.45(2).

### 4.2.2 Standards covering technical requirements

#### 4.2.2.1 Trustworthy systems and products

Under art. 24, QTSP are to use *"trustworthy systems and products"* and *"trustworthy systems for storage"*, which can be assumed to meet these requirement should they conform to identified technical standards.

This section exclusively concerns the requirements applicable to all QTSP. Specific services are addressed in their respective sections.

| Article | Standard | Status | Comment |
|---|---|---|---|
| 24(5) | Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token: Parts 2,3,4 (ANSSI/BSI document TR 3110) | Published | Specific trustworthy product |
| 24(5) | Signature creation and administration for eIDAS token (ANSSI/BSI document) | Published | Specific trustworthy product |
| 24(5) | EESSI Conformity Assessment Guidance - Part 3 - Trustworthy systems managing certificates for electronic signatures (CEN CWA 14172-3) | Published | Specific area (signature service) |
| 24(5) | Business guidance on cryptographic suites (ETSI TR 119 300) | Published | Applicable to all services |
| 24(5) | Cryptographic Suites for Secure Electronic Signatures (ETSITS 119 312) | Published | Specific area (signature service) |
| 24(5) | Algorithms and Parameters for Secure Electronic Signatures (ETSI SR 002 176/TS 102 176) | Published | Specific area (signature service) |
| 24(5) | Information technology - Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions (ISO/IEC 10118-3:2004) | Published | Applicable to all services |

| Article | Standard | Status | Comment |
|---|---|---|---|
| 24(5) | Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (ISO/IEC 13335-1:2004) | Published | IT security management |
| 24(5) | Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO/IEC 27000:2009) | Published | IT security management |
| 24(5) | Information technology -- Security techniques -- Information security management systems -- Requirements (ISO/IEC 27001:2013) | Published | IT security management |
| 24(5) | Information technology -- Security techniques -- Code of practice for information security controls (ISO/IEC 27002:2013) | Published | IT security management |
| 24(5) | Information technology -- Security techniques -- Information security management system implementation guidance (ISO/IEC 27003:2010) | Published | IT security management |
| 24(5) | Information technology -- Security techniques -- Information security management -- Measurement (ISO/IEC 27004:2009) | Published | IT security management |
| 24(5) | Information technology - Security techniques - Information security risk management (ISO/IEC 27005:2011) | Published | IT security management |
| 24(5) | Protection profiles for TSP Cryptographic modules (ETSI EN 419 221, parts 1-5) | Draft | Trustworthy products |
| 24(5) | Security requirements for trustworthy systems supporting server signing (signature generation services) (ETSI EN 419 241, parts 1-3) | Draft | Signature services |
| 24(5) | Security requirements for trustworthy systems managing certificates for electronic signatures (EN 419 261) | - | - |

Article 24 mentions :

a) trustworthy systems and products (art.24.2.(e)), and
b) trustworthy systems for personal data storage (art.24.2.(f)).

The main issue with (a) is that "trustworthiness" is an abstract notion, which corresponds, in practice, to different properties for different trust services. There are thus two possible solutions that are not necessarily exclusive. First, implementing acts could refer to generic security practices, applicable to all TSPs, such as ETSI EN 319 401 or ISO/IEC 27001:2013. Second, implementing acts could refer to specific standards, depending on each trust service, such as protection profiles for signature services.

Candidate standards for referencing by Art.24(a) are:

- prCEN/EN 419 221 - PP for TSP cryptographic modules, in particular its Part 5 PP for cryptographic modules for TSPs, aimed at being aligned with eIDAS Regulation.
- prCEN/EN 419 231 PP for trustworthy systems supporting time stamping.
- prCEN/EN 419 241 security requirements and PP's for trustworthy systems supporting server signing.
- prCEN/TS 419 261 (was prTS 419 221-1, was prTS 14167-1) - Security requirements for Trustworthy Systems (incl. Managing Certificates for Electronic Signatures).

While no standard has been identified as candidate for being referenced under Art.24(b), it could be expected that prCEN/TS 419 261 could include provisions for trustworthy systems to meet Art.24(2)f requirements.

#### 4.2.2.2 QSCD

| Article | Standard | Status | Comment |
|---|---|---|---|
| 29(2)<br>39(2) | Application interfaces for secure signature creation devices - Parts 1-5 (CEN EN 419 212) | Published | Partial (see below) |
| 29(2)<br>39(2) | Protection profiles for secure signature creation devices – Parts 1-6 (CEN EN 419 211) | Published | Partial (see below) |
| 29(2)<br>39(2) | Protection profiles for TSP Cryptographic modules – Part 1-5 (CEN EN 419 221) | Draft<br>(part 5 is a CEN prEN 419 221-5) | Partial (see below) |
| 29(2)<br>39(2) | Trustworthy systems supporting server signing (signature generation services) - Parts 1-3 (CEN EN 419 241) | Draft<br>(TS 419241 is published) | Partial (see below) |

Annex II on qualified electronic signature/seal creation device require "by appropriate technical and procedural means", that:

*1.[…] such device ensures:*

*(a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;*

*(b) the electronic signature creation data used for electronic signature creation can practically occur only once;*

*(c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;*

These properties are fully addressed in the protection profiles for cryptographic module and signature devices (CEN EN 419 211, CEN EN 419 221). *Common Criteria* and FIPS PUB security evaluation have been successfully used for SSCD for several years now, and the eIDAS Regulation is no reason for change on this matter.

*(d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.*

*2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.*

These requirements are addressed in the standards on signature creation applications (CEN EN 419 212 and CEN EN 419 241).

*3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.*

That requirement is purely procedural and cannot be addressed in a standard.

*4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:*

*(a) the security of the duplicated datasets must be at the same level as for the original datasets;*

This point is addressed as 1.(a)-(c) in the protection profiles for cryptographic modules and other ETSI standards.

*(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.*

That requirement is purely procedural and cannot be addressed in a standard.

Notification of QSCD

Articles 31(3) and 39(3) consider the publication of a list of certified qualified electronic signature/seal creation devices.

There exists currently no standard for the would-be formats of such a list.

#### 4.2.2.3 Signature Validation

| Article | Standard | Status | Comment |
|---|---|---|---|
| 32(3) | Electronic Signature Verification Application (CC3.1)(ANSSI ANSSI-CC-PP 2008/06) | Published | Protection profile for a verification system (not service) |
| 33(2) | Electronic Signature Verification Module (CC3.1)(ANSSI DCSSI-PP 2008/06) | Published | Protection profile for a verification system (not service) |
| 32(3) | Conformity assessment for signature creation and validation applications (and procedures)(CEN EN 419 103) | - | - |

| Article | Standard | Status | Comment |
|---|---|---|---|
| 32(3) | Protection profiles for signature creation and validation application (CEN EN 419 111) | Published | Protection profile |
| 32(3) | Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation (ETSI TS 119 102-1) | Published | Technical process description |
| 32(3) | Policy and security requirements for signature creation and validation (ETSI TS 119 101) | - | - |
| 32(3) | Profiles for TSPs providing signature validation services (ETSI EN 319 442) | - | - |
| 32(3) | Signature validation procedures and policies (ETSI/CEN TS 102 853) | Published | Partial |
| 32(3) | DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports (OASIS DSS-VR ) | Published | Partial |

Validation of qualified electronic signatures/seals must ensure that (art. 32(3)):

*(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;*

*(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;*

*(f) the electronic signature was created by a qualified electronic signature creation device;*

*ETSI/CEN TS 102 853:* trust management is out of the scope of the standard. These requirements are thus not addressed. However, the qualified status of the signature's certificates is considered among the available constraints.

*ETSI TS 119 102-1:* not addressed in the standard.

*(c) the signature validation data corresponds to the data provided to the relying party;*

*(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;*

*(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;*

*(g) the integrity of the signed data has not been compromised;*

*(h) the requirements provided for in Article 26 were met at the time of signing* [the signature is an advanced signature].

*ETSI/CEN TS 102 853, ETSI TS 119 102-1:* these checks are covered in the standard.

*2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.*

*A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who […] allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service. [art. 33(2)]*

These requirements are not addressed in the standards.

#### 4.2.2.4 Advanced Signatures and seals

| Article | Standard | Status | Comment |
|---|---|---|---|
| 27(5)<br>37(5) | ASiC Baseline Profile (ETSI/CEN TS 103 174) | Published | See below (about profiles) |
| 27(5)<br>37(5) | CAdES Baseline Profile (ETSI/CEN TS 103 173) | Published | See below (about profiles) |
| 27(5)<br>37(5) | PAdES Baseline Profile (ETSI/CEN TS 103 172) | Published | See below (about profiles) |
| 27(5)<br>37(5) | XAdES Baseline Profile (ETSI/CEN TS 103 171) | Published | See below (about profiles) |
| 29(2)<br>39(2) | Protection profiles for signature creation and validation application (CEN EN 419 111) | Published | See below (about profiles) |
| 29(2)<br>39(2) | Security requirements for trustworthy systems managing certificates for electronic signatures (CEN EN 419 261) | Published | See below (about profiles) |
| 27(5)<br>37(5) | Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation (ETSI TR 119 102-1) | Published | See below (about profiles) |
| 27(5)<br>37(5) | Cryptographic Suites for Secure Electronic Signatures (ETSI TS 119 312) | Published | See below (about profiles) |
| 27(5)<br>37(5) | PDF Advanced Electronic Signature Profiles; Parts 1-6 (ETSI/CEN TS 102 778) | Published | See below (about profiles) |
| 27(5)<br>37(5) | PDF Advanced Electronic Signatures (PAdES); Usage and implementation guidelines (ETSI/CEN TR 102 923) | Published | Guidance document |

| Article | Standard | Status | Comment |
|---|---|---|---|
| 27(5)<br>37(5) | Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES) (ETSI/CEN TS 102 734) | Published | See below (about profiles) |
| 27(5)<br>37(5) | Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES) (ETSI/CEN TS 102 904) | Published | See below (about profiles) |
| 27(5)<br>37(5) | XML Advanced Electronic Signatures (XAdES) (ETSI/CEN TS 101 903) | Published | See below (about profiles) |
| 27(5)<br>37(5) | CAdES - CMS advanced electronic signatures (ETSI EN 319 122) | EN approval | See below (about profiles) |
| 27(5)<br>37(5) | PAdES - PDF advanced electronic signatures (ETSI EN 319 142) | EN approval | See below (about profiles) |
| 27(5)<br>37(5) | XAdES - XML advanced electronic signatures (ETSI EN 319 132) | EN approval | See below (about profiles) |
| 27(5)<br>37(5) | Procedures for signature creation and validation (ETSI EN 319 102) | EN approval | Interoperability |

With a few exceptions, all the above standards are technical signature profiles and how they are to be implemented in binary (CAdES/CMS), XML and PDF formats[42]. In these standards, the signature are "advanced" in the sense that they are technically more complex than the "basic" signatures formats they extend, and that they ensure more evolved security properties (long-term duration of electronic signatures, timestamping, etc.).

Requirements on advanced electronic signature are defined in article 26:

*(a) [must be] uniquely linked to the signatory;*

*(b) [must be] capable of identifying the signatory;*

*(d) [must be] linked to the data signed therewith in such a way that any subsequent change in the data is detectable.*

Practically, these requirements are enforced by the "advanced" signature formats: the link with the signer and his/her identity come from the digital certificate, and the integrity-protected link between signature and signed data, from cryptographic methods.

[42] The term "advanced electronic signature" in these standards has absolutely no relationship with the notion used y the eIDAS Regulation

*(c) [must be] created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control;*

That requirement is not directly addressed by signature profiles. Indirectly, through the use of qualified certificate attributes specified in the "advanced" standards, however, it is possible to determine that an electronic signature has been made using a SSCD, which is a sufficient condition for (c) to be met (see below); but this only applies to a specific kind of electronic signatures.

As with "trustworthy systems", condition (c) seems difficult to technically characterize using standards; audits and case-by-case assessment are more relevant with such requirement.

### 4.2.3 Standards covering other requirements

#### 4.2.3.1 Trusted Lists

The current technical specifications of the EU Member State national trusted lists are defined by CD 2009/767/EC as amended and currently rely on ETSI TS 119 612 v1.1.1.

The technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 are laid down in Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 (OJ L 235, 9.9.2015, p26-36). CID 2015/1505/EU relies on TS 119 612 v2.1.1 for establishing such specifications.

Additional standards (see section 3.2.7 – Table 7) could support the correct management of trusted lists (ensuring interoperability and correct practices for TL managers), but this is actually mostly outside the scope of the implementing acts.

#### 4.2.3.2 QTSPs/QTSs conformity assessment bodies accreditation, assessment report and auditing rules

Considering the work done at the level and by European cooperation for Accreditation (EA), there is a need for adopting Art.20.4 implementing acts to legitimate the EA proposed model for CAB accreditation and QTSs/QTSPs evaluation of conformity as well as to cover the missing part to that model i.e. the applicable “QTS/QTSP audit criteria” as discussed in section 2.2.

# 5. Conclusions – identified gaps

Based on the mapping between the requirements of eIDAS and the analysis of existing standards, it can be concluded that the European Norms will be good candidates for meeting several requirements covered by foreseen implementing acts, at least those regarding compliance with Annex I, III and IV. Some of the standards only cover a part of a requirement – and these parts might also only be covered partly (like requirements for QTSPs providing validation or preservation services). Some others cover a variety of different matters addressed by various eIDAS articles (e.g. new norms EN 319 431 and EN 319 432).

Some of the standards are not yet available and it is still too early to assess them.

Existing standards can be endorsed for being used within the frames of eIDAS Regulation, to the extent presented in the previous sections.

Considering the work done at the level and by European cooperation for Accreditation (EA), It might be considered to adopt in the future the implementing acts set in article 20(4) to legitimate the EA proposed model for CAB accreditation as well as to cover the applicable "QTS/QTSP audit criteria" to be developed in an "outcome based" model as discussed in section 2.2.

The analysis also led, however, to a shortlist of gaps, where specific eIDAS requirement are not yet covered by EU standards (ETSI/CEN/CENELEC).

| **Area of open issue** | **Open standard (draft or even not yet drafted) or description of open issue** |
|---|---|
| QTSPs providing validation services | General requirements on testing compliance and interoperability of signature creation and validation (ETSI TS 119 104) |
| | ISO and ETSI/CEN standards exist for data preservation services. Absence of requirements in the Regulation makes them eligible. |
| QTSP providing preservation services (section 4.2.1.5) | Data preservation services through signing (ETSI EN 319 522) |
| | Policy and security requirements for data preservation service providers (ETSI EN 319 521) |
| | Time-stamping Protection Profile (prCEN/TS 419231) |
| | Secured electronic postal services (SePS) interface specification (Parts A& B, (UPU S43a-4 & S43b-4)) |
| QTSP providing electronic registered delivery service (section 4.2.1.7) | Policy and security requirements for registered electronic mail (REM) service providers (ETSI EN 319 511) |
| | Registered electronic mail (REM) services (ETSI EN 319 512) |
| | Testing compliance and interoperability of REM service providers (ETSI TS 119 514) |

| | |
|---|---|
| | Protection profiles for TSP Cryptographic modules (ETSI EN 419 221, parts 1-5) |
| | Security requirements for trustworthy systems supporting server signing (signature generation services) (ETSI EN 419 241, parts 1-3) |
| QTSP providing certs for website authentication (section 4.2.1.8) | Security requirements for trustworthy systems managing certificates for electronic signatures (EN 419 261) |
| | Generic security standards seem applicable. Further analysis needed for specific TSP's:<br><br>Existing published standards and draft versions are adequate for art. 42(2)<br><br>Reference to *Common Criteria* profiles for timestamping module could be taken into consideration for implementing acts |
| Trustworthy systems and products (section 4.2.2.1) | Conformity assessment for signature creation and validation applications (and procedures)(CEN EN 419 103) |
| QSCD (section 4.2.2.2) | Policy and security requirements for signature creation and validation (ETSI TS 119 101) – under approval |
| Signature validation (section 4.2.2.3) | Profiles for TSPs providing signature validation services (ETSI EN 319 442) |
| | Trusted Lists :<br><br>Testing compliance and interoperability of trusted lists (ETSI TS 119 614)<br><br>Policy and security requirements for trusted lists providers (ETSI TS 119 611) |
| Advanced signatures and seals (section 4.2.2.4) | Trusted Lists :<br><br>Testing compliance and interoperability of trusted lists (ETSI TS 119 614)<br><br>Policy and security requirements for trusted lists providers (ETSI TS 119 611) |
| Others requirements (section 4.2.3) | ETSI EN/TS 319 411-2 (not published yet) |
| **General remarks:** | |
| Qualified certificates for website authentication | No eligible standard |

| | |
|---|---|
| Processes for sending and receiving data | No eligible standard |
| Standard for Advanced Signature | No eligible standard (existing standards address technical validation only) |
| Notification of QSCD | No eligible standard |
| Signature Validation | No eligible standard |

# Annex A: Standards and other documents assessed

## A.1 ETSI/CEN standards

### A.1.1 Area 0 – Framework documents

- TR 119 000 – Framework presentation
- TR 119 001 – Definitions and abreviations

### A.1.2 Area 1 – Signature Creation & validation

- TR 119 100 – Business Guidance
- TS 119 101 – Policy requirements for creation&validation of digital signatures
- EN 419 111 – Protection Profile for signature creation&validation applications
- EN 319 122 – CAdES digital signatures
- EN 319 132 – XAdES digital signatures
- EN 319 142 – PAdES digital signatures
- EN 319 162 – Associated Signature Containers (ASiC)
- TS 103 171 – XAdES profile
- TS 103 172- PAdES profile
- TS 103 173 – CAdES profile
- TS 103 174 – ASiC baseline profile
- EN 319 102-1 – Procedures for creation & validation of AdES digital signatures
- TS 119 172-1 – Signature policies. Part 1 : building blocks and table of contents for human
- EN 419 103 – Conformity assessment for signature creation and validation

### A.1.3 Area 2 – Signatures & other related services

- TR 419 200 – Business guidance
- EN 419 211 – Protection profile for secure signature creation device
- EN 419 221 – Protection profile for TSP cryptographic modules
- EN 419 231 – Protection profile for trustworthy systems supporting time stamping
- EN 419 241 – Security requirements for trustworthy systems supporting server signing
- EN 419 251 - Security requirements for device for authentication
- EN 419 261 – Security requirements for trustworthy systems managing certificates for electronic signatures

### A.1.4 Area 3 – Cryptographic suites

- TR 119 300 – Business guidance on cryptographic suites
- TS 119 312 – Cryptographic suites

### A.1.5 Area 4- TSPs supporting signatures

- TR 119 400 – Business guidance
- EN 319 403 – Requirements for CABs assessing TSPs
- EN 319 401 – TSP policy requirements. General requirements
- EN 319 411-1 – TSPs issuing certificates
- EN 319 411-2 – TSPs issuing qualified certificates
- EN 319 421 – Policy requirements for time-stamping authorities
- EN 319 412 part 1 to part 5 – Certificate profiles

- EN 319 422 – Time-stamp profiles

### A.1.6 Area 5 – Trust Application Service Providers

- TR 119 500 – Business guidance
- SR 019 050 – Study on e-delivery

### A.1.7 Area 6 – TSLs & trusted lists

- TR 119 600 – Business guidance
- TS 119 612 – Trusted lists

## A.2 Other standardization bodies

This is a list of the main documents and specifications coming from different standardization bodies related or affected by the eIDAS regulation. Most of them are indicated in the ETSI/CEN standards as the basis for the specific requirements.

The list is organized by the standardization body.

### A.2.1 ISO

The International Organization for Standardization (ISO) is the world´s largest developer of voluntary international standards. Founded in 1947, has published more than 19500 international standards covering almost all aspects of technology and business.

- ISO 8601:2000 – Date and time format
- ISO/IEC 9798:2010 - Entity authentication
- ISO/IEC 11770:2010 - Key management
- ISO/IEC TR 14516:2002 - Guidelines for the use and management of Trusted Third Party services
- ISO/IEC 14888:2008 - Digital signatures with appendix
- ISO/IEC 15408:2009 - Evaluation criteria for IT security
- ISO/IEC TR 15443:2012 - Security assurance framework
- ISO/IEC 15945:2002 - Specification of TTP services to support the application of digital signatures
- ISO/IEC 16363:2012 – Space data and information transfer systems – audit and certification of trustworthy digital repositories
- ISO/IEC 17065:2012 – Conformity assessment – requirements for bodies certifying products, processes and services
- ISO/IEC 18014:2009 – Information technology – security techniques – timestamping services
- ISO/IEC 19790:2012 - Security requirements for cryptographic modules
- ISO/IEC 20000:2011 – Information technology – service management
- ISO/IEC 24760:2011 - A framework for identity management
- ISO/IEC 27001:2013 - Information security management systems
- ISO/IEC 29115:2013 - Entity authentication assurance framework
- ISO 19005-1 – PDF/A Specification
- ISO 14641-1:2012 – Electronic archiving - Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation. ISO/IEC, 2012.
- ISO 14721:2012 – Space data and information transfer systems - Open archival information system (OAIS) - Reference model. ISO/IEC, 2012.
- ISO 15489-1:2001 – Information and documentation – Records management. ISO/IEC, 2001.
- ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security - Part 1. ISO, 2009.

- ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security - Part 2. ISO, 2008.
- ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security - Part 3. ISO, 2008.

### A.2.2 IETF

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors and researches concerned with the evolution of the Internet architecture. The IETF is an organized activity of the Internet Society (ISOC).

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

- RFC 2251 – Lightweight Directory Access Protocol
- RFC 2528 - Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates
- RFC 2560 – Online Certificate Status Protocol
- RFC 2986 – PKCS#10: Certification Request Syntax specification version 1.7
- RFC 3029 – Internet PKI data validation and certification server protocols
- RFC 3161 – Time-Stamping protocol
- RFC 3494 - Operational Protocols - LDAPv2
- RFC 3628 - Policy Requirements for Time-Stamping Authorities (TSAs)
- RFC 3647 – Certificate policy and certification practices framework
- RFC 3739 – Qualified Certificates Profile
- RFC 4210 - Public Key Infrastructure Certificate Management Protocol (CMP)
- RFC 4523 - LDAPv2 Schema
- RFC 4806 – OCSP extensions to IKEv2
- RFC 5246 – The Transport Layer Security (TLS) protocol version 1.2
- RFC 5280 – Certificate and CRL profile
- RFC 5759 – Suite B Certificate and CRL profile
- RFC 6066 – TLS extensions: Extension definition
- RFC 6239 – Suite B cryptographic suites for secure shell
- RFC 6379 – Suite B cryptographic suites for IPsec
- RFC 6460 – Suite B profile for transport layer security (TLS)
- RFC 6844 – DNS certification Authority Authorization (CAA) resource record
- RFC 6960 – Internet PKI Online Certification Status Protocol - OCSP
- RFC 6961 – TLS multiple certificate status request extension
- RFC 7633 – X.509 v3 Transport Layer Security (TLS) feature extension
- RFC 4998 - Evidence Record Syntax (ERS)

### A.2.3 OASIS

OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS was founded under the name "SGML Open" in 1993. The consortium changed its name to "OASIS" (Organization for the Advancement of Structured Information Standards) in 1998 to reflect an expanded scope of technical work.

OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas. OASIS open

standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

- PKCS 11 TC
  - PKCS#11 Cryptographic Token Interface Base Specification Version 2.40
  - PKCS #11 Cryptographic Token Interface Profiles Version 2.40
  - PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 2.40
  - PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 2.40
- Digital Signature Services TC
  - Digital Signature Services v1.0
  - DSS Core Protocols, Elements, and Bindings v1.0
  - DSS German Signature Law Profile
  - DSS Advanced Electronic Signature Profiles
  - DSS Asynchronous Processing Abstract Profile
  - DSS J2ME Code-Signing Profile
  - DSS Abstract Code-Signing Profile
  - DSS Electronic PostMark (EPM) Profile
  - DSS Entity Seal Profile
  - DSS Signature Gateway Profile
  - DSS XML Timestamping Profile
- Other
  - OASIS, Ed., DSS Core. OASIS, 2007.
  - OASIS, Ed., DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports. 2010.
  - OASIS, Ed., ebXML Messaging Transport Binding for Digital Signature Services. 2008.
  - OASIS, Ed., Visible Signature Profile of the OASIS Digital Signature Services. OASIS, 2009.

### A.2.4 CA/Browser Forum

Organized in 2005, the CA/Browser Forum is a voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing.

- Baseline requirements for the issuance and management of publicly-trusted certificates v 1.3.1 2015.
- EV SSL certificate guidelines v1.5.7 2015.
- EV code signing certificate guidelines, v 1.3, 2014.

### A.2.5 ITU

The International Telecommunication Union (ITU) is the United Nations specialized agency for information and communication technologies – ICTs.

ITU allocates global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide.

ITU was founded in Paris in 1865 as the International Telegraph Union. It took its present name in 1934, and in 1947 became a specialized agency of the United Nations.

- X.501: Information technology – Open Systems Interconnection – The Directory: Models

- X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
- X.519: Information technology – Open Systems Interconnection – The Directory: Protocol specifications
- X.520: Information technology – Open Systems Interconnection – The Directory: Selected attribute types
- X.600-X.699: OSI networking and system aspects
- X.680-X.699: Abstract Syntax Notation One (ASN.1)
- X.680: Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation
- X.681: Information technology – Abstract Syntax Notation One (ASN.1): Information object specification
- X.682: Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification
- X.683: Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications
- X.690: Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- X.691: Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)
- X.692: Information technology – ASN.1 encoding rules: Specification of Encoding Control Notation (ECN)
- X.693: Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)
- X.694: Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1
- X.695: Information technology – ASN.1 encoding rules: Registration and application of PER encoding instructions
- X.696: Information technology – Specification of Octet Encoding Rules (OER)
- X.1200-X.1299: Cyberspace security
- X.1250-X.1279: Identity management
    - X.1250: Baseline capabilities for enhanced global identity management and interoperability
    - X.1251: A framework for user control of digital identity
    - X.1252: Baseline identity management terms and definitions
    - X.1253: Security guidelines for identity management systems
    - X.1254: Entity authentication assurance framework
    - X.1255: Framework for discovery of identity management information
    - X.1275: Guidelines on protection of personally identifiable information in the application of RFID technology
- X.1000-X.1099: Information and network security
- X.1050-X.1069: Security management
    - X.1051: Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
    - X.1052: Information security management framework
    - X.1054: Information technology - Security techniques - Governance of information security
    - X.1055: Risk management and risk profile guidelines for telecommunication organizations
    - X.1056: Security incident management guidelines for telecommunications organizations
    - X.1057: Asset management guidelines in telecommunication organizations

### A.2.6 NIST

- SP 800-38 – Computer security - Cypher modes
- SP 800-53 – Computer security – Assessing security and privacy controls
- SP 800-56 – Computer security – recommendation for pair-wise key-establishment
- SP 800-67 – Computer security – recommendation for triple data encryption
- SP 800-133 – Computer security – Recommendation for cryptographic key generation
- SP 800-150 – computer security – Guide to cyber threat information sharing (draft)
- SP 800-177 – Computer security – trustworthy email (draft)
- FIPS 140-2 – Security requirements for cryptographic modules
- FIPS 180 – Secure Hash Standards
- FIPS 197 – Advanced Encryption Standard
- FIPS 198 – The keyed-hash message authentication code (HMAC)

### A.2.7 ANSI

- X9.95 – Trusted timestamps

### A.2.8 UPU

- S33 – Interoperability framework for postal PKI
- S52 – specifications for postal registered electronic mail

### A.2.9 IEEE

- P1363 – Standards specifications for public-key cryptography

### A.2.10 Others

- "Common Criteria." CCRA Management Committee
- "Spécifications fonctionnelles d'un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps." AFNOR, Jul-2012.
- *EESSI Conformity Assessment Guidance - Part 7 - Cryptographic modules used by Certification Service Providers for signing operations and key generation services*. CEN, 2004.
- *EESSI Conformity Assessment Guidance - Part 2 - Certification Authority services and processes*. CEN, 2004.
- *EESSI Conformity Assessment Guidance - Part 3 - Trustworthy systems managing certificates for electronic signatures*. CEN, 2004.
- *Electronic Signature Verification Application (CC3.1)*. ANSSI, 2011.
- *Electronic Signature Verification Module (CC3.1)*. ANSSI, 2008.
- *Time-stamping System (CC3.1)*. ANSSI, 2008.
- "Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents." 07-Nov-2008.
- *Audit and Certification of Trustworthy Digital Repositories*. CCSDS, 2012.
- *Corps du RGS*. ANSSI, 2014.
- "Exigences spécifiques pour la qualification des prestataires de services de confiance." COFRAC, Jan-2009.
- *Référentiel d'exigences applicables aux prestataires d'audit de la SSI*. ANSSI, 2014.

# Annex B: Abbreviations

| | |
|---|---|
| AdES | Advanced Electronic Signature |
| ASiC | Associated Signature Containers |
| CAB | Conformity Assessment Body |
| CAdES | CMS Advanced Electronic Signature |
| CAR | Conformity Assessment Report |
| CB | Supervisory Body |
| CCSDS | Consultative Committee for Space Data Systems |
| CEN | European Committee for Standardisation |
| CID | Commission Implementing Decision |
| CRL | Certificates Revocation List |
| DVCS | Data Validation and Certification Server |
| EA | European cooperation for Accreditation |
| eCODEX | e-Justice Communication via Online Data Exchange |
| eIDAS | Electronic IDentification And Signature |
| EN | European Norm |
| ESI | Electronic Signatures and Infrastructures |
| ETSI | European Telecommunications Standards Institute |
| ISO | International Organisation for Standardisation |
| ITU | International Telecommunication Union |
| NAB | National Accreditation Body |
| OCSP | Online Certificate Status Protocol |
| PAdES | PDF Advanced Electronic Signature |
| PEPPOL | Pan-European Public Procurement Online |
| PP | Protection Profile |
| QC | Qualified Certificate |
| QESeal | Qualified Electronic Seal |

| | |
|---|---|
| QESig | Qualified Electronic Signature |
| QSCD | Qualified Signature Creation Devices |
| QTS | Qualified Timestamp |
| QTSP | Qualified Trust Service Provider |
| QWAC | Qualified Website Authentication Certificate |
| REM | Registered Electronic Mail |
| SBN | Security Breach Notifications |
| SCC | Sole Control Component |
| SPOCS | Simple Procedures Online for Cross-Border Services |
| STORK | Secure idenTity acrOss boRders linKed |
| TASP | Trust Application Service Providers |
| TR | Technical Report |
| TSA | Time-Stamping Authority |
| TSCM | Trustworthy Signature Creation Module |
| TSP | Trust Service Provider |
| TTP | Trusted Third Party |
| UPU | Universal Postal Union |
| XAdES | XML Advanced Electronic Signature |

## ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

## Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece



Catalogue Number TP-01-15-932-EN-N



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu



ISBN: 978-92-9204-153-3
DOI: 10.2824/540231