Security framework

Guidelines for trust services providers – Part 1

Version 1.0 – December 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

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

Tomas Gustavsson, Primekey

Alexander Wiesmaier, AGT International

Clara Galan, Ministry of Defense, Spain [1]

Sławomir Górniak, ENISA

Contact

For contacting the authors please use sta@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank the numerous experts who reviewed this paper for their contributions. We also thank the following organizations for voluntarily taking part in the survey on security aspects of trust service providers launched by ENISA. The survey was conducted during the months of June and July 2013, 46 respondents from different organisations completed the survey. The list of the organisations taking part in this exercise is available in Annex 4 of this document.

[1] Seconded National Expert at ENISA during the time of the study

Legal notice

Copyright Notice

Executive summary

E-Government services have significant potential to make public services more efficient for the benefit of citizens and businesses in terms of time and money. And while these benefits are increasingly being felt nationally, e-Government services still face administrative and legal barriers on a cross-border level, although pan-European projects like STORK[2] have shown that technical issues of interoperability of electronic identifications can be overcome. In order to remove existing barriers for cross-border e-ID based services the Commission has proposed in June 2012 a draft regulation on electronic identification and trust services for electronic transactions in the internal market [38], which will replace the existing Electronic Signature Directive 1999/93/EC [37]. The main goals of this action are to:

- ensure mutual recognition and acceptance of electronic identification across borders
- give legal effect and mutual recognition to trust services
- enhance current rules on e-signatures
- provide a legal framework for electronic seals, time stamping, electronic document acceptability, electronic delivery and website authentication.
- ensure minimal security level of trust services providers systems
- enforce obligation of notifications about security incidents at trust services providers

In Article 15 of the above mentioned draft regulation the Commission proposes that trust services providers have to demonstrate due diligence, in relation to the identification of risks and adoption of appropriate security practices, and notify competent bodies of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

In this context, the European Union Agency for Network and Information Security (ENISA) developed in 2013 the *Guidelines for trust services providers*, discussing the minimal security levels to be maintained by the trust services providers. The study is split into three parts:

Security framework: describing the framework surrounding trust service providers (TPSs), focusing on EU standards, but taking into account others where relevant.

Risk assessment: discussing the principles and concepts of managing the risks applicaple to TSPs by defining and controlling threats and vulnerabilities.

Mitigating the impact of security incidents: recommending measures to mitigate the impact of security incidents on trust service providers (TSP) by proposing suitable technical and organisational means to handle the security risks posed to the TSP.

All three parts can also be used separately, as they address different issues and target different audience, so the introductory sections overlap.

This document, Part 1: Security framework, describes the framework surrounding trust service providers (TPSs) – the concepts and standards related to operations of a TSP. It focuses on EU standards, but also takes into account others where relevant.

The document specifically outlines security requirements for qualified[3] and non-qualified trust service providers. It references the most important standards and standardization bodies involved in technical specification, as well as certification, auditing and supervision schemes that can be used in order to qualify as a notified trust service provider.

[2] https://www.eid-stork.eu/

[3] which meets the requirements laid down in Annex I of the Directive 1999/93/EC [37]

The document also presents result of a survey[4] conducted by ENISA amongst European trust service providers related to the different aspects.

Finally, the document gives some summary recommendations for TSPs considering standards and auditing schemes, grouped in the following areas:

- Trust service providers in the EU regulatory framework
- Standardization in the area of trust services
- Certification of electronic signature products
- Supervision and audit of trust service providers
- Cryptographic algorithms in certification services

[4] For the in-depth description of the study, please refer to the document "TSP services, standards and risk analysis report", ENISA 2013. The participants are mentioned in the acknowledgements at the beginning of this document.

Table of Contents

Executive summary iv

1 The concept of Trust Service Providers 1

2 Trust service providers in the EU regulatory framework 3

2.1 The concept of certification services in the legal framework 3

2.2 The concept of trust services in the legal framework 4

2.3 The qualification scheme 5

2.4 Security requirements for trust service providers 6

2.5 Specific requirements for qualified certification services 7
2.5.1 Requirements on the trust service provider 8
2.5.2 Requirements for the components of the certification service 9

3 Standardisation in the area of trust services 12

3.1 Organizations involved in the development of standards for certification services 12

3.2 Standards for certificate profiles 13

3.3 Standards for Certification Practice Statements 14

3.4 Standards for trustworthy systems 15

3.5 Standards for secure signature creation devices 16

4 Certification of electronic signature products 17

4.1 Harmonized standards in the area of electronic signatures 17

4.2 Existing certification schemes 18

4.3 Certification of cryptographic modules for TSP signing operations 19

4.4 Certification of secure signature creation devices 20

4.5 Certification of trustworthy systems 21

5 Supervision and audit of trust service providers 22

5.1 Government supervision 22
5.1.1 Under Directive 1999/93/EC 22
5.1.2 Under the proposed Regulation 22

5.2 Independent auditing schemes 23

5.3 Current practices 24

6 Cryptographic algorithms in certification services 26

6.1 Current practices 26
6.1.1 Public key algorithms 26
6.1.2 One way hash functions 28

7 Recommendations 31

7.1 Trust service providers in the EU regulatory framework 31

7.2 Standardization in the area of trust services 31

7.3 Certification of electronic signature products 31

7.4 Supervision and audit of trust service providers 31

7.5 Cryptographic algorithms in certification services 31

Annex 1 – Definitions 32

Annex 2 – Abbreviations 34

Annex 3 – Bibliography 36

Annex 4 – List of organisations taking part in the survey 43

1 The concept of Trust Service Providers

A trust service provider (TSP) is a supplier facilitating electronic security services to customers. The scope of such services includes, but is not limited to, electronic signatures and seals, electronic time stamps, and electronic authentication. Usually, these services rely on electronic certificates issued by certificate service providers (CSP) which is a type of TSP. For the sake of simplicity, we use the CSP as a running example for a TSP within the document at hand. All recommendations apply analogously to other types of TSP as well.

An electronic certificate (or certificate for short) is an electronic document that binds certain pieces of data together and is signed by a trusted third party that vows for the binding. For example, an attribute certificate binds an identity, such as a person, a service, or a device, to certain attributes, such as profession or access rights. Another example is a public key certificate that binds an identity to a public key. This certificate can then be used, amongst others, to verify the identity or signature of the certificate holder. In order to keep things understandable, we use public key certificates as running example throughout this document. All recommendations apply analogously to other types of certificates as well.

Electronic certificates rely on public key cryptography. In public key cryptography, two separate keys, mathematically linked, are provided to an entity. One of the keys is public and can be disseminated, while the other key is private and needs to be under the sole custody of the key pair owner. The private key cannot be derived by sole knowledge of the public key, but one key completes the other in terms of cryptographic operations. For example, a cipher text created using the public key can be decrypted using the private key; equally, the public key can be used to verify signatures that were created by the private key. Because of this property of public key cryptography, and by ensuring the secrecy of the private key and the authenticity of the public key, a relying party can verify that an entity presenting a certificate is who it claims to be or that a signature is valid.

However, a third party is needed to ensure that the information contained in the certificate, including the public key, is actually linked to the real identity of the entity. This is done by a TSP, which uses its so-called certificate authority (CA) signing keys to sign the entities' certificates. With this operation the TSP attests that the certificate was issued to the entity whose information is contained in it. Hence, we distinguish between two different types of certificates:

- Subject certificates, also called end entity certificates, that are used for day to day tasks such as authentication, signatures, or encryption. The holder of such a certificate is called the subject.
- CA signing certificates that are used to sign other certificates. Apart from signing subject certificates, CA certificates are often also used to sign other CA certificates to establish a trust relationship between CAs.

Electronic certificates can be used for a variety of purposes, some of the most common being to support electronic signatures, electronic seals or website authentication. Electronic signatures or seals are meant for natural persons (signatures) or legal entities (seals) to be able to produce digital signatures on documents or messages in order to ensure:

- The integrity of the document or message: attest that the document or message has not been altered.
- The authenticity and non-repudiation: attest that the document or message was produced by the certificate owner.

In the context of authentication, when an entity A presents itself to another entity B with its electronic certificate, entity B can verify that the entity A is actually who it claims to be by checking that entity A is in possession of the private key associated with the public key included in the certificate.

In the case of encryption, electronic certificates can also be used to provide confidentiality. The use of public key cryptography for the exchange of session keys ensures the confidentiality of the communication. Here, the session key is the entity that carries out the encryption of the messages.

The service of Certificate Service Providers can be broken down into the following component services

- Registration service: verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.
- Certificate generation service: creates and signs certificates based on the identity and other attributes verified by the registration service.
- Dissemination service: disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the CA's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- Revocation management service: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.
- Revocation status service: provides certificate revocation status information to relying parties. This may be based upon certificate revocation lists or a real time service which provides status information on an individual basis. The status information may be updated on a regular basis and hence may not reflect the current status of the certificate.

and optionally:

- Subject device provision service: prepares and provides a signature-creation device to subjects.

2 Trust service providers in the EU regulatory framework

2.1 The concept of certification services in the legal framework

The main legal text addressing the area of electronic certification services in the EU is the Directive 1999/93/EC on a Community framework for electronic signatures [37]. The objective of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition.

The Directive defines a 'certification service provider' as an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures, while 'certificate' is defined as an electronic attestation which links signature-verification data to a person and confirms the identity of that person. This definition stresses the fact that the scope of the current regulatory framework is limited to certificates for electronic signatures. Providers of other types of certificates, or complementary services related to electronic certificates but not oriented to electronic signatures, are not regulated by the provisions set by the Directive.

This limitation in scope is about to change, as the current Directive is expected to be superseded by a new Regulation on electronic identification and trust services for electronic transactions in the internal market [38], which was presented as a proposal in July 2012. The proposal introduces some important changes in the reach of the services covered. It extends the concept of certification services further from electronic signatures to any type of electronic certificates.

In June and July 2013 ENISA conducted a survey among trust services providers, in which 46 participants took part. Its goal was to identify security practices in force at these organisations[5]. The results show that a majority of the EU providers participating in the survey already issue these other types of certificates. While 95% of the respondents report issuing certificates for individuals, making it the most common type of service, 80% of participants also report issuing certificates for web site authentication. Certificates for legal entities are also issued by 80% of the respondents.

Additionally, 33% of respondents reported issuing other types of certificates. Among the most cited types were:

- Code signing certificates, used to verify the integrity and authenticity of software programs;
- Server certificates, used for automated signing operations by computer servers;
- Device certificates, used for the authentication of devices;
- Issuing CA certificates, used for generating intermediate CAs (CAs which issue certificates to end users) from a root CA;

[5] For the in-depth description of the study, please refer to the document "TSP services, standards and risk analysis report", ENISA 2013. The participants are mentioned in the acknowledgements at the beginning of this document.

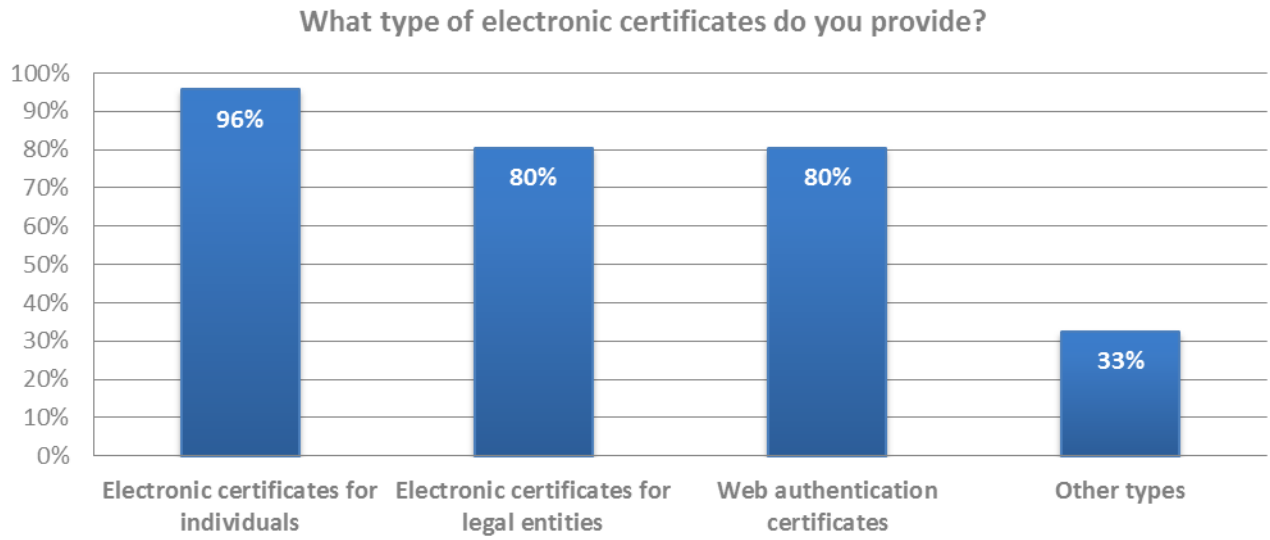

Figure 1: Types of provided electronic certificates

2.2 The concept of trust services in the legal framework

In order to achieve a common nomenclature for all services related to electronic certificates issuance and added services, the proposal introduces the new concept of trust services, which are defined as any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.

In the new framework, certification services providers become a type of trust service providers. ENISA's survey on security practices of trust service providers shows that a majority of the EU providers participating in the survey, 85%, already provide other services, such as time stamps or long term signature preservation, in addition to pure certification services.

Trust service providers can be located both within the EU and outside of EU. How some of the EU specific terms are to be interpreted for non EU located TSPs is not defined.

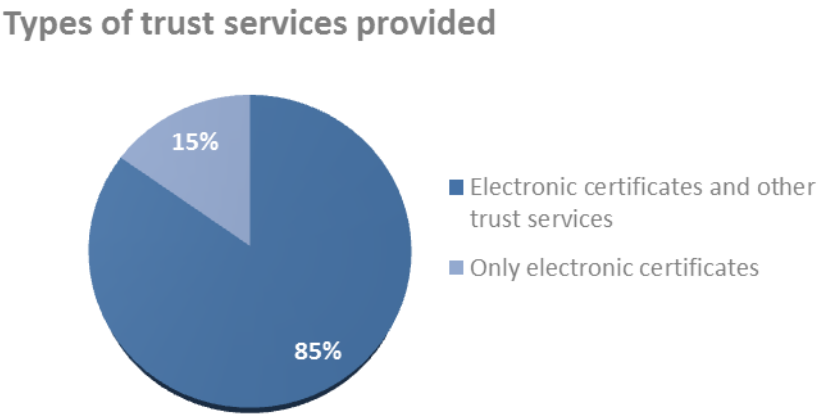

Figure 2: Types of trust services provided

2.3 The qualification scheme

The Directive 1999/93/EC [37] introduced the concept of qualification of electronic signatures. The main objective of the qualification scheme is to establish a certain set of requirements for an electronic signature that, when conforming to it, would make the signature "satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based" and "admissible as evidence in legal proceedings".

It shall be noted, however, that the fact that an electronic signature isg non-qualified does not invalidate the electronic signature. The difference lies in the fact that an electronic signature under the qualification scheme will have a presumption of legal validity, while, for others, the univocal link between the signatory and the signature, and the integrity of the signature, may have to be demonstrated. The exact legal consequences however differ between member states because the Directive had to be transposed to every member states national legislation.

The introduction of the qualification concept in the European legislation gave a legal foundation to electronic signatures. This stimulated the European market of electronic certificates, where trust service providers started to issue qualified certificates that could be used by EU citizens, especially in their relationships with public administrations. As a result, many European providers issue qualified certificates for electronic signatures nowadays, although there are large differences between member states. ENISA's survey on security practices of trust service providers shows that a majority of the EU providers participating in the survey, 93%, issue qualified certificates.

However, the restriction of the scope of the qualification scheme to electronic signatures, combined with the practice of most European providers of issuing several types of certificates, has prompted as the most common practice to issue both qualified and non-qualified certificates, with 80% of the respondents following this practice. Only 13% issue exclusively qualified certificates, while another 7% issue exclusively non-qualified certificates. These later group is mainly composed of providers focused on web authentication certificates used for TLS/SSL connections in internet.

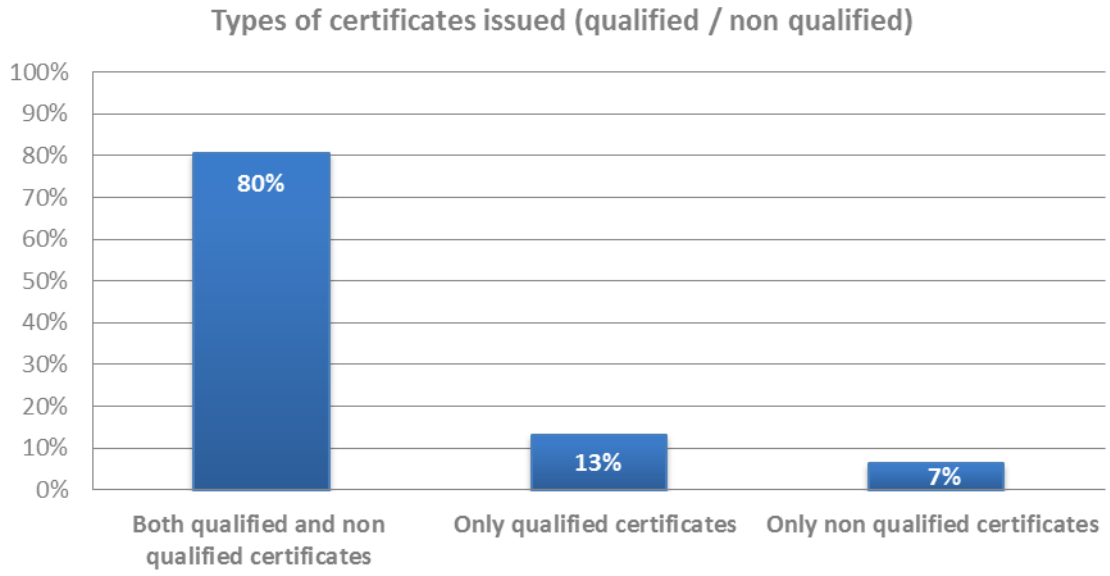

Figure 3: Provision of qualified certificates

This double schema may have come as a burden for providers, which may be subject to government supervision to issue qualified certificates, but that can apply this qualification only for electronic signature certificates. They must follow a set of restrictive requirements for qualified certificates and may not be able to leverage this supervision for other trust services they may provide in the same conditions and subject to the same security requirements.

This issue has been addressed by the new proposal for a Regulation, which, in the same way it extends the scope of the certification services, extends the possibility of qualification to other types of certificates. Specifically three types are contemplated:

- Qualified certificate for electronic signature.
- Qualified certificate for electronic seal.
- Qualified certificate for website authentication.

In the new framework, a qualified electronic signature, aimed at natural persons, "shall have the legal effect of a handwritten signature". This definition is very similar to that existing in the current Directive. A qualified electronic seal, aimed at legal entities, "shall enjoy the legal presumption of ensuring the origin and integrity of the data to which it is linked". Qualified website authentication certificates, aimed at web domains, are meant to "be an attestation which makes it possible to authenticate a website and links the website to the entity to whom the certificate is issued".

Aside from introducing new types of qualified certificates, the proposal also foresees the existence of other qualified trust services, which are derived from the use of electronic certificates: electronic time stamps, qualified electronic delivery services, qualified validation service for qualified electronic signatures and qualified electronic signature preservation services. The ENISA study focuses in more detail on the security aspects of these new types of trust services that are foreseen in the new Proposal.

2.4 Security requirements for trust service providers

Directive 1999/93/EC didn't introduce any general security requirements applicable to all providers, regardless of the type of certificates they issue, requirements were only set for providers of qualified certificates for electronic signatures. However, the maturity of the market has proved that electronic certificates, whether they are used for binding signatures with legal presumption, or for securing private electronic communications and transactions in the Internet, need to be provided and maintained within a secure environment to protect the sensitive operations they are employed for.

In this context, the new proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market has introduced a specific provision addressing the security of trust services, which are applicable to all providers. These provisions are compiled in Article 15. Article 15 establishes that all providers must:

- Take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.
- Introduce measures to ensure that the level of security is appropriate to the degree of risk.
- Take measures to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents.

All providers are required in the new framework to conduct a risk assessment exercise on their services, to implement the appropriate security measures to minimize the possibility of incidents taking place, and to have in place the adequate measures to respond and manage possible incidents.

As ENISA's survey on security practices of trust service providers shows, a majority of the EU providers participating in the survey already apply measures for these purposes. 96% of respondents report having an approved information security policy. Conducting a formal risk assessment is not so systematic yet, however 72% report having a business risk assessment document. Regarding the management of incidents and continuity of operations, 83% declare having an incident response plan and 80% a business continuity plan.

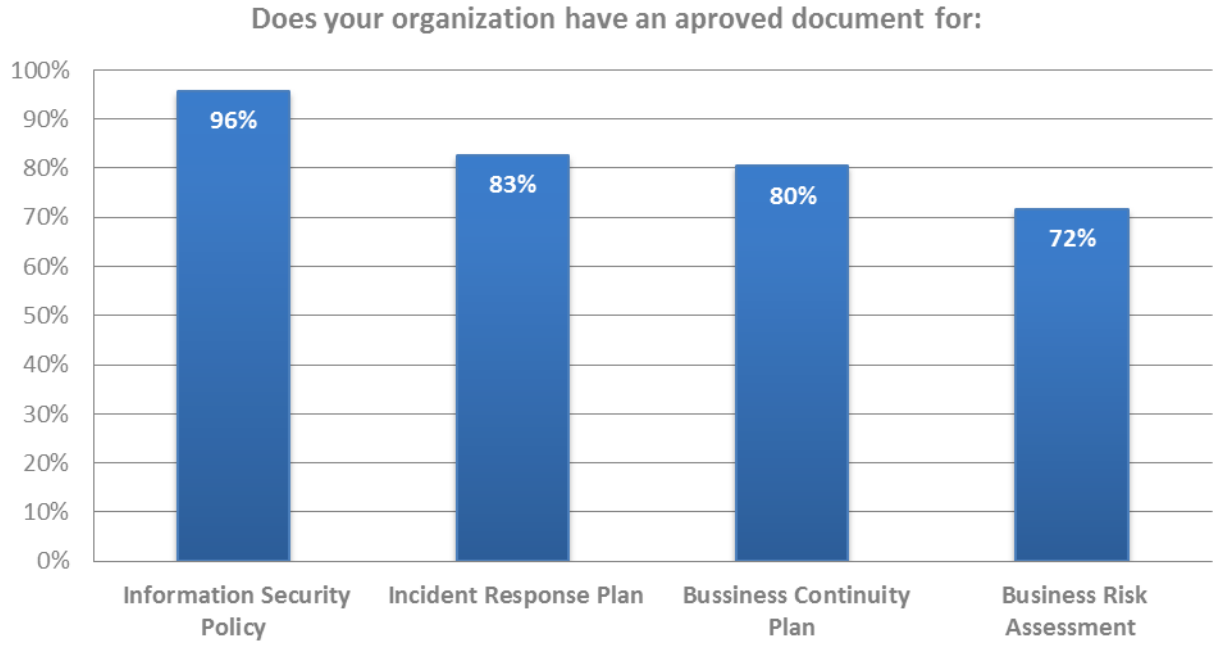

Figure 4: Security documents

Besides those security requirements, Article 15 also foresees that trust service providers must, without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

The topic of breach notifications in trust service providers has been approached in more detail in the ENISA report "Implementation of Art 15: Security breaches notifications in trust services"[6].

2.5 Specific requirements for qualified certification services

Requirements for the different components of a qualified certification service were extensively found in different sections of the Directive 1999/93/EC. These requirements concern both technological measures to guarantee the confidentiality and integrity of the signature creation data, as well as contractual and legal issues for the provider.

All the requirements for the components of a certification service derive from the requisite set for an electronic signature to be considered qualified. A qualified electronic signature must be:

- An advanced electronic signature
- Created with a secure signature creation device

[6] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/implementation-of-article-15

- Based on a qualified certificate issued by a trust service provider.

In the new Proposal, requirements for qualified electronic signatures or seals are analogous to the ones present in the current Directive. For a web authentication certificate to be qualified it must be issued by a qualified trust service provider and based on qualified certificates for website authentication.

The following sections describe in detail what are the requirements set in the current and proposed framework for a provider to be accredited as qualified, as well as for the certification components to fulfill the provisions set for them.

2.5.1 Requirements on the trust service provider

Qualified certificates can only be provided by qualified certificate providers. Therefore the first stage for a trust service provider to issue qualified certificates is to become a qualified trust service provider. The requirements for qualified trust service providers are laid down in the Article 19 of the new Proposal, and concern the following aspects:

Reliability in the service: Qualified trust service providers must demonstrate reliability for providing the service. They must implement adequate policies and procedures which are in line with current standards, and employ qualified and trained personnel with sufficient knowledge on the area of electronic signatures and security procedures.

Proper establishment of contractual relationships: Qualified trust service providers must inform individuals, before entering a contractual relationship with them, of the terms and conditions applicable to the service. This information should include the use of the certificate, including any limitations, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement.

Subject registration: Qualified trust service providers must verify, in accordance with national law, the identity of the subject to whom the certificate is issued. Directive 1999/93/EC didn't specify how this verification of identity needs to be done, for example, if registration through electronic means is possible. The new Proposal clarifies how the registration can be conducted:

1. By physical presence of the subject.
2. Remotely, using an identification means under a notified scheme that was issued through physical presence.

The possibility of identifying the subject electronically, by means, for example, of the use of a national electronic identity card is opened.

Use of trustworthy systems: Qualified trust service providers are required to use trustworthy systems which are protected against modification and ensure the technical and cryptographic security of the process supported by them. The Directive establishes that trustworthy systems that store certificates must meet these requirements:

- Only authorised persons can make entries and changes.
- Information can be checked for authenticity.
- Any technical changes compromising these security requirements are apparent to the operator.
- Certificates are publicly available for retrieval in only those cases for which the certificate holder's consent has been obtained, and depending on member states' data protection laws.

The requirements for trustworthy systems set in Article 19 are similar to those established in the Directive 1999/93/EC, with two variations. The first is that the new framework only foresees that

trustworthy systems need to ensure the reliability, not the cryptographic security, of the processes supported by them. This acknowledges the fact that the possible vulnerabilities that may appear in algorithms considered secure until a certain moment are outside the control of the provider. The second change is that in the new framework the requirements set for the systems storing certificates are extended to all systems storing the information provided to the CSP.

Liability: Qualified trust service providers are required to maintain financial resources to operate under the obligations laid down in the regulations and to be able to bear the risk of liability when failure to comply results in damages for a certificate subject.

Accountability: Qualified trust service providers must keep records and logs of all relevant events concerning the certificate life cycle, and record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

Confidentiality and integrity: Qualified trust service providers must take measures against forgery of certificates to ensure their integrity. The current framework establishes that they must not store a copy of the signatory signature creation data of the certificate subjects. In the cases where the provider generates the signature creation data for the subject, it must ensure the confidentiality of this data when delivering them to the individual. The provider should not be in possession of the subject's private key, which must be under the sole custody of the certificate holder.

However this provision is not included in the new framework, as the possibility of providers to store the signature creation data (for primary or back up purposes) on behalf of the certificate subject is opened, as long it is done with the appropriate level of security.

Revocation status information: Qualified trust service providers must ensure the operation of a secure and prompt security directory and an immediate revocation service, as well as the precision and availability of the certificate issuing and revocation times.

ETSI [11] defines a time limit for providers issuing qualified certificates to process the revocation of the certificate within 24 hours. ENISA's survey on security practices of trust service providers shows that, among EU trust service providers participating in the survey, 40% report that 5 minutes is the maximum latency they guarantee for including the revocation of a certificate in the certificate database after such revocation has taken effect, however 23% report one day latency, with the rest providing intermediate latencies. The responses however do not differ between technically updating the revocation database and the complete process of revocation, so answers may not be comparable.

Termination: Providers need to have in place an up-to-date termination plan to ensure continuity of service in accordance with arrangements issued by the supervisory body. ENISA's survey on security practices of trust service providers shows that, among trust service providers participating in the survey shows that 75% of providers already have an approved CA Termination Plan.

2.5.2 Requirements for the components of the certification service

Qualified certificate profiles

A requirement set by the Directive 1999/93/EC [37] for an electronic signature to be considered qualified is that such a signature be based on a qualified certificate. A qualified certificate is an electronic certificate issued by a certificate provider that contains a minimum set of information which is described in the Annex I of the Directive. These data include:

- Indication that the certificate is issued as a Qualified Certificate
- Identification of the provider and the state where it is established

- Name or pseudonym of the signatory, and if applicable, specific attributes used in the certificate
- Identity code and validity period of the certificate
- Signature verification data
- Advanced electronic signature of the trust service provider issuing the certificate
- Limitations on the scope and value of transactions to be performed by the certificate, if applicable

In the new Proposal, requirements for a qualified certificate are similar to those set in the Directive 1999/93/EC, with the introduction of some additional compulsory information, which are meant to facilitate the verification of the status of the certificate and the provider:

1. Indication of the location where the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider is available.
2. Indication of the location of the certificate validity status services that can be used to enquire about the validity status of the qualified certificate.
3. If the electronic signature creation data are located in a qualified electronic signature creation device, an indication of this.

Additionally, the new framework also defines qualified certificates requirements for electronic seals in its Annex III, which are analogous to those for certificates for electronic signatures; with some adaptions for electronic seal certificates being conceived for legal entities.

The requirements for certificates for website authentication are similar to those for qualified certificates for electronic signatures and seals, with some differences, for example the certificate must include the domain name operated by the legal entity to whom the certificate is issued. Also, due to their nature, there is no provision for information regarding electronic signature validation data or signature creation device.

Advanced electronic signature

The Directive 1999/93/EC determines that qualified electronic signatures are advanced electronic signatures created with a secure signature creation device. Within the current Directive, an advanced electronic signature is an electronic signature which fulfils these requirements:

- Is uniquely linked to the signatory
- Capable of identifying him/her
- Created using means that the signatory can maintain under his/her sole control
- Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

The requirements set in the Proposal for an electronic signature to be considered advanced are similar to those set in the previous the Directive 1999/93/EC. The only variation related to it is that while in the current Directive the signature needs to be created using electronic signature creation data that the signatory can maintain under his/her sole control, in the new Regulation the requirement specifies can maintain under his/her sole control “with a high level of confidence”, acknowledging the fact that there may some vulnerabilities that are outside the control of the certificate subject or the provider.

Secure signature creation device

The other requirement set by Directive 1999/93/EC for an electronic signature to be considered qualified is to be created in a secure signature creation device. Secure signature creation devices are configured software or hardware that is used to implement the signature process with the signature

data. They must ensure that the signature has been produced with the subject private key and implement measures to guarantee its confidentiality.

The conditions for a signature creation device to be considered secure are set in the annex III of the Directive 1999/93/EC:

- Ensure that the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured.
- Ensure that the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology.
- Ensure that the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
- Not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

In the new proposal, the requirements for signature creation devices to be qualified are similar to those established in the Directive 1999/93/EC for secure signature creation devices, with some variations which concern mainly the handling of the signature creation data, including the key pair, by the provider in behalf of the certificate subject. This possibility, which was not foreseen by the Directive, is opened both for the managing of the keys themselves, as for back up purposes:

1. Generation or managing of the signature creation data by the provider can be done by qualified trust service providers.
2. The provider may keep a backup copy of the signature creation data on behalf of the signatory, provided that the duplicated data sets are subject to the same level of security and that they are the minimum necessary to ensure the continuity of the service.

As noted before there are no provisions for secure signature devices for website authentication certificates.

3 Standardisation in the area of trust services

Standards are specifications, adopted or created by a standardisation organization or user group, for repeated or continuous application, with which compliance is not compulsory. The field of trust services has produced several standards and technical specifications. One reason for the existence of a large set of standards and technical specifications in the field of trust services is a high need for interoperability and assurance, as trust services are meant to add security in the exchange of information between different organizations and individuals.

Regulations in the area of trust services have also provided a high level of detail in terms of security requirements of the services, especially due to the qualification scheme, and several of the standards that have been created are oriented to offer guidance regarding compliance with the regulations. But even for providers outside the compliance scope, standards have helped them to obtain guidance in order to ensure the service is delivered with the appropriate level of assurance in an international context.

Standards are always evolving, and the standards referenced in this chapter may be superseded by updated standards from time to time.

The European Interoperability Framework (EIF) [51] is a set of recommendations which specify how Administrations, Businesses and Citizens communicate with each other within the EU and across member states borders. The goal is to provide a framework to enable interoperability and reuse leading to improved public service delivery and lower cost.

The EIF recommends some basic principles regarding use of standards, such as that the use of ICT should create equal opportunities for all citizens and businesses through inclusive services that are publicly accessible without discrimination. Bearing this in mind it is important for TSPs operating under the Directive, and the new proposal, to have a good understanding on standards relevant for the field.

3.1 Organizations involved in the development of standards for certification services

Several bodies have been involved in the creation of standards for certification services. One of the first to develop the area of certification services was the International Telecommunication Union (ITU) with the X.509 framework, which has been universally adopted as the standard for public key infrastructures. Subsequently, several organizations, both at the international and European level, have undertaken the task of developing standards in this area:

- The European Telecommunications Standards Institute (ETSI) has produced several standards to support the implementation of the European legislation in the area of trust services, as well as to promote the adoption of international and industry standards in Europe. Within ETSI, the ESI technical committee is in charge of producing technical specifications in the area of trust services.
- The European Committee for Standardisation (CEN) has produced a series of technical recommendations in the form of CEN Workshop Agreements (CWAs) in the area of products for electronic signatures, some of which have become harmonized European standards.
- The Internet Engineering Task Force (IETF) is an independent organization that produces technical specifications, denominated Requests for Comments (RFCs), that have been widely adopted as industry standards in several IT technology fields. In the area of certification services IETF has produced several specifications that are widely employed and that have been adapted by European standardization bodies to be used in European market.

The ENISA survey on security practices of trust service providers shows that a majority of the EU providers participating in the study are following standards from these three organizations. The figure below shows that ETSI standards are, with 89% of responses, the most employed, probably because they provide guidance for providers of qualified certificates, which most European trust service providers issue. Nevertheless, IETF standards are also widely used, by 84% of the providers, due to these standards being the most followed in the field internationally. Finally 80,4% of respondents either employ a CEN standard, or more commonly, use products certified against a CEN Workshop Agreement, as CEN standards are more focused on products.

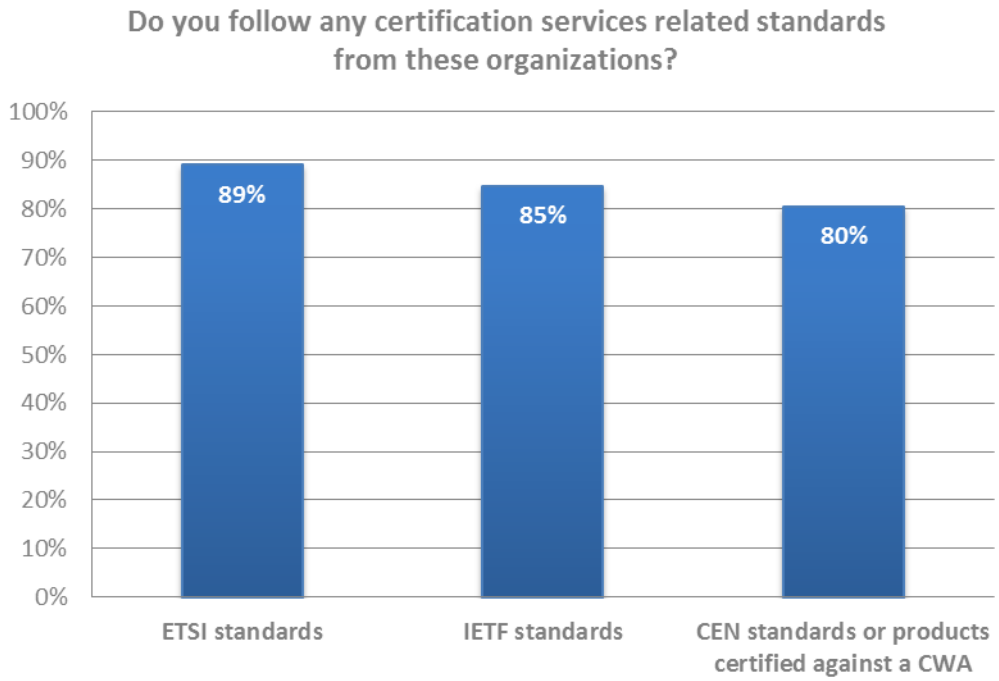

Figure 5: Use of certification services related standards

3.2 Standards for certificate profiles

Certificate profiles define the formats and fields that certificates must contain in order to be interoperable and readable by all participating parties. The basis for defining the complete framework on public key infrastructures, including the formats for electronic certificates is the *ITU-T Recommendation X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*. This recommendation, adopted as an international standard by ISO/IEC 9594-8:2008 [5], has been widely accepted as a standard for formats for public key certificates, among others components of a public key infrastructure.

Based on the X.509 framework, the most widely employed standard for the definition of an electronic certificate profile is the IETF technical specification *RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [22]*. RFC 5280 profiles the X.509 v3 certificate and X.509 v2 certificate revocation list for use in the Internet.

For qualified certificates, the ETSI European Norm *EN 319 412-5 Qualified Certificate profil[11e]* defines, based on the technical specifications of the IETF, the format of qualified certificates complying with the Directive 1999/93/EC.

Another ETSI technical specification, *TS 119 412-2 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons[11b]* defines a common profile dependant on the IETF standards for

implementation of X.509 V.3 and the ETSI standard TS 101 862 (EN 319 412-5) [11e] , to allow actual interoperability of certificates.

The CA and Browser Forum (CA/B Forum) is an organization of public Certificate Authorities and browser vendors. The CA/B Forum establishes guidelines and requirements for web server certificates on the Internet. If the CSP issues certificates for web servers the CA/B Forum requirements[7] define many properties for web server certificates.

3.3 Standards for Certification Practice Statements

In order to document and make available to its customers all the policies and procedures that a trust service provider follows, two standardized document formats have been created: the Certificate Policy and the Certification Practice Statement. These documents provide to users essential information regarding aspects such as contractual issues and the security practices of the provider. These two standards are widely used to obtain guidelines in the elaboration of these documents for any trust service provider, issuing qualified or not qualified certificates:

At the international level, The IETF technical specification *RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [23]* provides a framework to assist the writers and users of certificate policies or certification practice statements in drafting and understanding these documents.

At a European level, the *ETSI standard TS 102 042 Policy requirements for certification authorities issuing public key certificate [16]* defines policy requirements on the operation and management practices of certification services providers such that users and relying parties may have confidence in the applicability of the certificate in support of cryptographic mechanisms.

Regarding providers of qualified certificates, the most widely used standard is the ETSI standard *TS 101 456 Policy requirements for certification authorities issuing qualified certificates [12]*. TS 101 456 defines policy requirements on the operation and management practices of certification authorities similar to those of TS 102 042 but meant to comply with the provisions set in the Directive 1999/93/EC. To support the implementation of TS 101 456, ETSI also produced the technical specification *TR 102 437 Guidance on TS 101 456* which provides guidelines on interpreting the TS 101 456 requirements.

All these standards are widely followed by European providers. ENISA's survey on security practices of trust service providers shows that among trust service providers participating in the survey, 84,8% of respondents reported following RFC 3647, 80,4% ETSI 101 456 and 54,3% ETSI TS 102 042.

[7] https://www.cabforum.org/

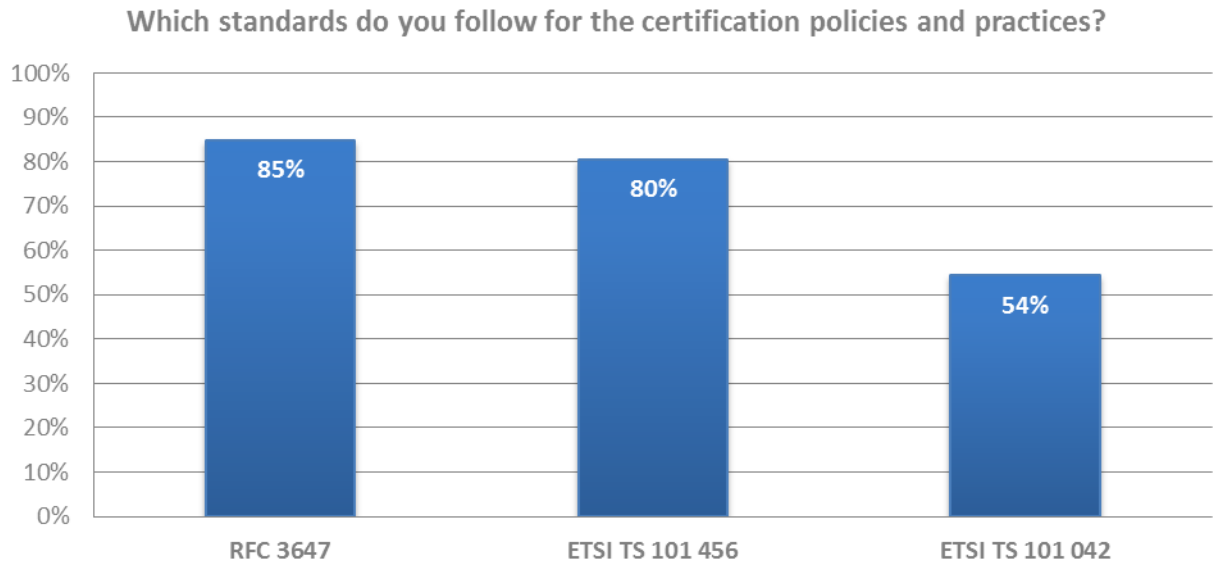

Figure 6: Use of standards for certification policies and practices

When results are combined, results show that 98,8% followed at least one of the three standards (RFC 3647, ETSI TS 101 456 or ETSI TS 102 042), with 45,7% of the survey participants reporting following the three of them.

The ETSI Policy Requirement standards are currently in the process of being updated.

3.4 Standards for trustworthy systems

The Directive 1999/93/EC defined the concept of trustworthy systems. These systems are to be used internally by the CSP in the operations for the certificate lifecycle management, especially regarding the CA signing key usage.

To address the security requirements of trustworthy systems, CEN produced the workshop agreement *CWA 14167 Security requirements for trustworthy systems managing certificates for electronic signatures*. CWA 14167 is divided in four parts, the first one addressing systems security requirements, and the other three parts addressing the security of the cryptographic module used for CSP key generation services:

1. CWA 14167-1 Part 1: System Security Requirements [26a]
2. CWA 14167-2 Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP) [26b]
3. CWA 14167-3 Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP) [26c]
4. CWA 14167-4 Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP [26d]

The CWA 14167-1 and the CWA 14167-2 have been adopted as harmonized standard Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC.

These standards are in the process of being updated at the time of writing this document.

3.5 Standards for secure signature creation devices

Secure signature creation devices are configured software or hardware that is used to implement the signature process with the signature data. They manage the cryptographic operations performed with the subject key pair, and as such they must have comprehensive security properties.

The main technical specification for the security aspects of the signature creation devices for providers of qualified certificates is the CEN workshop agreement *CWA 14169 Secure Signature-creation devices [27]*.

CWA 14169 has been adopted as a harmonized standard Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament.

Other standards have been created to support the CWA 14169. The CEN workshop agreement, *CWA 14170 Security requirements for signature creation applications* [29] specifies security requirements and recommendations for signature creation applications that generate advanced electronic signatures by means of a hardware signature creation device.

Additionally, to facilitate the implementation of secure signature creation devices in different platforms, the CEN workshop agreement *CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices* [28] gives guidance on the implementation of secure signature creation devices Protection Profiles (SSCD PPs) for specific platforms (e.g. smart cards, personal data assistants, mobile phones, or PCs), and the operation in specific environments (e.g. public terminals or secured environments).

In the case the secure signature creation device platform is a smart card, *the CWA 14890 Application Interface for smart cards used as Secure Signature Creation Devices* [30] (divided in two parts CWA 14890-1 and 14890-2) specifies the application interface to smart cards used as secure signature creation devices.

In the case of software based signature creation devices, the *CWA 14365-2 Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices* provides a Protection Profile (PP), based on the Common Criteria, for signature creation devices suitable for general electronic signatures, which can be used for providers of non-qualified signatures.

These standards are in the process of being updated at the time of writing this document.

4 Certification of electronic signature products

Proof of compliance with standards and technical specifications can be achieved by obtaining a certificate of compliance. Certification is defined as the process by which a product or process is awarded a conformity certificate after undergoing a conformity assessment process, usually conformity against a regulation, a standard or a technical specification.

Providers or products often get certified in order to comply with regulations, although this is not the sole driving force for certification. Within the European Union, the certification framework for products follows a general certification scheme set in the Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products. Under this scheme, each member state must designate an Accreditation Body, which itself accredits certification bodies which are competent to conduct conformity assessments[8]. The use of accreditation varies among member states.

In this European product certification framework, conformity assessment is conducted against harmonised standards. A harmonized standard is a standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation. Products which are in conformity with harmonised standards which have been published in the Official Journal of the European Union are to be presumed to be in conformity with the requirements covered by those standards set out in the corresponding regulations.

4.1 Standards in the area of electronic signatures

Regarding products to be employed in electronic certification services, the Commission issued the Decision 2003/511/EC on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC, which set the following standards:

1. Recognised standards for trustworthy systems:
    a. CWA 14167-1 (March 2003): security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System Security Requirements [26a]
    b. CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures - Part 2: cryptographic module for CSP signing operations - Protection Profile (MCSO-PP) [26b]
2. Recognised standards for secure signature creation products:
    a. CWA 14169 (March 2004, update foreseen in December 2013): Secure Signature-creation devices [27]

Further, from the publication of recognized standards against which manufactures of electronic signature products may become certified, an additional requirement was introduced for secure signature creation devices. The Directive established that the conformity of these devices shall be determined by appropriate public or private bodies designated by member states, and that the criteria for member states to determine whether a body should be designated should be produced.

The criteria were set by the Commission Decision 2000/709/EC on the minimum criteria to be taken into account by member states when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for

[8] This scheme currently does not apply to product certification within the scope of the draft regulation [38]. Another scheme under consideration is the informal SOG-IS MRA, http://www.sogisportal.eu/uk/mra_en.html.

electronic signatures. The names of these notified bodies able to assess conformity with the requirements for secure signature creation devices need to be made available to all member states; and the certifications they issue recognised by all member states.

Currently the Protection Profiles are not adapted to the latest version of Common Criteria. These standards will be updated for the new proposal.

4.2 Existing certification schemes

Conformity assessment of products performing cryptographic operations has been foreseen by the European legislation to be assessed within the Common Criteria framework for information technology security evaluation. The Common Criteria is a multilateral agreement for mutual recognition of ICT security products certifications, and has been adopted as an international standard by the *ISO/IEC 15408 Series: Information technology, Security techniques, Evaluation criteria for IT security* [9].

In the Common Criteria framework [42], certification candidates choose a Protection Profile for the evaluation. Different protection profiles exist for different ICT products. The CWA 14167 [26] defines profiles for cryptographic modules for CSP signing operations, while the CWA 14169 [27] does the same for secure signature creation devices. Common Criteria evaluations can be conducted in different levels of depth, denominated Evaluation Assurance Levels (EAL), which rank from 1 to 7. In the case of the CWA 14169, the specified Evaluation Assurance Levels (EAL) is EAL 4+.

Aside from the European certification framework, the American certification scheme, the Federal Information Processing Standards (FIPS) by the National Information Standardization Institute (NIST) are relatively widely used by European providers. In the case of products for electronic signatures, the Federal Information Processing Standard NIST FIPS 140-2 [36] on requirements for cryptographic modules is used to accredit cryptographic modules. Similarly to the EAL level in Common Criteria, NIST FIPS 140-2 establishes four security levels regarding the deep of security testing that a product must undergo.

The main reason for the use of FIPS certified products among European trust service providers is the higher availability of FIPS certified products versus Common Criteria products for some components. Some European countries accept FIPS certifications for electronic signature products as equivalent to Common Criteria certified. The ENISA survey shows that 89% of respondents report using at least some product with a NIST FIPS certification, while 80% of use at least one Common Criteria certified product.

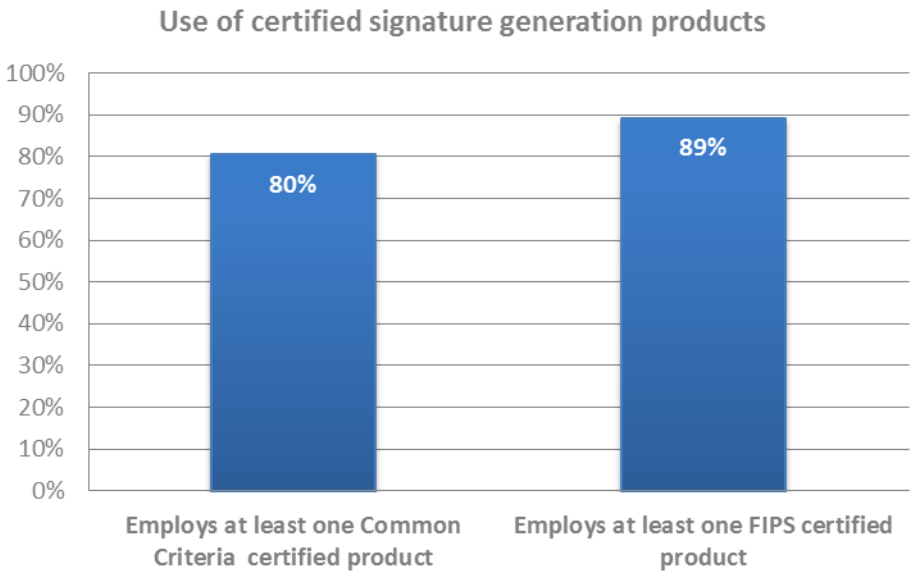

Figure 7: Use of certified signature generation products

4.3 Certification of cryptographic modules for TSP signing operations

Cryptographic modules for TSP signing operations are hardware devices that manage the cryptographic operations performed with the keys of a Certification Authority. Trust service providers must ensure the confidentiality and integrity of the key pairs that their CAs use to sign the certificates they issue. This is a critical component in the chain of trust that a CSP must protect.

This confidentiality and integrity is achieved by the use of devices with strict anti-tampering properties, widely known as Hardware Security Modules (HSMs). HSMs are employed for the protection of cryptographic keys, and, although not exclusively meant for public key cryptography, this is one of their main applications. HSMs are capable of performing cryptographic operations, such as CA key pair usage for signing user certificates. The keys don't exit the HSM and are protected from unauthorized access.

In the European framework, the CEN standard CWA 14167 [26] defines Common Criteria protection profiles for cryptographic modules for CSP signing operations:

1. CWA 14167-2 Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)
2. CWA 14167-3 Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)
3. CWA 14167-4 Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP

The CWA 14167-2 was adopted as a recognized standard against which certification presumes the product to be compliant with EU regulations.

Currently the Protection Profiles are not adapted to the new version of Common Criteria. These standards are in the process of being updated for the new proposal.

Aside from the European framework, NIST FIPS 140-2 [36] certified products are common among HSMs used by European trust service providers, which can be explained due to the wider availability of these products on the market. The ENISA survey shows that 87% of respondents report using products having a NIST FIPS 140-2 certification. Only slightly more than half, 53%, of used products

have a CWA 14167-2 Common Criteria certification. However, as the graphic shows, it is becoming regularly more common for manufacturers to achieve both certifications to adapt both the European and American markets, and already 40% of the products do hold both.

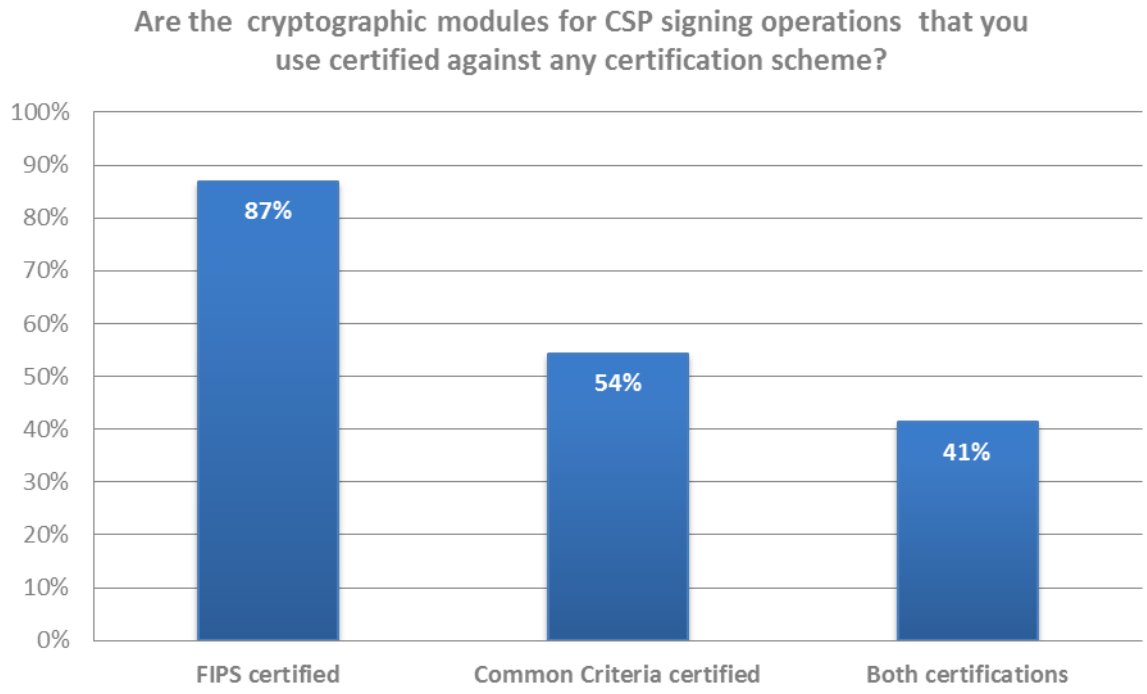

Figure 8: Use of certified products for CA signing operations

4.4 Certification of secure signature creation devices

The main technical specification for the security aspects of signature creation devices for providers of qualified certificates is the CEN workshop agreement *CWA 14169 Secure Signature-creation devices 'EAL 4+'*. [27]

Conformity assessment against the CWA 14169 is assessed within the framework of the Common Criteria, with a specified Evaluation Assurance Level (EAL) of EAL 4+. EAL4 level stands for methodically designed, tested, and reviewed, while "+" refers to certain augmentations over the base level.

Currently the Protection Profiles are not adapted to the new version of Common Criteria. These standards are in the process of being updated for the new proposal.

Common Criteria certified secure signature creation devices are used by the majority of the providers, with 76% of the respondents reporting they used subject devices with this certification. Half of the providers use FIPS certified products. When results are combined, they show around one third of providers use products with both Common Criteria and FIPS certification. Additionally, a small minority of providers report using products certified against other certification schemes or with no certification.

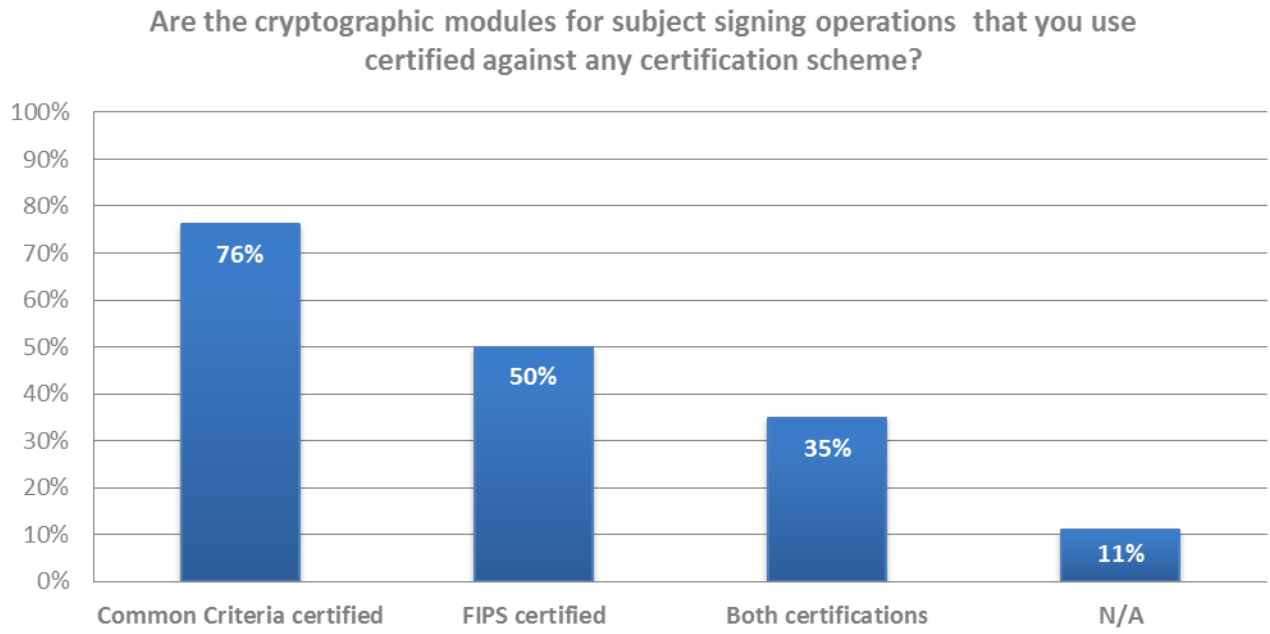

Figure 9: Use of certified products for subject signing operations

4.5 Certification of trustworthy systems

Trust service providers primarily have their systems audited, and do not seek certification based on Common Criteria. The provider or auditor may require that products used by provider are certified. For software used by trust service providers the Certificate Issuance and Management Components (CIMC) Protection Profile[9] issued by NIST is the most common used protection profile for PKI software and there are many products on the market compliant with this PP.

[9] http://www.commoncriteriaportal.org/files/ppfiles/PP_CIMC_SL1_V1.0.pdf

5 Supervision and audit of trust service providers

Supervision plays an important role in independently attesting that organizations in a certain sector comply with the requirements set either in regulations, standards or best practices for that sector. Supervision doesn't include necessarily the conduction of audits; however this is a common practice to be able to assess security practices.

Supervision is mainly foreseen to control if a certain set of requirements established by a regulatory framework (usually defining safety or security requirements or protecting customers) is fulfilled..Independent supervision usually takes place in unregulated sectors where however providers adhere voluntarily to enhance their customers trust.

In many sectors, like the case of trust service providers, both supervision and audit coexist with different focuses. The following section introduces the existing schemes and current auditing practices for certification services.

5.1 Government supervision

5.1.1 Under Directive 1999/93/EC

The Directive 1999/93/EC [37] included some provisions regarding the supervision of trust service providers. Supervision was foreseen primarily for providers who issue qualified certificates, however the possibility of introducing voluntary accreditation schemes in member states for non-qualified trust service providers was also introduced.

Within the qualification scheme, the Directive foresaw for each member state to ensure the establishment of an appropriate system that allows for supervision of trust service providers which are established on its territory and issue qualified certificates to the public. Following the entry in force of Directive, all European member states designated a supervisory body and created a supervision scheme.

Supervisors were set in charge of overseeing that providers of qualified certificates meet the requirements established in the Directive. However, due to the lack of details of the Directive 1999/93/EC regarding supervisory functions or supervision schemes, the EU framework left some gaps. This caused national legislation to differ, applying different requirements for supervision of providers in each member state, regarding:

1. Enforcement or periodicity of audits, characteristics of the audits.
2. Documentation required for the TSP to be submitted to the supervisor.
3. Compliance with standards and needs for certification (further to those set by the European legislation).

Another function of the supervisors was to maintain the denominated "Trusted Lists". The Directive established that member states have to notify the Commission and other member states regarding the names and addresses of all accredited national trust service providers. This has been achieved through the Trusted Lists, lists with standardized formats that contain information regarding all the providers of qualified, and sometimes non qualified, certificates in their respective member state for manual and automatic processing. This list is meant to increase interoperability, so that member states can accept qualified certificates issued in another member state.

5.1.2 Under the proposed Regulation

The new proposed Regulation [38] clarifies and strengthens the role of supervisory authorities in the field of trust services. Within the scope of the new Regulation, the supervisory authority must not

only supervise qualified trust service providers to ensure they fulfill the specific requirements laid down in the Regulation, but also monitor that all trust service providers established in their country fulfill the requirements laid down in Article 15 (security requirements).

Provisions regarding audits are also introduced:

1. Qualified trust services providers must send to the supervisory body an annual security audit conducted by a recognized independent body. In addition, the supervisory body may conduct security audits at any time on them, informing data protection authorities in the case of personal data breaches. In the event of failures to comply detected in the audit reports, the authority has the power to issue binding instructions to the provider. The provider may lose its qualification status due to neglect to remedy the detected failures.

2. In the case of non-qualified trust service providers, the proposal foresees that any trust service provider may submit the report of a security audit carried out by a recognised independent body to the supervisory body to confirm that appropriate security measures have been taken.

Although no authorization is needed to establish a trust service in Europe, supervisors must receive an initial notification by qualified trust service providers intending to enter the market. This initial notification needs to be accompanied by a security audit that will be reviewed by the supervisory body to verify that they comply with the requirements set down in the Regulation.

In case of termination of a provider, the supervisory body must ensure that all relevant information concerning data issued and received by the qualified trust service provider, in particular for the purpose of providing evidence in legal proceedings, are preserved and kept accessible after the activities of the provider have ceased, for an appropriate time with a view to guaranteeing continuity of the service.

Finally, supervisors must produce a yearly report containing information regarding its supervisory activities, statistics about the trust service market in the country and received breach notifications. They must as well cooperate with supervisory bodies of other member states, especially regarding information exchange and support in inspection activities, and continue to maintain the Trusted Lists of qualified providers.

5.2 Independent auditing schemes

The main technical specifications used as a base for independent audit in the area of trust service providers policies and practices are the *TS 102 042 Policy requirements for certification authorities issuing public key certificates [16]* and the *TS 101 456 Policy requirements for certification authorities issuing qualified certificates [12]*. Audits against TS 101 456 is sought mainly by providers of qualified certificates, while certification against TS 102 042 is sought by all providers. Also audits against the, more technical, CWA 14167-1 [26a] is being sought by CSPs.

However, there is not a clear European wide framework regarding auditing bodies accredited to perform audits against these standards, and implementations depend on national regulations.

Aside from audit programs carried out against European standards, the program “WebTrust for Certification Authorities” has a relatively high penetration in European, and non European, CSPs. Webtrust is a program created by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) which provides a framework to assess the adequacy of the controls in CAs that is consistent with international standards. CSPs adhered to the Webtrust program must undergo audits every 12 months.

Apart from these auditing schemes which are specific to certification services, providers may also seek to undergo audits against general certification schemes such as the ISO/IEC 27000:2009 (Information technology -- Security techniques -- Information security management) systems family of standards. Conformity assessment against the widely adopted ISO 27000 framework can be sought for the general security practices used by the provider. ENISA survey shows that 82% report following the ISO 27000 series.

For CA certificate inclusion in web browsers, audit requirements are determined by each browser vendor.

5.3 Current practices

ENISA's survey on security practices of trust service providers shows that, among trust service providers participating in the survey, most providers are already included in some external auditing scheme, with 91% reporting undergoing external audits.

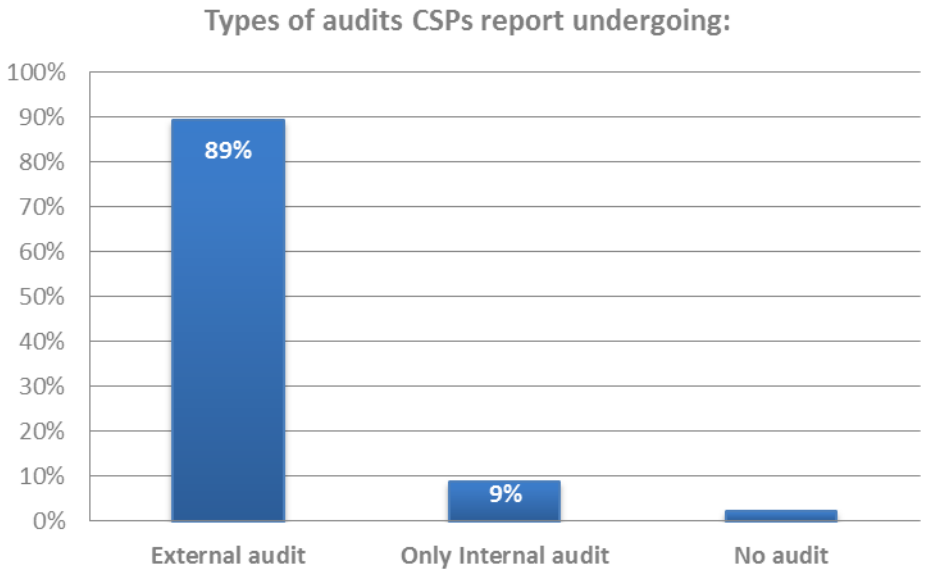

Figure 10: Types of audits CSPs undergo

73% report to be subject to audits on the scope of a government audit scheme, and 78% report to have joined an industry led / independent audit scheme. Finally, more than half of providers are subject to both.

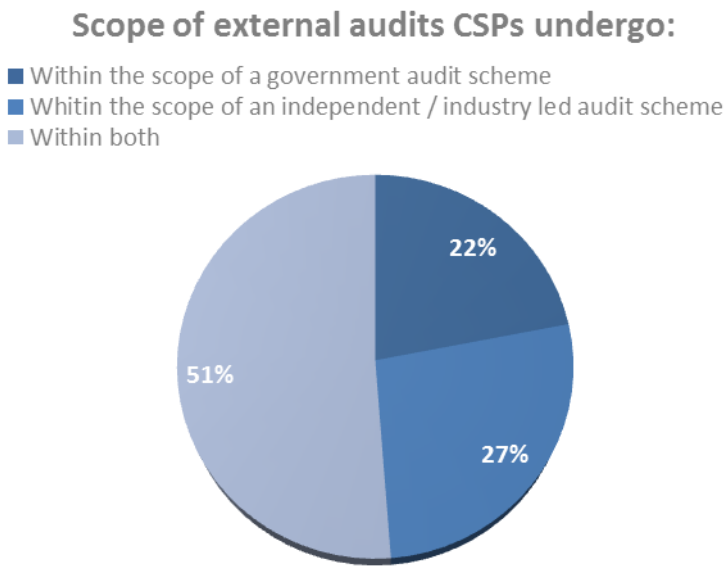

Figure 11: Scope of external audits

Regarding periodicity of audits, 72% of respondents report undergoing an audit at least yearly or more frequently, while only 7% report frequency periods of more than one year. The new proposal for a Regulation on trust services sets yearly audits as a provision for qualified trust service providers.

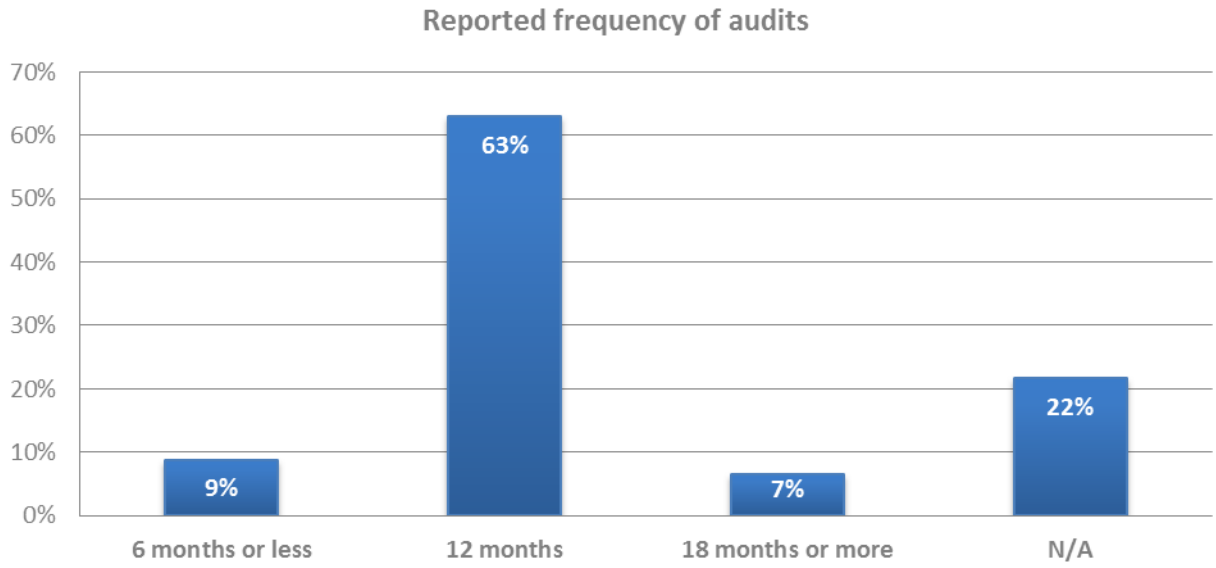

Figure 12: Frequency of audits

6 Cryptographic algorithms in certification services

Certification services rely on public key cryptography as their main component to provide authenticity and integrity, to some extent also confidentiality. Two types of cryptographic algorithms are employed in the electronic certification services: public key algorithms and one way hash functions.

European legislation has not introduced any provisions regarding the cryptographic algorithms and key sizes to be used in electronic certificates, not even in qualified ones, although some member states have defined accepted algorithms and key sizes for qualified certifications services in their country. In general, the choice of algorithms is to be made by the CSP as long as the algorithm is considered to provide the appropriate level of security for the intended service, otherwise the CSP could face liability, or not be able to pass an audit.

Several algorithms exist both for public key algorithms and one way hash functions. This study has focused only on those widely employed by European providers.

However, several standards and technical documents provide guidance to providers regarding recommended algorithms and key lengths. ETSI produced the technical specification *TS 102 176 Algorithms and Parameters for Secure Electronic Signatures [18]* specifies a list of hash functions, as well as a list of signature schemes together with the requirements on their parameters, as well as the recommended combinations of these schemes with hash functions and padding methods in the form of "signature suites".

There are also recommendations in the NIST 800 series of documents [34], and requirement from the CA/B Forum [32][33] to consider.

6.1 Current practices

6.1.1 Public key algorithms

Several public key algorithms exist that can be implemented for certification services suites. The ENISA survey on security practices of trust service providers shows that the most commonly employed algorithm is RSA, created by RSA laboratories and defined in the document PKCS #1: RSA Cryptography Standard. All survey respondents report using this standard for at least one of their CAs.

Employed key sizes range from 1024 to 4096 bits. For Certification Authorities, 67% of participants report having at least one CA using RSA-4096, 52% RSA-2048 and 4% RSA-1024. Meanwhile, a few participants use eliptic curves cryptography algorithms (ECC) – 7% use ECC-256 and only 2% ECC-384.

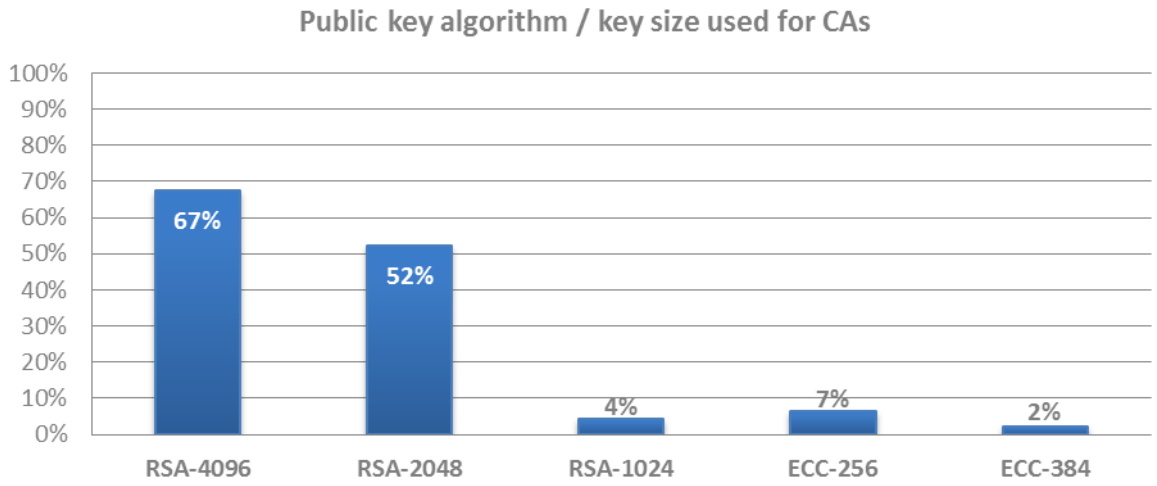

Figure 13: Algorithm and key size use for CA signature

Regarding subject key sizes, ENISA survey results show that 96% of participants report issuing certificates using RSA-2048, 33% RSA-1024 and 13% RSA-4096.

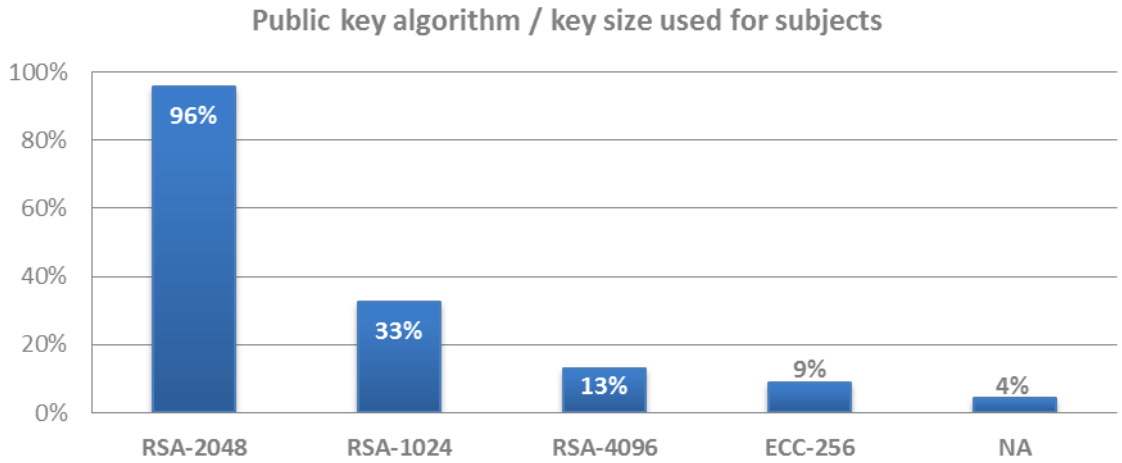

Figure 14: Algorithm and key size use for subject signatures

When looking more into depth in the RSA algorithm, results show that exactly half of the respondents only use RSA-4096 and no smaller key sizes. 46% use a minimum of RSA-2048, but there is a minority of 4% that still employ RSA-1024. While the use of RSA with key sizes of 2048 or 4096 for medium term use is accepted, the use of RSA with a key size of 1024 is not recommended by most studies [34].

NIST and ETSI recommended the discontinuation of RSA 1024 for key generation as from 2010, to be used for legacy purposes from 2011 to 2013, and discontinued by 2013. For key verification purposes, RSA 1024 should be used only for legacy systems since 2010. Similarly, the ECRYPT II recommendations deemed key sizes of less than 1248 only sufficient for short-term protection against medium organizations and medium-term protection against small organizations; a key size of more than 1776 should be used for legacy standard level, and a key size of more than 2436 for medium term security. The German regulator for electronic signatures established that RSA 1024 should not be used for keys for qualified certificates since 2008, while RSA 2048 is deemed acceptable until at least 2018.

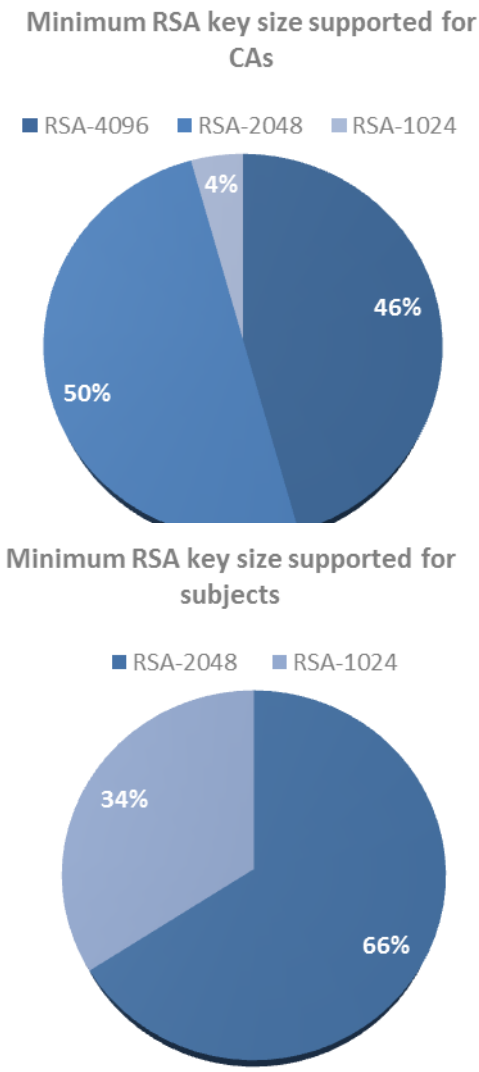

Figure 15: Minimum supported RSA key size

Elliptic curve algorithms are also being used by 9% of survey participants. Use of elliptic curves for digital signatures is described in the American National Standard X9.62-2005 on the Elliptic Curve Digital Signature Algorithm (ECDSA).

In elliptic curves, the majority of providers using them issue ECC-256 signatures, and a minority ECC-384. In the case of ECC, the three mentioned studies report the use of elliptic curves with key sizes above 256 bits acceptable for current use at least until 2018.

6.1.2 One way hash functions

The ENISA survey on security practices of trust service providers shows the current standard practice among trust service providers is to use the SHA algorithm, with all respondents employing it. The SHA algorithm is defined in the NIST guides FIPS 180-1 and NIST FIPS 180-2 RIPEMD, defined in ISO/IEC 10118-3 [8], is also used by a small minority of survey participants.

Regarding one way hash functions for CA signatures, results that 65% of participants report using SHA-1, 63% SHA-256 and 2% SHA-512 for the hash function of at least one CA.

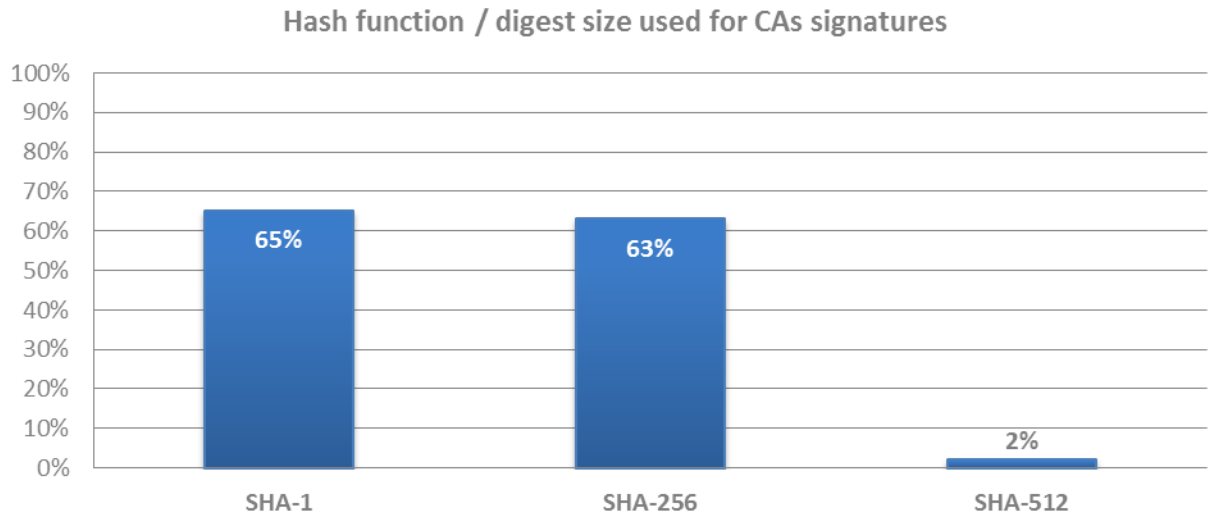

Figure 16: Hash functions and digest sizes for CAs signatures

In the case of one way hash functions for subjects' signatures, ENISA's survey results show that 67% of participants report using SHA-1, 59% SHA-256, 4% SHA-384 and 7% SHA-512 for at least one type of certificate.

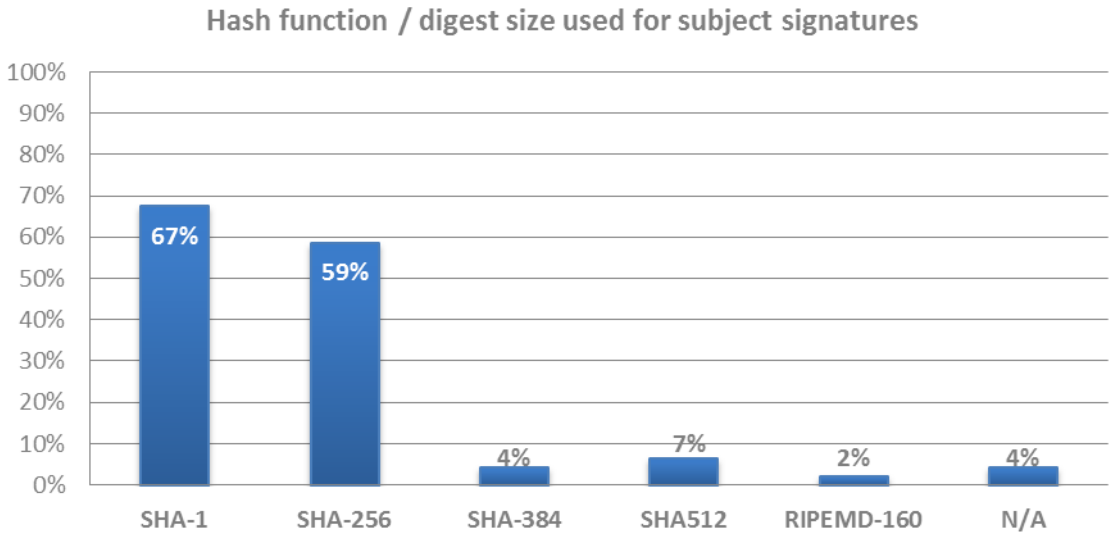

Figure 17: Hash functions and digest sizes for subjects' signatures

When looking more into depth in the message digest sizes, results show that only around a third of the respondents use a SHA-256 for all CAs, while the majority, two thirds, still use SHA-1. In the case of subject certificates, results show that 71% of the respondents use SHA-1, 27% use SHA-256 and 2% use SHA-512.

NIST recommended the discontinuation of SHA-1 for digital signature generation from 2010, to be used for legacy purposes from 2011 to 2013, and discontinued by 2013. For digital signature verification purposes, SHA-1 should be used only for legacy systems since 2010. SHA-256 and SHA-512 are accepted for all hash function applications. Similarly the ECRYPT II recommends against the use of SHA-1 in new applications, and to phase out of SHA-1 for signature applications with medium to high security. The German regulator for electronic signatures established that SHA-1 should not be used for German qualified signature generation since 2008 and for certificate generation since

2010; it can be used for verification of qualified certificates until 2015, while SHA-256, SHA-384 SHA-512 are deemed acceptable until at least 2019.

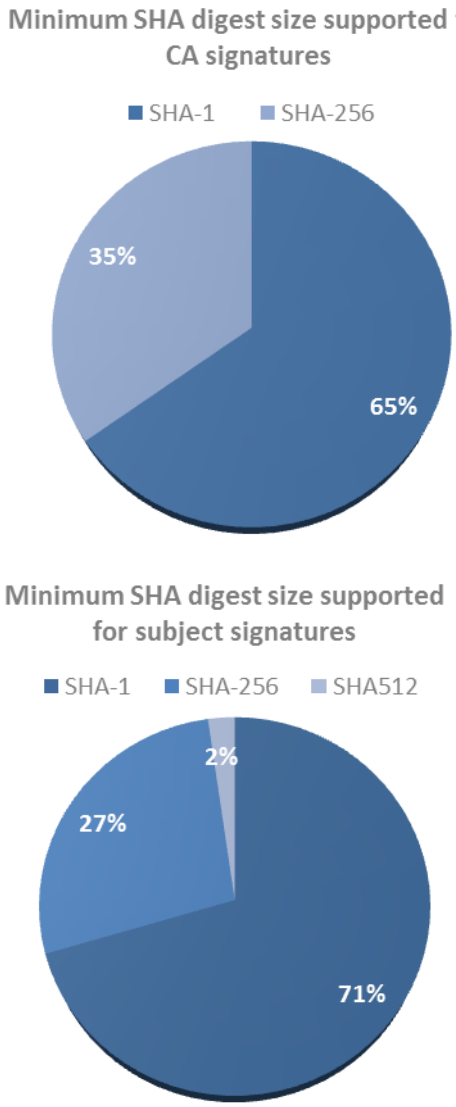

Figure 18: Minimum SHA digest size supported

RIPEMD (RACE Integrity Primitives Evaluation Message Digest), created by KU Leuven, is reported to be used by a minority. Only 2% of the participants use RIPEMD with a digest size of 160. The German regulator for electronic signatures established that RIPEMD-160 should not be used for German qualified certificate generation since 2010; it can be used for verification of qualified certificates until 2015.

7 Recommendations

7.1 Trust service providers in the EU regulatory framework

Regarding the legal framework of trust service providers in the EU regulatory framework it is worth noting that local variations exist. It is therefore recommended to verify with local authorities regarding local policy and regulations in the area, and also investigate variations in other member states where the TSP is intended to operate.

It is also recommended to consider the scope and usage of the TSP services, since requirements may differ depending on the scope and usage of the services offered by a TSP.

For TSPs located outside of Europe it is important to investigate regulations for the services intended to be offered within the scope of the EU regulation.

7.2 Standardization in the area of trust services

Regarding standards in the area of trust services it is recommended comply with standards like ETSI TS 101 456 [12], ETSI TS 102 042 [16], RFC 3647 [23], CWA 14167 [26] (explanation in section 3) in the area where the TSP operates.

It is important that before implementing any standards to check for updated version of the standards. The standards mentioned in this report may be updated at any time.

7.3 Certification of electronic signature products

Different standards for certification of products have different, and sometimes low, penetration in the market.

It is recommended that TSPs use certified products (Common Criteria [42] or FIPS 140-2 [36], as explained in section 4), where possible and practical, and pay attention to supervision and auditing within the area and member state there the TSP operates.

7.4 Supervision and audit of trust service providers

In general TSPs can choose which auditing scheme to follow and should choose an appropriate auditing scheme depending on the intended scope and usage.

TSPs should consider auditing against ETSI, WebTrust, or equivalent auditing schemes. It is important to investigate the requirements for the specific services the TSP intends to offer. For example if the TSP aims to seek inclusion of CA certificates in web browsers, different browsers may have different requirements.

7.5 Cryptographic algorithms in certification services

Several organisations publish recommendations regarding cryptographic algorithms, the most notable being referenced by this document.

TSPs should investigate the latest recommendations, and keep themselves up to date, regarding the choice of algorithms for CAs and subjects. The recommendations may differ slightly depending on the intended scope, usage and member state.

In order to maintain maximum interoperability TSPs should consider using appropriate algorithms and key sizes (ECRYPT [45] and similar studies can be a good guide).

Annex 1 – Definitions

Asset: any person, facility, material, information or activity that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission.

Authentication: process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data;

Certificate: Electronic attestation which links electronic signature or seal validation data of a natural or a legal person respectively to the certificate and confirms those data of that person; **Certification Authority:** An entity trusted to issue certificates. A certification service provider may have one or several Certificate Authorities. It is generally a trusted party or trusted third party that accepts the responsibility of managing the certificate process by issuing, distributing and verifying certificates.

Certification Service Provider: An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Contingency Plan: A plan for emergency response, backup operations, and post-disaster recovery in a system, as part of a security program, to ensure availability of critical system resources and facilitate continuity of operations in a crisis.

Cryptographic module: An umbrella term covering:

- cryptographic algorithms (e.g. encryption, hashing, key generation, ...)
- cryptographic parameters (e.g. key length, elliptic curve, ...)
- cryptographic protocols (e.g. key exchange, ...)
- cryptographic implementations (e.g. software libraries, HSMs, …)

Data Availability: The fact that data is accessible and services are operational. It can be described as the property of being accessible and useable upon demand by an authorized entity. In the context of service level agreements, availability generally refers to the degree to which a system may suffer degradation or interruption in its service to the customer as a consequence of failures of one or more of its parts.

Data Confidentiality: The protection of communications or stored data against interception and reading by unauthorized persons. Confidentiality means keeping the content of information secret from all entities except those that are authorized to access it.

Data Integrity: The confirmation that data which has been sent, received, or stored are complete and unchanged, which implies that the items of interest (facts, data, attributes etc.) have not been subject to manipulation by unauthorized entities.

Electronic seal: Data in electronic form which are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data; (Proposal eSignatures)

Electronic Signature: Data in electronic form which is attached to or logically associated to other electronic data and serves as a method of authentication.

From a legal perspective, an electronic signature is not necessarily considered equivalent to a handwritten signature. When it meets a number of conditions, it can be put on par with a handwritten one.

Event: Occurrence of a particular set of circumstances

Evidence: Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action. Evidence does not necessarily prove truth or existence of something but contributes to establish proof.

Hash Function: A mathematical function which maps values from a large (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a set of values in the domain will be evenly distributed and apparently at random over the range.

Impact: The result of an incident.

Incident: An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system.

Mitigation: Limitation of any negative consequence of a particular event

Probability: Extent to which an event is likely to occur.

Private Key: In a public key cryptosystem, that key of a user's key pair which is known only by that user

Public Key: In a public key cryptosystem, that key of a user's key pair which is publicly known.

Public Key Infrastructure (PKI): The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

Relying Party: A user or agent that relies on the data in a certificate in making decisions.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

Risk Analysis: A process that examines an organization´s information resources, its existing controls, and its remaining organization and computer system vulnerabilities.

Risk Assessment: A process used to identify and evaluate risk and their potential effects

Risk Management: The discipline of identifying and measuring security risks associated with an information system, and controlling and reducing those risks to an acceptable level. The goal of risk management is to invest organizational resources to mitigate security risks in a cost-effective manner, while enabling timely and effective mission accomplishment.

Signature Creation Data: Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

Signature Creation Device: Configured software or hardware used to create an electronic signature

Subject: Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

Threat: Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Trust Service: Any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals

Vulnerability: The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Annex 2 – Abbreviations

CA Certification Authority

CABF CA/Browser Forum

CC Common Criteria

CEN European Committee for Standardization (Comité Européen de Normalisation)

CIMC Certificate Issuance and Management Components

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSP Certification Service Provider

CWA CEN Workshop Agreement

EAL Evaluation Assurance Level

ECC Elliptic Curve Cryptography

ECDSA Elliptic Curve Digital Signature Algorithm

EN European Standard

ETSI European Telecommunications Standards Institute

FIPS Federal Information Processing Standards

GCD Greatest Common Divider

HSM Hardware Security Module

HTTP Hypertext Transfer Protocol

HTTPS HTTP Secure

HW Hardware

ISO International Organization for Standardization

NIST National Institute of Standards and Technology

OCSP Online Certificate Status Protocol

PDS PKI Disclosure Statement

PIN Personal Identification Number

PKI Public Key Infrastructure

PP Protection Profile

PSE Personal Security Environment

QCP Qualified Certificate Policy

RA Registration Authority

RFC Requests For Comments

RSA Rivest, Shamir and Adleman, the persons who first described the algorithm

SHA Secure Hash Algorithm

SSCD Secure Signature Creation Device

SW Software

TLS/SSL Transport Layer Security/Secure Socket Layer protocol

TS (ETSI) Technical Specification

TSA Time Stamping Authority

TSP Trust Service Providers

TR (ETSI) Technical Report

VA Validation Authority

Annex 3 – Bibliography

ISO

[1] ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

[2] ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management

[3] ISO/IEC 24760:2011 Information technology - Security techniques - A framework for identity management

[4] ISO/IEC Guide 73 Risk management – Vocabulary – Guidelines for use in standards

[5] ISO/IEC 9594-8:2008 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks

[6] ISO/IEC 27000:2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary

[7] ISO/IEC 17021 Conformity assessment -- requirements for bodies providing audit and certification of management systems

[8] ISO/IEC 10118-3:2004 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions

[9] ISO/IEC 15408 Series: Information technology -- Security techniques -- Evaluation criteria for IT security. It consists of three parts:

- [9a] ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408.
- [9b] ISO/IEC 15408-2:2008 defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408
- [9c] ISO/IEC 15408-3:2008 defines the assurance requirements of the evaluation criteria.

ETSI

[10] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting electronic signatures - http://www.etsi.org/deliver/etsi_en/319400_319499/319401/01.01.01_20/en_319401v010101c.pdf

[11] ETSI EN 319 412 Profiles for TSPs issuing Certificates

- [11a] 319 412-1: Overview and common data structures
- [11b] 319 412-2: Certificate profile for certificates issued to natural persons
- [11c] 319 412-3: Certificate profile for certificates issued to legal persons
- [11d] 319 412-4: Certificate profile for web site certificates issued to organisations
- [11e] 319 412-5: Qualified certificate statements for qualified certificate profiles

[12] ETSI TS 101 456 Policy requirements for certification authorities issuing qualified certificates: http://www.etsi.org/deliver/etsi_ts/101400_101499/101456/01.04.03_60/ts_101456v010403p.pdf

[13] TR 102 437 Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates) http://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.03_60/ts_101862v010303p.pdf

[14]TS 102 158 Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates http://www.etsi.org/deliver/etsi_ts/102100_102199/102158/01.01.01_60/ts_102158v010101p.pdf
[15]TR 102 040 International Harmonization of Policy Requirements for CAs issuing Certificates http://www.etsi.org/deliver/etsi_tr/102000_102099/102040/01.03.01_60/tr_102040v010301p.pdf
[16]ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates: http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/01.01.01_60/ts_102042v010101p.pdf
[17]ETSI TS 101 862 Qualified Certificate profile: http://www.etsi.org/deliver/etsi_ts/101800_101899/101862/01.03.03_60/ts_101862v010303p.pdf
[18]ETSI TS 102 176-1 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.00.00_60/ts_10217601v020000p.pdf
[19]TR 119 300 Business Driven Guidance for Cryptographic Suites
[20]TS 119 312 Cryptographic Suites for Secure Electronic Signatures
[21]EN 319 403 Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

IETF

[22]RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile http://www.ietf.org/rfc/rfc5280.txt
[23]RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://www.ietf.org/rfc/rfc3647.txt
[24]RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://www.ietf.org/rfc/rfc2560.txt
[25]RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP http://www.rfc-editor.org/rfc/rfc6960.txt

CEN

[26]CWA 14167 Security requirements for trustworthy systems managing certificates for electronic signatures:
[26a] CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-01-2003-Jun.pdf
[26b] CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP) ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-02-2004-May.pdf
[26c] CWA 14167-3 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-03-2004-May.pdf

[26d] CWA 14167-4 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14167-04-2004-May.pdf

NOTE: CEN Workshop Agreement 14167 is currently under revision to become the basis of a European Norm in CEN TC 224.

[27] CWA 14169 Secure Signature-creation devices 'EAL 4+' ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14169-00-2004-Mar.pdf

[28] CWA 14355 Guidelines for the implementation of Secure Signature-Creation Devices Description ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14355-00-2004-Mar.pdf

[29] CWA 14170 Security requirements for signature creation applications ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14170-00-2004-May.pdf

[30] CWA 14890 Application Interface for smart cards used as Secure Signature Creation Devices

[30a] CWA 14890-1: Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

[30b] CWA 14890-2: Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

[31] CWA 14172 European Electronic Signature Standardisation Initiative (EESSI) Conformity Assessment Guidance. It is divided in 8 parts:

[31a] CWA 14172-1: EESSI Conformity Assessment Guidance - Part 1: General introduction ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-01-2004-Mar.pdf

[31b] CWA 14172-2: EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-02-2004-Mar.pdf

[31c] CWA 14172-3: EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-03-2004-Mar.pdf

[31d] CWA 14172-4: EESSI Conformity Assessment Guidance - Part 4: Signature-creation applications and general guidelines for electronic signature verification ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-04-2004-Mar.pdf

[31e] CWA 14172-5: EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-05-2004-Mar.pdf

[31f] CWA 14172-6: EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-06-2004-Mar.pdf

[31g] CWA 14172-7: EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-07-2004-Mar.pdf

[31h] CWA 14172-8: EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-08-2004-Mar.pdf

CA/B Forum

[32] Baseline requirements for the issuance and management of publicly-trusted certificates version 1.1.6 https://www.cabforum.org/Baseline_Requirements_V1_1_6.pdf

[33] EV SSL certificate guidelines version 1.4.3 https://www.cabforum.org/Guidelines_v1_4_3.pdf

NIST

[34] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths: http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

[35] NIST: Discussion Draft of the Preliminary Cybersecurity Framework, August 28, 2013. http://www.nist.gov/itl/cyberframework.cfm

[36] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules". http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf

Legislation

[37] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:PDF

[38] Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF

[39] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm

Others

[40] EU Trusted Lists of Certification Service Providers: https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers

[41] Trust Service Principles and Criteria for Certification Authorities Version 2.0: http://www.cica.ca/resources-and-member-benefits/growing-your-firm/trust-services/item10797.pdf

[42] The common criteria framework: http://www.commoncriteriaportal.org/

[43]Notification with regard to electronic signatures in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance http://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/Areas/ElectronicSignature/PublicationsNotifications/SuitableAlgorithms/2012_algokatpdf.pdf?__blob=publicationFile
[44]PKCS #1: RSA Cryptography Standard: http://www.rsa.com/rsalabs/node.asp?id=2125
[45]ECRYPT II European Network of Excellence in Cryptology II: http://www.ecrypt.eu.org/documents/D.SPA.20.pdf
[46]RIPEMD (RACE Integrity Primitives Evaluation Message Digest): http://homes.esat.kuleuven.be/~bosselae/ripemd160.html
[47]Fox-IT – RSA-512 Certificates abused in the wild. https://www.fox-it.com/en/blog/rsa-512-certificates-abused-in-the-wild/
[48]Smartfacts – Factoring RSA keys from certified smart cards: Coppersmith in the wild. http://smartfacts.cr.yp.to/smartfacts-20130916.pdf
[49]ANSI X9.79 Public Key Infrastructure (PKI) - Practices and Policy Framework
[50]CIMC Protection Profile: http://www.commoncriteriaportal.org/files/ppfiles/cert-issu-v15-sec-eng.pdf
[51]EIFv2: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

European Commission standardisation mandate

[52]Standardisation mandate to the European standardisation organisations CEN, CENELEC and ETSI in the field of information and communication technologies applied to electronic signatures: http://www.etsi.org/images/files/ECMandates/m460.pdf

Under this mandate, the following standards are being developed at the moment of publication of this document:

- TR 1 19 000 Rationalised structure for electronic signature standardisation
- TR 4 19 010 Extended rationalised structure including IAS
- SR 0 19 020 Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment
- TR 4 19 030 Rationalised structure for electronic signature standardisation - Best practices for SMEs
- TR 4 19 040 Rationalised structure for electronic signature standardisation - Guidelines for citizens
- TR 1 19 100 Business driven guidance for signature creation and validation
- TS 1 19 101, EN 3 19 101 Policy and security requirements for signature creation and validation
- EN 3 19 102 Procedures for signature creation and validation
- EN 4 19 103 Conformity assessment for signature creation and validation applications (and procedures)
- TS 1 19 104 General requirements on testing compliance and interoperability of signature creation and validation
- EN 4 19 111 Protection profiles for signature creation and validation application
- EN 3 19 122 CAdES - CMS advanced electronic signatures
- TS 1 19 124 CAdES testing compliance conformance & interoperability
- EN 3 19 132 XAdES - XML advanced electronic signatures
- TS 1 19 134 XAdES testing compliance conformance & interoperability
- EN 3 19 142 PAdES - PDF advanced electronic signatures
- TS 1 19 144 PAdES testing compliance conformance & interoperability

- TS/EN 13 19 152 Architecture for Advanced electronic signatures in mobile environments
- TS 1 19 154 Testing compliance conformance and interoperability of AdES in mobile environments
- EN 3 19 162 ASiC - Associated signature containers
- TS 1 19 164 ASiC testing compliance conformance and Interoperability
- EN 3 19 172 Signature policies
- TS 1 19 174 Testing compliance and interoperability of signature policies
- TR 4 19 200 Business driven guidance for signature creation and other related devices
- EN 4 19 203 Conformity assessment of secure devices and trustworthy systems
- EN 4 19 211 Protection profiles for secure signature creation devices
- EN 4 19 212 Application interfaces for secure signature creation devices
- EN 4 19 221 Security requirements for trustworthy systems managing certificates for electronic signatures
- EN 4 19 231 Security requirements for trustworthy systems supporting time-stamping
- EN 4 19 241 Security requirements for trustworthy systems supporting server signing (signature generation services
- EN 4 19 251 Protection profiles for authentication device
- EN 4 19 261 Security requirements for trustworthy systems managing certificates for electronic signatures
- TR 1 19 300 Business driven guidance for cryptographic suites
- TS 1 19 312 Cryptographic suites for secure electronic signatures
- TR 1 19 400 Business driven guidance for TSPs supporting electronic signatures
- EN 3 19 401 General policy requirements for TSPs supporting electronic signatures
- EN 3 19 403 Requirements for conformity assessment bodies assessing Trust Service ProvidersGeneral requirements and guidance for conformity assessment of TSPs supporting e-signatures
- EN 3 19 411 Policy and security requirements for TSPs issuing certificates
- EN 3 19 412 Profiles for TSPs issuing certificates
- EN 3 19 413 Conformity assessment for TSPs issuing certificates
- EN 3 19 421 Policy and security requirements for TSPs providing time-stamping services
- EN 3 19 422 Profiles for TSPs providing time-stamping services
- EN 3 19 423 Conformity assessment for TSP providing time-stamping services
- EN 3 19 431 Policy and security requirements for TSPs providing signature generation services
- EN 3 19 432 Profiles for TSPs providing signature generation services
- EN 3 19 433 Conformity assessment for TSPs providing signature generation services
- EN 3 19 441 Policy and security requirements for TSPs providing signature validation services
- EN 3 19 442 Profiles for TSPs providing signature validation services
- EN 3 19 443 Conformity assessment for TSPs providing signature validation services
- TR 1 19 500 Business driven guidance for trust application service providers
- EN 3 19 503 General requirements and guidance for conformity assessment of trust application service providers
- TS 1 19 504 General requirements for testing compliance and interoperability of trust application service providers
- EN 3 19 511 Policy and security requirements for registered electronic mail (REM) service providers
- EN 3 19 512 Registered electronic mail (REM) services
- EN 3 19 513 Conformity assessment for REM service providers

- TS 1 19 514 Testing compliance and interoperability of REM service providers
- EN 3 19 521 Policy and security requirements for data preservation service providers
- EN 3 19 522 Data preservation services through signing
- EN 3 19 523 Conformity assessment of data preservation service providers
- SR 0 19 530 Study on standardisation requirements for e-delivery services applying e-signatures
- TR 1 19 600 Business driven guidance for trust service status lists providers
- EN 3 19 601 General policy and security requirements for trust service status lists providers
- EN 3 19 602 Trust service status lists format
- EN 3 19 603 General requirements and guidance for conformity assessment of trust service status lists providers
- TS 1 19 604 General requirements for testing compliance and interoperability of trust service status lists providers
- EN 3 19 611 Policy and security requirements for trusted lists providers
- EN 3 19 612 Trusted lists format
- EN 3 19 613 Conformity assessment of trusted list providers
- TS 1 19 614 Testing compliance and interoperability of trusted lists

NOTE:

For the purpose of the document, the risk assessment phases defined in [2]are followed:

- Risk identification: Identifying the different factors (assets, threats, vulnerabilities, consequences and incident scenarios) that will identify and evaluate the risks:
    - System scope delimitation: Determining the scope included in the risk assessment and its boundaries
    - Asset identification: Identifying any type of item that has value to the organization and that could cause damage if it is involved in an incident.
    - Threat analysis: identifying all agents, either natural or human made, accidental or intentional, internal or external, that could pose a threat to the organization.
    - Vulnerability analysis: Identifying all potential weakness in the organization that could facilitate a successful attack and cause damage to the assets.
    - Consequence determination: Identifying the possible consequences that different events could have on the organization.
    - Incident scenario identification: Determining the possible events that could have an impact on the organization and that will serve as a base to identify the risks.
- Risk analysis: Determining the risk level based on the impact of each incident scenario and their probability of occurrence.
- Risk evaluation: Producing a scored list of all the identified risks, based on the risk analysis results; the business criteria; the affected assets and their vulnerabilities and the potential threats.

Annex 4 – List of organisations taking part in the survey

ENISA gratefuly acknowledges the organisations that contributed to the study conducted in 2013. Mentioned are only these that expressed their consent to be acknowledged in the report.

Organization	Country
AC Camerfirma S.A.	Spain
AS Sertifitseerimiskeskus	Estonia
Banco de Espana	Spain
Borica - Bankservice AD	Bulgaria
British Telecom PLC	United Kingdom
Bundesnetzagentur	Germany
Commfides Norge AS	Norway
Consejo General de la Abogacia Espanola	Spain
DATEV eG	Germany
Direccion General de la Policia	Spain
DHIMYOTIS	France
Digidentity	Netherlands
DigiSign SA	Romania
DigitalSign - Certificadora Digital, SA	Portugal
Disig, a.s.	Slovakia
D-TRUST GmbH	Germany
EADTrust	Spain
e-commerce monitoring GmbH	Austria
EDICOM	Spain
ESG de electronische signatuur B.V.	Netherlands
Fabrica Nacional de Moneda y Timbre	Spain
Firmaprofesional	Spain
Halcom d.d.	Slovenia
Health and Social Care Information Centre	United Kingdom
I.CA	Czech Republic
InfoNotary Plc.	Bulgaria
Information Services Plc.	Bulgaria
Izenpe	Spain
Ministry of Finance and Public Administrations	Spain
Ministry of Defense	Spain

Ministry of Interior	Czech Republic
Multicert S.A.	Portugal
National Security Authority	Slovakia
OpenCA Labs	Italy
Population Register Centre	Finland
Post.Trust	Ireland
QuoVadis Trustlink B.V.	Netherlands
Science and Technology Facilities Council	United Kingdom
Spektar JSC	Bulgaria
Viafirma S.L.	Spain

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

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