Draft ETSI TR 103 684 V0.0.4 (2019-08)

Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services

Interim Draft: Subject to change

Reference
DTR/ESI-000123

Keywords
conformity, e-commerce, electronic signature,
security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

To be added

Introduction

To be added

1 Scope

The present document presents the results to study existing trust services that operate in different regions of the world, and their possible mutual recognition / global acceptance. In particular, the study aims to identify further steps which could be taken to facilitate cross recognition between EU trust services, based on ETSI standards supporting the eIDAS Regulation (EU) No 910/2014 [i.4], and trust services from other schemes. The study concentrates on existing PKI-based trust services as these are the most prevalent across the world.

The report firstly identifies the methodology used in the comparison of other PKI based trust services with those defined in the existing ETSI standards based around the four main elements of a trust service: application context, supervision and audit, technical standards, and trust representation. Then the information collected concerning major PKI trust service schemes around the world and how they relate to the European based trust service scheme based on eIDAS and ETSI standards is presented. Finally, conclusions are presented on the steps which could be taken on how mutual recognition might be facilitated.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] United Nations Commission on International Trade Law (UNCITRAL), Working Group IV (Electronic Commerce) - A/CN.9/WG.IV/WP.158 - Explanatory Remarks on the Draft Provisions on the Cross-border Recognition of Identity Management and Trust Services.

https://undocs.org/en/A/CN.9/WG.IV/WP.158

[i.2] United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce

[i.3] United Nations Commission on International Trade Law (UNCITRAL) Model law on electronic signatures

[i.4] Regulation (EU) 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

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

[i.6] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [i.9] EU Regulation 765/2008 for Accreditation and Market Surveillance (RAMS).

[i.8] IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

[i.9] ISO/IEC 18014-1 to 3 Information technology -- Security techniques -- Time-stamping services, Part 1 Framework, Part 2 Mechanisms producing independent tokens, Part 3 Mechanisms producing linked tokens

[i.10] ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services

[i.11] ISO/IEC 27002 Information Technology Security Techniques Code Of Practice For Information Security Controls

[i.12] ISO/IEC 21188 Public key infrastructure for financial services -- Practices and policy framework

[i.13] NIST FIPS 140-2 Security Requirements for Cryptographic Modules

[i.14] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

[i.15] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

[i.16] ETSI TS 101 861 Electronic Signatures and Infrastructures (ESI); Time stamping profile

[i.17] ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates

[i.18] ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities

[i.19] ETSI TS 102 231 Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information

[i.20] ETSI TS 119 612 Electronic Signatures and Infrastructures (ESI); Trusted Lists.

[i.21] ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[i.22] ETSI TR 119 001 Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations

[i.23] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[i.24] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[i.25] ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[i.26] ETSI EN 319 412 part 1 to 5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles

[i.27] ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

[i.28] ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Note: Further reference material relating to specific PKI based trust services schemes analysed in clause 5 are given at the sub-clause relating to that specific scheme.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.22] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.22] and the following apply:

CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CID	Commission Implementing Decision
eIDAS	Regulation (EU) 910/2014 [i.4] on electronic identities and trust services [for authentication and signatures]
IdM	Identity Management
MLEC	UNCITRAL Model Law on Electronic Commerce [i.2]
MLES	UNCITRAL Model Law on Electronic Signatures [i.3]
NAB	National Accreditation Body
QTS	Qualified Trust Service
QTSP	Qualified Trust Service Provider
QTSP/QTS	Qualified Trust Service Provider and the Qualified Trust Service it provides
SB	Supervisory Body
TS	Trust Service
UNICITRAL	United Nations Commission on International Trade Law

4 Study methodology

4.1 Introduction

The 21st century has seen a significant growth in the adoption of electronic trust services to support a similar growth of electronic activity and transactions in a wide range of domains and sectors, e.g. banking, transport, commerce, governmental services, etc.

The adoption of electronic trust services would not be possible without a defined level of reliability they offer in securing and protecting the supported electronic activities or transactions. The level of reliability of an electronic service may be conditioned by many factors including the associated legal or regulatory provisions, the practices used to provide them and the underlying policy and security requirements they abide by, the technology being used, and the level of control on the implementation of those practices to meet the expected rules.

These levels of reliability may hence differ widely from one domain of implementation to another, from one region to another, as the element that will constitute and define them may in turn be very different. When comparable level of reliability can be achieved between two electronic trust service models, then cross-model interactions and use of respective trust services would be greatly enhanced. Applied to nations, this would greatly facilitate the mutual recognition of electronic trust services and hence greatly enhance cross-border electronic transactions supported by them, especially when addressing trust services that would meet a level of reliability defined to allow for legal effect recognised as equivalent in concerned nations. At the level of application domains, the recognition of trust services

being of the same level of reliability, independently from which domain they are originating, will greatly enhance cross-domain reliable transactions.

Being able to compare and achieve comparable level of reliability for electronic trust services will greatly contribute to the globalisation of those services and by there, the globalisation of electronic transactions supported by them.

NOTE: In order to avoid confusion, the present document will refer to levels of reliability when addressing trust services, to make a clear distinction with the term "levels of assurance" that will be used only when referring to electronic identification schemes (or systems). The notion of levels of assurance should not be used with respect to trust services, since electronic identification means or schemes offering a high level of assurance could be used for trust services with different levels of reliability. There is no correlation between levels of assurance of electronic identification means/schemes and levels of reliability of a trust service. This is in line with the latest work done at the level of the United Nations Commission on International Trade Law, Working Group IV (Electronic Commerce) [i.1].

4.2 Areas of comparison between trust service schemes

The present section provides the description of a high-level methodology used for comparing different PKI-based trust service schemes against the eIDAS PKI-based trust services based on ETSI standards.

Four main areas of comparison have been identified, which underpin the provision of trust services. They are used to compare different models for electronic trust services, PKI-based electronic trust services in particular, in order to assess their differences or equivalences. A comparison based on key elements underlying those areas can be the basis for initiating a process of establishing a mutual recognition between trust service schemes. The four areas are described as follows

a) **Legal context**: Before working on the details it is important to identify the legal context in which a PKI-based trust service scheme operates. This legal context can be ruled by a contractual agreement or be driven by specific regulatory provisions, established in a national, regional or even more global context. Also, the scheme will be based around supporting the functions required for a particular application related trust service whether legal based (such as equivalence to handwritten signature) or application based (secure web service access). Regulatory context can result from laws and ancillary legislations or more generally from policy or implementing rules governing the provision and use of electronic trust services. In the context of those agreements or regulatory provisions, the following comparison elements can be identified:

    a. The target community (e.g. all public, country / group of states, community based on agreement);

    b. The trust service relating supporting the application function (e.g. certificate issuing for electronic signature, certificate issuing for electronic seal, electronic time-stamping, certificate issuing for website authentication, register e-delivery, signature verification, signature preservation);

    c. The provisions on the effects (e.g. legal, security or otherwise) of the trust service, or specific types thereof;

    d. The requirements that might be imposed on the *trust service providers* (TSP) and on the trust service(s) they provide (hereafter collectively denoted as TSP/TS).

b) **Supervision and auditing systems**: This consists of comparing and assessing the equivalences and differences between the various applicable rules on:

    a. The supervisory activities of the entity or entities in charge of the oversight of the TSP/TS and of the verification that they actually meet the agreed or regulatory imposed provisions;

    b. The auditing requirements on the TSP themselves and on the trust service(s) they provide;

    c. The requirements on the auditing bodies when conducting audits on the TSP/TS;

    d. The approval and oversight systems applicable to auditing bodies for them to be eligible to conduct audits on the TSP/TS

    This comparison should take into account the life-cycle of the trust service provisioning, i.e. its initiation, its normal regime provisioning and its termination.

Without prejudice that a PKI may not be aimed at particular regulatory provisions but to meet a need for a particular community, auditing, conformity assessment or certification can significantly assist in establishing trust in TSP/TS. It will increase their level of reliability as a method used to verify their conformance to the prescribed requirements. Comparing different models or schemes regarding the methods used to verify such conformity should take into account whether the assessment is self-performed, performed by an external entity, with such an external entity being self-declared as competent, or its competence being verified by a third party, under a private or institutionalised approval or accreditation scheme, with or without peer review or alike system to ensure homogeneity and confidence in the system.

The fact that the verification of conformance is preformed ex ante or ex post is also to be considered.

Supervision schemes (which can also be called trust management schemes) are used in addition to or in substitution of conformity assessments or auditing schemes. The nature of the supervisory bodies (e.g. public or private), the powers given to them (e.g. final decision on approval/disapproval of TSP/TS, investigation power, ability to issue fines), their resources, the tasks assigned to them, and the scope of the supervision (e.g. entire set of requirements, entire life-cycle of TSP/TS) are some of the many points of comparison that should be addressed.

c) **Best practice**: This area of comparison addresses the technical interoperability standards and best practices requirements applicable to the technical implementation of a trust service by a TSP aimed at meeting the requirements of a particular trust service as specified by the contractual or regulatory requirements for the legal context. In the case of trust services for issuing certificates this is commonly termed the Certificate Policy. It includes:

   a. the policy and security requirements;

   b. the technical criteria and specific requirements;

   c. the requirements on interoperable protocols and formats.

This comparison between to the best practices for PKIs operating in different legal contexts need to confirm:

i. The ability of the practices to meet the requirements for a trust service to be mutually recognised as specified in both legal contexts;
ii. That the practices achieve an equivalent level of security;
iii. That the practices support interoperability between the applications using the trust services.

This comparison can be done at the level of the technical standards and best practices that are referenced, adopted or enforced in a trust model, but have a degree of flexibility that the above aims are met. They can evidently be fine-tuned with regard to the specific type of trust service being considered, including the validation of the output of the considered trust service. When comparing policy and security requirements, a standardised table of contents for the declaration of trust service practices or policies like RFC 3647 [i.3] might be used as a skeleton but it may appear to be a very cumbersome tool, in particular, for other types of trust services than those consisting in issuing digital certificates.

Collectively, all the requirements applicable to the TSP/TS, be they regulatory requirements, be they related to the supervision and auditing system, or be they technical requirements, if any, may be grouped under the term “approval criteria”.

d) **Trust representation**: This area addresses the way the approval and the level of reliability of a TSP supporting given trust services is represented and disseminated; or more precisely how the confirmation that a TSP/ supporting given trust services meets the approval criteria applied by the supervision and auditing systems used for acceptance under the requirements of the legal context. Such a representation can be implemented in different ways such as trusted lists (e.g. as defined in ETSI TS 119 612 [i.20]), trust service stores, by root-signing or cross-certifying trust services, or through bridging mechanisms.

In order to achieve interoperability a common means of trust representation needs to be agreed. This does not necessarily need to be the means of trust representation used within the PKI systems but is required to contain equivalent information so that they may be mapping to/from the agreed trust representation when exchanged.

4.3 Comparison process

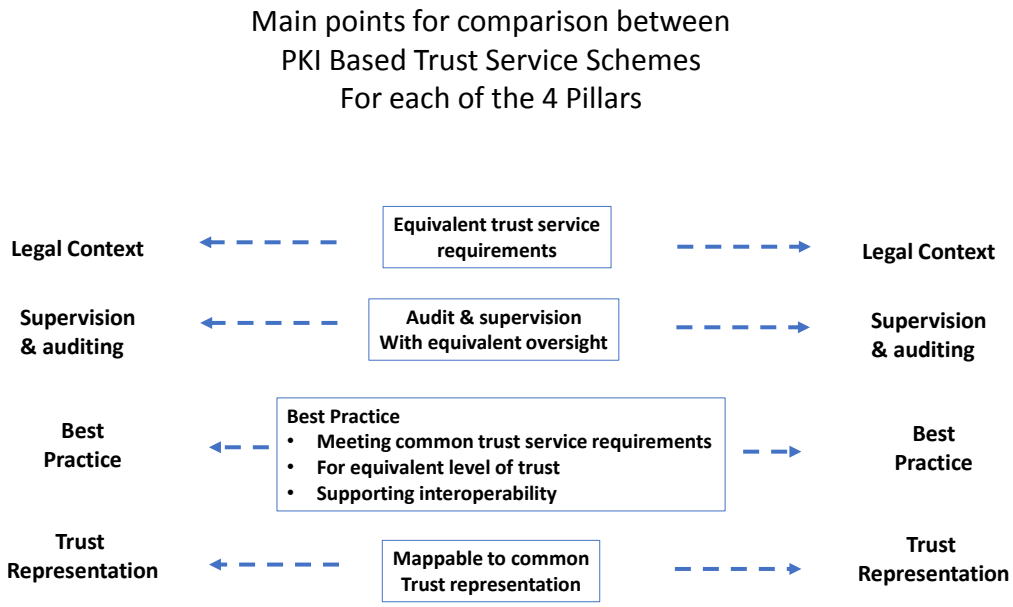


Figure 1: Main points for comparison between PKI Based Trust Service Schemes for each of the 4 Pillars

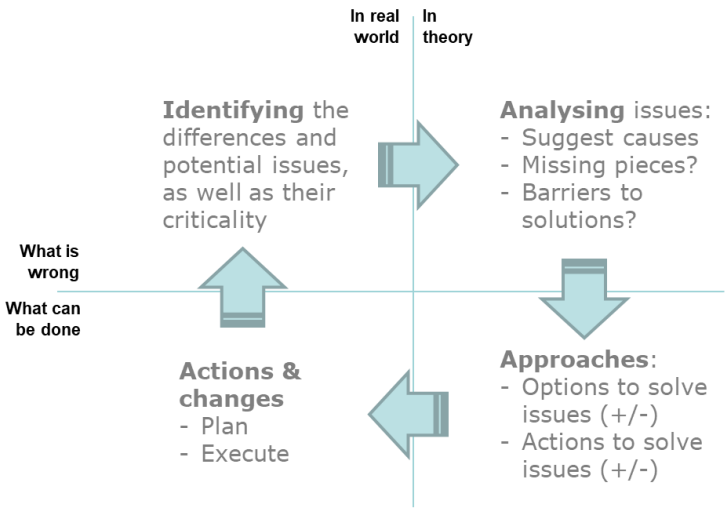
The high-level process for comparing two or more PKI-based trust service schemes along the four comparison areas described in clause 4.2 can be sketched into the following general steps used in problem resolution and illustrated as identified above.:

(i) Identifying the differences between the two models, and the issues potential preventing achieving the objective of equivalence and mutual recognition. Those issues should be ranked in terms of their importance and criticality to this extent.

(ii) Analysing the identified issues: This step should include the suggestion of the potential causes for each issue, examine the missing elements, if any, and what could be the barriers to solutions.

(iii) Approaches to what can be done to solve the issues should then consider the options available for solving the issues together with the identified actions to be undertaken in order to reach a solution.

(iv) Actions & changes: The actions identified and selected in the previous step are planned and executed leading to potential changes to one or both of the models under comparison.



NOTE: Adapted from "The four basic steps in inventing options", Roger Fisher and William Ury, in "Getting to Yes, Negotiating an agreement without giving in", second edition by Fisher, Ury and Patton. RANDOM HOUSE BUSINESS BOOKS.

Figure 2: Four basic steps in comparison process with regards to solving potential issues

The comparison process, when executed with the aim to achieving a mutual recognition, may of course be iterative and several iterations might be needed to come to an acceptable situation in identifying and agreeing on what is acceptable as a basis for a mutual recognition agreement, or to the observation of not solvable issues.

It is not part of the scope of the present document to undertake a mutual recognition between the trust service model established by the eIDAS Regulation [i.4] and any third country similar model or between any PKI-based (qualified) trust service provided by an EU QTSP and any 3rd country TSP/TS. However, Annex A provides interested parties with a high-level mutual recognition process flow.

4.4 Equivalence versus strict compliance

The general principle that should underly the comparison between two (or more) trust models for TSP/TS is the evaluation of their equivalence, both functionally and in terms of levels of reliability. There are many reasons why the trust models or the requirements for TSP/TS cannot be identical and hence the provision of trust service and the trust services themselves not being strictly compliant to all trust models.

Comparability is not a sufficient concept to be used when assessing whether a TSP/TS from a trust model would satisfactorily meet the requirements for a TSP/TS of another trust model, while it is of course a necessary condition to be able to compare them. What matters is the ability to determine whether the level of reliability of a TSP/TS from a trust model would be at least equivalent to the level of reliability of a TSP/TS of another trust model.

The key point is to establish a measurement system that allows one to verify that two elements being subject to comparison can actually be compared and to what extent they are equivalent, functionally and in terms of reliability.

4.5 Study methodology

The study whose results are presented in this document aimed to:

a) Collect information about each PKI-based trust service scheme as identified in clause 5 of the document. For each scheme;

b) Present the information collected for each scheme along the four comparison areas described in clause 4.2;

c) Give a short analysis identifying, for each area, the differences between the particular PKI-based trust service scheme and a scheme based on eIDAS regulation and related ETSI standards;

d) Identify the issues that could prevent mutual recognition. Those issues, discussed in clause 6, are ranked in terms of the extent they are barriers to mutual recognition.

e) Identify, when applicable, potential solution at the technical and standardisation level that can facilitate the resolution of identified issues to mutual recognition.

5 Information Collected on Existing PKI based trust services schemes

5.1 Introduction

This clause provides information collected through questionnaires, presentations given at workshops and from online sources. Whilst this report aims to provide up-to-date information, reference should be made to the sources cited for the most accurate available information.

5.2 International Legal Framework

5.2.1 UNCITRAL

5.2.1.1 Introduction

This review summarises the notes as published by UNCITRAL Working Group IV on Electronic Commerce from the previous several sessions through the most recent: the fifty-eighth session in April 2019. WG IV has facilitated a number of discussions about important topics in recent years in consideration of the basis of trust inherent to identity management (IdM) and trust services (TS). These conversations include individual focuses on cross-border inter-operability, legal frameworks, levels of assurance, non-discrimination, clear liability and mutual recognition. One significant product of the most recent session is the "Draft Provisions on the Cross-border Recognition of IdM and Trust Services", which builds on the extensive work considered during previous sessions. Much of the language of the draft articles follows that of language from the eIDAS Regulation [i.4] , including basic definitions for e.g. individual trust services as well as core concepts such as e.g. functional equivalence and the liability of TSPs, among others.

UNCITRAL acknowledges the enabling legal environment that was established under the tenets of the eIDAS Regulation [i.4], but also that the borders of the signatory Member States of the European Union is the border at which this protective environment ends. A major goal of the development of this expansive legal framework appears to be to follow, as under eIDAS, the coverage of standards for IdM and TS that would function across borders, no matter which geographic area or political jurisdiction. As such, the recent drafting of the document sets forth the language which could be codified as a binding resolution following the objectives developed in the fifty-fifth session. These include the facilitation of the development of international trade law for which economic players can assume legal certainty of their electronic transactions. It would also contribute to harmonising larger emergent issues which are currently addressed in silos at the national and international levels. Like eIDAS, the proposed framework would also be applicable to both IdM and TS, especially in service of the ideas of international cross-border legal and technical interoperability.

5.2.1.2 Legal context

UNCITRAL texts contain functional equivalence rules for certain trust services, namely for electronic signatures, in article 7 of the Model Law on Electronic Commerce (MLEC) [i.2], article 6 of the Model Law on Electronic Signatures (MLES) [i.3], article 9(3) of the UN Convention on the Use of Electronic Communications in International Contracts (ECC) and article 9 of the Model Law on Electronic Transferable Records, and for retention and archiving in article 10 of MLEC [i.2]. Specifically, the MLES [i.3] was aimed at enabling and facilitating the use of electronic signatures and thereby establishing a modern, harmonized and fair legislative framework to effectively address the legal treatment of electronic signatures. This framework gave certainty to the status of e-signatures as equal to hand-written signatures before the law in many capacities, for instance on commercial, transport and official documents.

Concerning the current status of cross-border interoperability, legal recognition may be achieved on the basis of private contractual agreements stipulating the terms of service as well as technical specifications, though there does not appear to yet be an overarching standard governing the legal or technical requirements.

Much of the language of the draft articles follows that of the eIDAS Regulation [i.4], for instance, including definitions, functional equivalence, liability of TSPs, and etc. More in-depth discussion of provisions for trust services can be found in section Chapter IV – Trust services (draft articles 14-18) (A/CN.9/WG.IV/WP.157).

5.2.1.3 Supervision and auditing

Also proposed was the potential for establishment of a white list for IdM schemes and conditions that need to be met in order to be included on that list. This idea follows the trust status list (TSL) concept of eIDAS [i.4] and would provide a level of predictability and clarity for systems that exist and operate across borders. This approach of *ex ante* legal recognition would require setting up a centrally-managed conformity assessment and licensing institutional mechanism to assess each IdM scheme, case by case. However, like any whitelist, it would suffer from the disadvantage of possibly imposing technological and innovative constraints and also may deny legal recognition to schemes and services that are legitimate and functional but not presently included on the list. Worth noting is that such a system may be more effective when operating on a comparatively limited scale and in the framework of broader economic integration, but issues may also arise if implemented on a much larger (for instance global) scale due to significantly increasing levels of cooperation needed by members (A/CN.9/WG.IV/WP.153).

UNCITRAL texts, alternatively, have followed the path of *ex post* legal recognition, which relies on the basis of predetermined criteria for legal recognition and dispute resolution. This approach offers the advantage of maximum flexibility in terms of technological solutions and methods, and does not require the establishment of the centralized system discussed above, allowing for administration in a decentralized manner. However, one notable shortcoming is the requirement for third-party intervention in the adjudication process to evaluate the appropriateness of the cross-border IdM or trust service scheme. This additional process may be burdensome due to financial and time costs as well as the additional risk that it poses (A/CN.9/WG.IV/WP.153).

Moreover, a system for accreditation would be required, or at least a system for verifying existing accreditation schemes in order to fulfil such a white list scheme. However, UNCITRAL foresees that establishing such a body would entail notable administrative and financial consequences. Alternative or complementary mechanisms, such as third-party certification, may assist in achieving the goals pursued by supervision while reducing associated costs. Also noted was the fact that public authorities are becoming increasingly involved both in supervision and also in the development and deployment of IdM systems and the provision of IdM and TS. This necessitates separating supervisory functions from other functions carried out by public authorities (A/CN.9/965).

5.2.1.4 Best practice

Technology neutrality as a principle is at the heart of UNCITRAL (and many other legislative) texts dealing with the use of electronic communications. In the context of IdM and TS, it may be necessary to provide guidance on minimum system requirements by referring to system properties rather than specific technologies (A/CN.9/936). Alternatively, if a transactional approach is chosen, guidance may be required on minimum identity transaction requirements by referring to transaction properties. In the context of TS, the implementation of technology neutrality may require identifying the specific objectives to be achieved by each TS without mandating the use of any particular technology to achieve those objectives, a concept not unfamiliar to eIDAS [i.4].

Another particularly strong idea to come from the Report of WG IV on its fifty-fifth session was the potential for the creation of a 'legal toolbox' that would identify the various solutions relating to IdM and trust services; define their levels of reliability; and specify the legal consequences attached to each reliability level, including liability for failure to provide the specified level of reliability (A/CN.9/902/E). In fact, many of the provisions for the envisioned legal environment facilitative of a cross-border interoperability scheme for TS appear to have already been taken into consideration by the framers of the eIDAS Regulation [i.4]. In fact, special emphasis was placed on the tenets of eIDAS during this session given that it is an example of federated IdM system based on ISO standards that should be considered by UNCITRAL, given that it had already been accepted by 28 States with different IdM systems in place (A/CN.9/902/E). It could be foreseen, therefore, that the international legal framework set forth by UNCITRAL may reflect or parallel that set forth in eIDAS with a view to standards and best practices developed by e.g. ETSI and adopted widely by the European and other international communities.

5.2.1.5 Trust representation

No current consensus on trust representation.

5.2.1.6 Identified enablers

Clearly assessed liability for parties involved in trust services is a major obstacle in the promotion of IdM and trust services. These terms can be developed and understood in the language of individual contracts, but the content of these contracts may and often do vary significantly. Of course, the local legal provisions may dictate the scope of liability for active parties.

Obstacles that exist to broader, global uses of IdM and trust services include specific legal issues such as a lack of legislation giving legal effect to IdM and trust services, divergent laws and approaches to IdM, including laws that are based on technology-specific requirements, legislation requiring paper-based identification documents for entering into online commercial transactions and the absence of mechanisms for cross-border legal recognition of IdM and trust services.

5.2.1.7 Reference Material

Title	URL
UNCITRAL Model Law on Electronic Commerce [i.2]	http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
UNCITRAL Model law on electronic signatures [i.3]	http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
UNCITRAL Working group IV (Electronic Commerce)	http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html
UNCITRAL, Working Group IV (Electronic Commerce) - A/CN.9/WG.IV/WP.158 - Explanatory Remarks on the Draft Provisions on the Cross-border Recognition of Identity Management and Trust Services. [i.1]	https://undocs.org/en/A/CN.9/WG.IV/WP.158
UN Convention on the Use of Electronic Communications in International Contracts	https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf
UNCITRAL Model Law on Electronic Transferable Records	https://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf

5.3 International industry co-operations and standards bodies

5.3.1 Adobe Approved Trust List [In progress]

5.3.1.1 Legal context

5.3.1.2 Supervision and auditing

5.3.1.3 Best practice

5.3.1.4 Trust representation

5.3.1.5 Reference Material

5.3.2 Aerospace PKI [Planned]

5.3.2.1 Legal context

5.3.2.2 Supervision and auditing

5.3.2.3 Best practice

5.3.2.4 Trust representation

5.3.2.5 Reference Material

5.3.3 Certipath [Planned]

5.3.3.1 Legal context

5.3.3.2 Supervision and auditing

5.3.3.3 Best practice

5.3.3.4 Trust representation

5.3.2.5 Reference Material

5.3.4 ISO 27099 PKI -- Practices and policy framework

5.3.4.1 Legal Context

ISO 27099 [not yet published] is an international standard currently under development for public key infrastructure practices and policy framework. It is expected that this will be ratified in year 2020 or 2021. It is based on the ISO 21188 [i.12] a policy and practices framework standard used by WebTrust and the banking community.

It might be adopted as the basis for contractual requirements as is ISO 21188 [i.12] and being an International Standard the has specific recognition under EU legislation.

5.3.4.2 Supervision and auditing

No requirements specified.

5.3.4.3 Best practice

Many of the provisions in ISO 27099 [not yet published] are equivalent to requirements in ETSI EN 319 411-1 [i.24] and they both make used of general requirements for information security management in ISO 27002 [i.11].

5.3.4.4 Trust Representation

No requirements specified.

5.3.4.5 Reference Material

Title	URL
ISO 27099 [not yet published] publication status	https://www.iso.org/standard/56590.html

5.3.5 ISO 21188 PKI for financial services -- Practices and policy framework

5.3.5.1 Legal Context

ISO 21188 [i.12] is an international standard for public key infrastructure practices and policy framework for the financial services. This was first published in 2006 with the latest revision in 2018.

It is being adopted as the basis for contractual requirements for PKI such as WebTrust, and being an International Standard the has specific recognition under EU legislation.

5.3.5.2 Supervision and auditing

No requirements specified but see WebTrust.

5.3.5.3 Best practice

Many of the provisions in ISO 2188 are equivalent to requirements in ETSI EN 319 411-1 [i.24] as this ISO standard was used in the development of the earlier requirements for trust services for qualified electronic signatures in ETSI TS 101 456 [i.15].

5.3.5.4 Trust representation

No requirements specified.

5.3.5.5 Reference Material

Title	URL
ISO 21188 [i.12]	https://www.iso.org/standard/63134.html

5.3.6 WebTrust for CAs

5.3.6.1 Legal Context

The WebTrust for Certification Authorities program was developed to increase consumer confidence in the Internet as a vehicle for conducting e-commerce and to increase consumer confidence in the application of PKI technology. This program, which was originally developed jointly by AICPA and CICA, is now managed by the Chartered Professional Accountants of Canada. Public accounting firms and practitioners, who are specifically licensed by CPA Canada can provide assurance services to evaluate and test whether the services provided by a particular Certification Authority meet these principles and criteria. The posting of the WebTrust Seal of assurance is a symbolic representation of a practitioner's unqualified report. This seal, when provided, is displayed on the Certificate Authority's Web site and linked to the practitioner's report and other relevant information.

WebTrust is adopted by all the major web browser applications as the basis for accepting providers of web server certificates under contractual arrangements.

The trust framework for WebTrust is, at least in hierarchy, generally comparable with that of ETSI. Previous reporting on high- and low-level comparisons between ETSI and WebTrust audit schemes, for example in 2018 by ENISA, in fact revealed more similarities than differences. As far as organizational differences, as can be seen below in a comparison between figure 1 and figure 2, the level of national or international harmonization is where the most significant structural differences lie. Whereas eIDAS produces layers of supervision and accreditation, CPAC is responsible for the harmonization of the work produced by independent licensed practitioners. This is to say, unlike the system laid down by eIDAS, there are no other accreditation bodies responsible for this scheme which could possibly interpret requirements in a different way. Harmonization of results is achieved in part by a standardization of templates for reporting, though CPAC typically does not intend to provide quality control for the harmonization of such reporting. In this way, supervision is one aspect in which the WebTrust scheme finds an opportunity for improvement, as opposed to the stipulation of supervision provided for by ETSI.

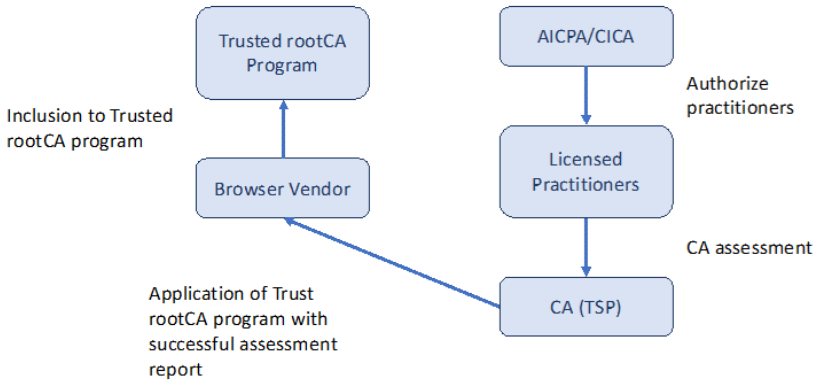


Figure 3: The trust framework of WebTrust for root CA program

5.3.6.2 Supervision and auditing

WebTrust is managed by the Chartered Professional Accountants of Canada.

WebTrust operate its own qualification scheme for acceptance of Certification Authorities.

Because the requirements for non-European / North American TSPs does not currently extend to the eIDAS / EU qualified level, the functional philosophy behind WebTrust is the provision of assurance that a TSP's services have, until the point of time the assessment is conducted, verifiably met a rigorous set of defined criteria. The operating assumption here is that fulfilling a checklist of objectives is the same as fulfilling the obligations to security for which TSPs are responsible in their operations. Similar to the ETSI scheme (EN 319 403 requires the observation of the past period of time to the previous audit), WebTrust is inherently interested in past performance, meaning that the ETSI certification gives the TSP one or two years in advance to keep going while WebTrust certifies what the TSP did last year.

The original (and latest) version of WebTrust is based on ISO 21188 [i.12] and all other offerings are based on controls that have been specified by the CA/B Forum Baseline Requirements (BR).

WebTrust currently offers a product for each service, as stated above, that is informed or based on ISO 21188 [i.12] and by CA/B Forum BR.

5.3.6.3 Best practice

WebTrust publishes its own criteria for Certification Authorities. This is based around ISO 21188 [i.12].

5.3.6.4 Trust representation

Used as the basis for root stores included with adopted by all the major web browser applications.

Trust through a WebTrust audit is represented in the use of a licensed seal. Auditors and TSPs (referred to by WebTrust as "practitioners" and "clients", respectively) may both display the seal on their websites; the rules for representation of a successful WebTrust certification are fairly straightforward. CPAC has the overall responsibility for the accreditation of auditors; a license is required in order to receive permission to use the seal.

Once a seal is issued, a TSP may display the seal on their website, provided they obtain an updated auditor's report on a regular basis. However, if the TSP falls out of compliance, they will remove the seal from their website. The interval between updates, which should never exceed twelve months, may depend on the complexity of the TSP's operation, the frequency of significant changes to their systems, policies and disclosures and the auditor's professional judgment.

Whereas, for example, the EU qualified website authentication certificate (QWAC) is vetted from the highest level for the reliability of its trustworthiness, and under supervision on the Trusted Lists, the WebTrust seal can be regarded as a less rigidly formal representation of the trustworthiness of a TSP or the licensed auditor.

5.3.6.5 Reference Material

Title	URL
WebTrust seal program	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services

5.3.7 SAFE-BioPharma®

5.3.7.1 Legal context

The SAFE-BioPharma ® Association was established by a number of leading biopharmaceutical companies in 2005, aiming to advance the transformation of the healthcare and life sciences sectors to a fully paperless environment by providing standards for digital identities and digital signatures legally binding to electronic documents. SAFE-BioPharma is focused on the alignment of digital certificates and signatures with the sector specific requirements such as FDA 21 CFR Part 11 (Food & Drug Administration), DEA (Drug Enforcement Administration), EMA (European Medicines Agency), HIPAA.

SAFE-BioPharma requirements are based on existing US Federal Government standards, NIST Special Publication 800-63 series and Federal Bridge Certification Authority (FBCA) technical and process requirements.

TSPs seeking to provide digital certificates compliant with SAFE-BioPharma standards should apply for cross-certification with Safe-BioPharma Bridge CA (SBCA).

5.3.7.2 Supervision and auditing

In order to become cross-certified with SBCA, the TSPs will have a compliance mechanism in place to ensure that the SAFE-BioPharma requirements are being implemented and enforced. The auditor is required to demonstrate competence in the field of compliance audits for security and PKIs. An auditor may demonstrate competence by asserting accreditation under ETSI EN 319 403. The audit will be repeated on annual basis.

5.3.7.3 Best practice

SAFE-BioPharma operates as a closed business system model. The TSPs aiming to provide digital certificates to pharmaceutical and life sciences sectors should meet the rules established by the SAFE-BioPharma Association. The rules are aligned with ETSI standards for Trust Service Providers issuing qualified certificates: EN 319 401 [i.23], EN 319 411-1 [i.24], EN 319 411-2 [i.25]

5.3.7.4 Trust representation

SAFE-BioPharma developed a tool that converts the list of TSPs cross-certified with SBCA into a Trust List which is placed in a public online repository.

5.3.7.5 Identified enablers

SAFE-BioPharma Association is already an ETSI member. Therefore, its standards are comparable with ETSI-specific standards for qualified trust services. However, opportunities lie in the following:

- ERDS
- TSA
- TSL update

5.3.7.6 Reference Material

Title	URL
Safe	http://safe-biopharma.org/index.html
FDA 21 CFR Part 11	https://www.fda.gov/media/75414/download
Trusted lists	http://safe-biopharma.org/SAFE_Trust_Lists.html

5.3.8 Kantara

5.3.8.1 Legal context

Kanatara is a commercial consortium.

5.3.8.2 Supervision and auditing

Kantara credential service providers and trust framework assessors are accredited through Kantara.

Kantara operates an identity assurance framework against which global credential service providers are certified for compliance.

Kantara, credential service providers are required to have policies and compliance mechanisms in place to ensure that Kantara requirements are being implemented and enforced.

5.3.8.3 Best practice

The Kantara Identity Assurance Framework complies with the US Federal Identity, Credential, and Access Management (FICAM) program and is based on the requirements of NIST SP 800-63-3 (Base and Volumes a, b and c).

5.3.8.4 Trust representation

Kantara certified credential service providers, TSP and assessors are listed on the Kantara website trust registry which is in a format aimed at display in a web browser.

5.3.8.5 Identified enablers

Kantara has created a separate, unconnected European Headquarters and has associate partners with several EU initiatives.

5.3.8.6 Reference Material

Title	URL
Kantara Trust Framework Operations program	https://kantarainitiative.org/trustoperations/
Trust status list	https://kantarainitiative.org/trust-registry/trust-status-list/

5.4 South America

Editorial Note: Content to be significantly reduced in size for all of this sub-clause to provide the same level of detail as other clauses.]

5.4.1 Argentina

5.4.1.1 Legal context

Argentinian Law nº 25.506 on digital signature (11-12-2001) regulates:

- Digital certificates, including validity period and requirements and foreign certificates recognition (Chapter II);
- Licenced certifiers (that's the name used in the Argentinian legislation to refer to a Trust Service Provider that has been accredited by a governmental entity to operate), including its functions and obligations; licence requirements and licenced certifiers activity cessation (Chapter III);
- Digital certificate title holder, including its rights and obligations (Chapter IV);
- The institutional organization, including the Digital Signature Infrastructure, the audit system and the Digital Signature Infrastructure Advisory Commission (Chapter V);
- The Application Authority, including its functions and obligations and licencing fees (Chapter VI);

- Argentinian audit system, including subjects to be audited and accreditation requirements for third parties that may carry on an audit process (Chapter VII);
- the Digital Signature Infrastructure Advisory Commission, including its internal operations and its functions (Chapter VIII);
- Licenced certifiers liability (Chapter IX);
- Penalties regime (Chapter X);

Argentinian Decree 182/2019 that regulates the Law nº 25.506 (11/03/2019) regulates:

- Digital Signature Infrastructure, including its composition; root Certification Authority; audit system types and report; digital certificates (validity in case of been issued by non-licenced certifiers; revocation); licence obtaining (requirements; effects; duration; licence expiry reasons); foreign certificates recognition; unique certification policy requirements; licence certifier obligations and liability; licence certifier resources; outsourced services (Chapter II);
- Application Authority and Licencing Entity, including its functions, the Argentinian root Certification Authority obligations; fees and penalties (Chapter III);
- Registration Authorities, including its functions and roles; cooperation between different Registration Authorities; licenced certifier liability related to the Registration Authorities; public sector licenced certifier Registration Authorities; guarantee insurance requirements and required subjects (Chapter IV);
- Trust Service Providers, including the definition of Argentinian trust services and Trust Service Providers types of subject.

Argentinian Decree 892/17 regulates the Remote Digital Signature Platform creation and requirements so that this kind of signature is included as one of the digital signatures admitted in the Electronic Document Management System.

Finally, Argentinian Decree 1063/16 regulates:

- The implementation of the Remote Procedures Platform as part of Electronic Document Management System (article 1), including its application area (article 3);
- The electronic document validity made though the platform (article 4);
- Documents digitalisation (article 5);
- Electronic Special Address (articles 6 and 7);
- Electronic notification (article 8);
- Report presentation time-stamping and users actions time-stamping (article 9);
- Electronic Document Management System digital signature (article 13); and,
- OID identification numbers Registration Authority (article 15);

As we said, the Law nº 25.506 distinguishes between electronic signature and digital signature. The electronic signature is a set of integrated electronic data, linked or associated in a logical manner to other electronic data, used by the signatory as an identification mean. That kind of signature does not comply with some of the legal requirements to be considered digital signature.

On the other hand, the digital signature is defined as to result of applying to a digital document a mathematical procedure that requires information of exclusive knowledge of the signer, being this one under the signer sole control. The digital signature is required to be verifiable by third parties, so that such verification simultaneously allows the signer identification and the detection of any alteration of the digital document after its signature.

According to article 3 of the Law 25506 on digital signature, when the law requires a handwritten signature, a digital signature also satisfies that requirement.

In the eIDAS terminology, the electronic signature will be equivalent to an ordinary electronic signature, and the digital signature, to a qualified electronic signature.

These providers are called Trust Service Providers, as in the EU, but also are known as Certification Service Providers (more in line with EU Directive 99/93/CE).

According to the articles 22 of the Decree 182/2019, the Modernization Government Secretariat, depending on Central Office of Cabinet of Ministers will act as the Application Authority, and that one of its functions is to authorize the operation of certification entities in Argentina and supervise and audit these certification entities.

According to article 16 of the Decree 182/2019 the Modernization Government Secretariat, depending on Central Office of Cabinet of Ministers, is authorised to elaborate and sign agreements of reciprocity with governments of foreign countries, in order to grant validity, in their respective territories, to the digital certificates issued by certifiers of both countries as long as the compliance with the conditions established by Law no. 25506, its modification and its regulation for certificates issued by national certifiers, is verified.

On the other hand, Law 25506 establishes in article 16 that digital certificates issued by foreign certifiers may be recognized under the same terms and conditions as required by this law and its regulatory standards

According to Article 36 of the Argentinian Decree 182/2019, a trust service is an electronic service provided by a trust third party. The same article defines the following trust services:

- Provision of digital documents digitally signed preservation services;
- The preservation of intention statements made in electronic format, electronic contracts, and any other transaction that the parties decide to entrust to a third depository party;
- Electronic documents reliable notification;
- The storage of intention statements made in electronic format.;
- The operation of block chains for the preservation of electronic documents, intelligent contracts management and other digital services;
- Electronic authentication services;
- Digital identification services; and,
- Other features established by the Certifying Entity.

5.4.1.2 Supervision and auditing

To obtain the accreditation, a certifier is required to comply with the following steps:

1) Application submission, including all the detailed documentation in Annex I of Resolution nº 399e/2016. This documentation includes the following:
    - Single Certification Policy, including the applicant data;
    - Framework agreement with subscribers;
    - Framework terms and conditions with Third Party Users ("relying parties");
    - Privacy Policy;
    - Contracts with the suppliers of the technological infrastructure, if applicable;
    - Procedures guidelines;
    - Activity Cease Plan;
    - Security Plan (includes security policy and procedures);
    - Business Continuity Plan;
    - Description of the technological platform, and,
    - Description of the services provided.
2) Application admissibility: Study of form through the verification of the submitted documentation.

3) Documentation analysis: Detailed study of all the documentation to determine its compliance with the requirements necessary to operate as a licensed certifier:

4) Conformity audit: Assessment of the control on the facilities and verification of compliance with technical and legal requirements;

5) Ability report: Issuance of the corresponding legal and technical opinion recommending the granting or denial of the license;

6) Grant the license: Dictation of the resolution by the Ministry of Modernization;

7) Digital certificate of the certifier: Issuance of a digital certificate in the name of the certifier by the Root Certifying Authority; and,

8) Operations start of the licensed certifier: Upon the issuance of its digital certificate, the licensing certifier may issue digital certificates to individuals, legal entities or applications, within the framework of the approved certification policy.

According to Article 14 of Decree 182/19, the accreditation validity is for five (5) years and, after that it may be renewed after an audit that certifies compliance with current regulations and technical conditions and procedures at the time of accreditation.

Also that accredited certifiers will annually make an affidavit stating compliance with the rules established in Law 25506 and its amendment, in Decree 182/19 and in other complementary regulations, as well as the procedures detailed in the accrediting documents. The Licensing Entity is required to subject accredited certifiers to annual periodic audits according to the guidelines determined by it.

On the other hand, article 27 of Law 25506 on digital signature establishes that the Application Authority, with the assistance of the Advisory Commission for the Digital Signature Infrastructure, will design an audit system to evaluate the reliability and quality of the systems used, the integrity, confidentiality and availability of data, as well as compliance with the procedure manual specifications and the security and contingency plans approved by the licensing body.

Article 6 of Decree 182/19 describes several audit types, i.e.:

1) Initial audit: as a requirement to obtain the accreditation to operate as a TSP;

2) Renovation audit: as a requirement to obtain the renovation of the licence;

3) Annual periodic audit: requested by the licensor;

4) Extraordinary audit: requested by the licensor;

The audits may be on the certifiers who are applying for a license, on the licensed certifiers and on the registration authorities. The Licensing Entity will determine the periodicity of the audits.

Finally, article 20 of Decree 182/19 establishes that services or infrastructure contracted to third parties, including the systems and security measures of the contracted provider, is required to also be audited and inspected.

5.4.1.3 Best practice

According to Articles 23 of the Decree 182/19 the Administrative Modernization Secretariat, depending on the Modernization Government Secretariat, depending on Central Office of Cabinet of Ministers, will act as the Application Authority, and that one of the functions of that authority is to establish the applicable technological and safety standards in accordance with international standards.

The documents “Unique Certification Policy v.3.0” and “Procedures Manual v.3.0” (both versions of January of 2019, set up the following ETSI standards, that are applicable to:

- ETSI TS 102 023 [i.18] related with the policy requirements for time-stamping authorities; and,
- ETSI TS 101 861 [i.16] related with the time-stamping profile.

5.4.1.4 Trust representation

Although there is not a trust list or any formal trust representation for the Argentinian Trust Certification Providers, numeral 28 of article 23 of Decree 182/2019 establishes that one of the Argentinian Secretariat of Administrative Modernization is to publish on Internet or on a public access network data transmission/dissemination that substitutes Internet in the future in a permanent and uninterrupted form data contacts and digital certificates of:

- Licenced certifiers;
- Certifiers whose licence has been revoked;
- The Argentinian Root Certification Authority; and,
- Licencing entity.

5.4.1.5 Reference Material

Title	URL
Argentinian Law nº 25.506 on digital signature (11-12-2001)	http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
Argentinian Decree 182/2019 that regulates the Law nº 25.506 (11/03/2019)	http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/320735/norma.htm
Argentinian Decree 892/17 regulating Remote Digital Signature Platform creation and requirements	http://www.cac.com.ar/data/documentos/21_Dec.%20892%2017.pdf
Argentinian Decree 1063/16	http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/266197/norma.htm
Accreditation information	http://aaip.gob.ar/modernizacion/administrativa/firmadigital/entelicenciante
Application submission found in Annex I of Resolution nº 399e/2016	http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/266312/norma.htm
Unique Certification Policy v.3.0	http://pki.jgm.gov.ar/cps/cps.pdf
Procedures Manual v.3.0	http://pki.jgm.gov.ar/docs/Manual_de_Procedimientos_ACONTIv2.0.pdf

5.4.2 Bolivia

5.4.2.1 Legal context

Bolivian Law nº 164 on telecommunications and information and communication technologies (from here on: Law 164) and the General Regulation on Law nº 164 regulates:

- the legal and evidentiary validity of the digital document, the electronic data message and the digital signature (article 78 of Law 164);
- certification authorities (called “certification entities”) (article 82 of Law 164);
- the legal status of digital certificates issued by foreign certification authorities (article 80 of Law 164);
- the attributions of the Bolivian accreditation entity (article 81 of Law 164);
- the entity that will provide the public sector certification service and for general Bolivian population; i.e. the Development of the Bolivian Information Society Agency (article 83 of Law 164);
- Value-Added Services accreditation requirements (article 48 of General Regulation on Law 164).

The Bolivian Administrative Regulatory Resolution RAR ATT-DJ-RA-TL LP 32/2015 (9 January of 2015) (from now on: Resolution RAR 32) establishes:

- the approval of technical standards and other guidelines established for certification entities;
- digital certificate types, usage and formats (articles 5 and 6);
- Certification Entities and Registration Agency authorization requirements (article 8 to 13):
  - For public Certification Entities: legal, economic and technical requirements;

  - For Registration Agencies and outsourced services: same requirements as Certification Entities depending on if the agency is public or private.
  - For private Certification Entities: legal and economic requirements;

- Digital certificate and certificate revocation list format (CRL and OCSP) (Annex 1);
- Minimum contents of Certification Entities terms and conditions (Annex 3);
- Certificate Policy minimum contents for an accredited Certification Entity (Annex 4);
- Certificate Policy Statement minimum contents for a Certification Entity (Annex 5);
- Minimum contents of an accredited Certification Entity disaster recovery plans and procedures (Annex 6);
- Minimum contents of an accredited Certification Entity security and risk assessment plans and procedures (Annex 7 and 8);
- Minimum contents of the procedures and the conditions that is required to be complied by Certification Entities for the preservation of physical and digitised documents (Annex 9); Resolution
- Security levels (Annex 10);

The Bolivian Administrative Regulatory Resolution RAR ATT-DJ-RA-TL LP 1538/2015 introduces some modifications to the Resolution RAR 32. These modifications are related with the following aspects:

- natural person digital certificate format;
- legal person digital certificate format;
- public officer digital certificate format;

The Bolivian Administrative Regulatory Resolution RAR ATT-DJ-RA-TL LP 31/2015 (9 January of 2015) (from now on: Resolution RAR 31) approves the Root Certification Entity public documents; i.e.:

- Certification Policy;
- Certification Policy Statement;
- Guidelines for third-party acceptors acting within the National Digital Certification Infrastructure framework of the Plurinational State of Bolivia; an
- Certificate Entities accreditation process;

The Bolivian Supreme Decree nº1793 (from here on: SD 1793) regulates:

- Digital certificates and digital signature (Title IV, Chapter I SD 1793);
- The National Digital Certification Infrastructure framework (Title IV, Chapter II SD 1793), including its hierarchy structure; Telecommunications and Transport Regulation and Control Authority functions; Certification Entity and Registration Agency functions; digital certification services; Certification Entity obligations and liability; and audit process.

The Bolivian Administrative Regulatory Resolution RAR ATT-DJ-RAR-TL LP 876/2016 (from now on: Resolution RAR 876) regulates the technical standard applicable to time-stamping services. Also regulates:

- Time-stamping service authorization (article 10);
- Time-Stamping Authorities (from now on: TSA) Policy requirements (article 13);
- Public TSA economic requirements (article 11);
- Private TSA economic requirements (article 12);
- TSA’s obligations with the Telecommunications and Transport Regulation and Control Authority and with its users (articles 14 and 15);

- TSA digital certificate format; time-stamp format (annex 1);
- Reliable time source and applicable standard (annex 2);
- Contract model for the provision of time-stamping services (annex 3);
- TSA terms and conditions minimum contents (annex 4);
- TSA time-stamping policy minimum contents (annex 5);
- TSA Certification Policy Statement minimum contents (annex 6);

The Bolivian Administrative Regulatory Resolution RAR ATT-DJ-RAR-TL LP 272/2017 (from now on: RAR 272) regulates the technical standard applicable to the registration agencies performance. Also regulates:

- Contract model between the accredited Certification Entity and the Registration Agency (annex 1);
- Communication and access system policy (annex 2); and,
- Accredited Certification Entity and the Registration Agency control and supervision policy (annex 3)

According to article 1 of the Resolution RAR 32, the Telecommunications and Transport Regulation and Control Authority is responsible for the authorization, regulation, supervision, control and also is the entity responsible for conducting technical audits over the Certification Entities.

According to article 80 of the Bolivian Law 164 digital certificates issued by foreign certification entities have the same validity and legal effectiveness recognized in the law provided that such certificates are recognized by a national authorized certification entity that guarantees, in the same way as it does with its own certificates, the compliance with the requirements and the procedures as well as the validity and the validity period of the certificate.

Also, according to the second final provision of Supreme Decree nº 1793 public entities may opt for a foreign certifier for the use of digital certification services provided that the Development of the Bolivian Information Society Agency is established as a Certification Entity.

Bolivian legislation considers the following services:

- Provision of digital certification service (Article 41 SD 1793);
- Provision of digital signature validation service (document "Guidelines for third-party acceptors acting within the National Digital Certification Infrastructure framework of the Plurinational State of Bolivia" in RAR 31);
- Provision of time-stamping service (RAR 876)
- Provision of registration service (Article 41 SD 1793 and RAR 272), i.e:
  - Registration and identification of the natural or legal person in a reliable and complete manner (article 9 RAR 272); and,
  - Digital certificate approval or revocation request (article 9 RAR 272).
- Provision of other related certification services (Article 41 SD 1793);

5.4.2.2 Supervision and auditing

Accreditation

According to the Certification Entities authorisation process, included in the Resolution RAR 31, to obtain the accreditation to operate:

Application reception:

- The interested Certification Entity is required to submit the authorisation application to the Telecommunications and Transport Regulation and Control Authority general manager who is required to submit it to the Telecommunications and Transport Regulation and Control Authority Financial Administrative Office, including all the required documentation;

- The Financial Administrative Office assigns a roadmap number to the file that is summarising all the submitted documentation. Therefore, all actions generated in connection with the Certification Entity authorization procedure is required to be collected under the assigned number without exception whether these actions are generated by the requesting Certification Entity or by the Telecommunications and Transport Regulation and Control Authority staff;

- Once the roadmap number has been assigned:

  - it is required to be registered in the Telecommunications and Transport Regulation and Control Authority file management system;

  - in order to proceed with its follow-up during the authorization process; and,

  - the legal, economic and technical documentation is required to be submitted to the "Archive" area.

All this process is required to be done in no more than two days.

Documentation review

- the Archive area assigns the file number and the procedure number and sends the actions to the ICT Unit Central Office, and this entity proceeds to assign the procedure to one or more analysts, according to the kind of authorization request and the personal availability.

- The personal carries out a documentation analysis in order to verify the compliance of economic, technical requirements.

- The economic requirements to be verified are different according to the public or private certification entities nature; i.e.:

  - For Public Certification Entities:

    a. Financial statements (fiscal solvency certificate issued by the General National Audit Office);

    b. opening balance sheet or the last year exercise balance sheet presented to the National Tax Service verifying the presentation proof;

    c. a five-years business plan projection that also is required to contain the general investments programme to be made;

    d. Proof of purchase related to the fulfilment of the contract for 7% of gross income on the projections for the first year in order to support its activities during the validity of the authorization for the provision of digital services in accordance with article 45 of SD 1793.

    e. Advance payment to the Telecommunications and Transport Regulation and Control Authority of 1% of gross income derivate from digital certification service operation based on the Certification Entity gross income according to article 38 of SD 1793. This payment constitutes an inspection and regulation fee.

    f. Fee structure according to article 42 of SD 1793. In this section Certification Entities is required to make a record of the supported criteria used to determine the costs of digital certification services that it proposes to provide;

    g. copy of the administrative act or administrative resolution authorising the public entity to act as an Authorised Certification Entity.

Requirements d), e) and g) will be fulfilled once the authorisation is obtained by the Certification Entity, but the entity has to make a formal state on its own will to give compliance to all the requirements;

  - For Private Certification Entities:

    a. Fiscal solvency certificate issued by the General National Audit Office);

    b. A guarantee through an insurance policy issued by an insurance entity duly established in Bolivia that covers the amount established by the Telecommunications and Transport Regulation and Control Authority for the current year; and,

c. Documentation accrediting the funding sources, or the demonstration that the Certification Entity has the necessary resources to implement the technical project presented;

In this case, requirement b) will be fulfilled once the authorisation is obtained by the Certification Entity, but the entity has to make a formal state on its own will to give compliance to all the requirements;

- Technical requirements are the same for both entity types; i.e:

a) Description of the services to be provided, including duration and scope;

b) Certification policies that is required to be presented to the Telecommunications and Transport Regulation and Control Authority for its approval, taking into consideration the following elements:

   a. RFC 3647 or Annex 4 minimum contents;

   b. A plan to cease the Certification Entity activities according to article 51 of SD 1793;

   c. Personal data protection is required to be considered taking into account the considerations of Article 56 of SD 1793;

c) Certification Practice Statement whose contents is required to meet the Certification Entities Certification Practice Statement model and the IETF standard RFC 3647;

d) Documentation describing the technologic infrastructure, detailing the technologic platform technical aspects and including the available hardware, software, communication devices and security, its features, functionalities and operational ways. In this sense, if applicable, it will be demonstrated that processes have been implemented to guarantee the reliability and proper functioning of the certificate management platform, that all the elements used have the guarantees and the due level of operation and that the involved personnel has received the required training to operate them;

e) Authorised Certification Entity disaster recovery plans and procedures (ISO 22301 certification or the minimum contents included in Annex 6);

f) Certification Entity security and risk assessment plans and procedures (ISO 27001 certification or the minimum contents included in Annexes 7 and 8);

g) Procedures and conditions that is required to be met by Certification Entities for the preservation of physical and digitised documents ensuring its storage in servers located in the Bolivian territory and under the legislation of Bolivia (ISO 30300 certification or the minimum contents included in Annex 9);

h) Evidence showing that the Certification Entity has a permanent, update information system, freely accessible via web, containing the following information:

   a. Digital certification procedures;

   b. Conditions for digital certificate validation, renewal, revocation, suspension, fees and usages issued by the Certification Entity;

   c. Digital certificates issued, suspended and revoked with the following information:

      i. Serial number;

      ii. Date of issue; and,

      iii. Validity and applicable restrictions;

   d. Claim procedures;

   e. Certification policy, standard contract model with subscribers and other public documents generated by the Certification Entity;

   f. Registered office, telephone numbers, and contact e-mail;

i) Standard contract model with subscribers whose contents is required to be meet the Authorised Certification Entity Model;

j) Service terms and conditions with subscribers whose contents is required to be meet the Authorised Certification Entity Model;

k) Outsourced service contract, if applicable.

- In the documentation review process, the assigned analysts is required to verify:
  - That the Certification Entity has developed procedures that ensure a clear and reliable communication with applicants, subscribers and any other interested third party on the conditions of the digital certificate usage, its processing, renewal, suspension and revocation, and the content of the applicable Certification Policy; and,
  - the coherence between the contents of the different documents presented and the existence of suitable documentation administration procedures in order to ensure that any changes made in the operation or in the legal requirements are reflected in the documentation and that all modification is made with the corresponding authorization;
- During the review process, the assigned analysts prepare notes requiring the complementary and/or additional information considered necessary. These notes is required to be known by the ICT Unit Manager. This process will have maximum duration of twenty days.
- The Certification Entity have a maximum period of fifteen days to amend the documentation or to notify in writing its intention to withdraw the authorisation process;
- Once the observations have been amended, within fifteen days the technical report on economic and technical requirements compliance is required to be issued and submitted to the Telecommunications and Transport Regulation and Control Authority;
- In case that the observations have not been amended, one of the assigned analysts is required to write within fifteen days a rejection technical report and a note addressed to the applicant Certification Entity detailing the reasons to reject its application. This note also is required to be known by the ICT Unit Manager;
- This reviewing phase is required to not exceed seventy days. This period is suspended when the applicant Certification Entity has to amend one or various observations. The period calculation will resume once the activities have been received by the ICT Unit;

Legal requirements review and approval

- Once the authorization file has been received, the Telecommunications and Transport Regulation and Control Authority Legal Department highest authority assigns it to one or more analysts of the legal area who is required to be in charge of verifying compliance with legal requirements established in the applicable regulations.
- The legal requirements to be verified are different according to the public or private certification entities nature; i.e.:
  - For Public Certification Entities:
    a. Presentation of the accreditation application note duly signed by the authority responsible of the applicant entity, including the following information:
       i. Certification Entity name;
       ii. Certification Entity postal address;
       iii. Certification Entity phone numbers;
       iv. Certification Entity e-mail; and,
       v. Fax and post office box, if applicable.
    b. legal regulation on creation and disposition of appointment of the Holder and of an alternate who may eventually replace the Holder in the procedures, as documents certifying the applicant nature;
    c. Legalized photocopy of the designated Holder Identity Document and also the alternate designated Holder Identity Document;

d. Registration certificate to the National Register of Digital Biometric Taxpayers (PBD-11) and/or NIT (Tax Identification Number) Exhibit Document.

e. Legal representative sworn legal statement about not being included in the prohibitions of Article 39 of Law 164; and,

f. Judicial criminal record certificate of the legal representative issued by the competent authority;

- For Private Certification Entities:

a. Presentation of the accreditation application note duly signed by the authority responsible of the applicant entity, including the following information:

vi. Certification Entity name;

vii. Certification Entity postal address;

viii. Certification Entity phone numbers;

ix. Certification Entity e-mail; and,

x. Fax and post office box, if applicable.

b. Documentation certifying the nature of the applicant as a private company, a mixed company or a majority-state participation company: updated registration certificate issued by the Trade Registry and the company articles of incorporation (including statutes and subsequent articles of incorporation amendment documents) registered in the Trade Registry;

c. Legalized photocopy of the designates legal representative Identity Document;

d. Special power accrediting the legal representatives legal nature and specifying its faculties of appear in person and to perform procedures in the presence of the Telecommunications and Transport Regulation and Control Authority;

e. Registration certificate to the National Register of Digital Biometric Taxpayers (PBD-11) and/or NIT (Tax Identification Number) Exhibit Document.

f. Payroll and photocopies or identity documents of all board members and Board of Directors or partners of legal persons;

g. Natural or legal person, board members and Board of Directors sworn legal statement about not being included in the prohibitions of Article 39 of Law 164; and,

h. Judicial criminal record certificate of the owner or the legal representative issued by the competent authority.

- If observations to the legal requirements of both Certification Entities, public and private, are made, including lack of documentation or failure to comply with formal or substantive aspects, the assigned analyst within ten days is required to prepare the supplementary and/or additional information request notes, giving a maximum of fifteen days to the applicant certification entity to amend the observations or express its intention to withdraw its presentation, in a duly substantiated note;

- If observations made are amended a legal report on compliance is issued and submitted to the ICT Unit within ten days;

- On the other hand if observations made are not amended or if the Certification Entity have had expressed its intention to withdraw the authorisation process, then the analysts is required to draw up the rejecting legal report which has to be known by the Legal Department and is required to submit it to the ICT Unit within eight days;

- The analyst assigned to the ICT Unit is required to draw up within two days before the reception of the report the corresponding note informing to the Certification Entity about the rejection of the application and duly substantiating such decision. This note is required to be known by the ICT Unit Manager.

Article 7 of the Regulatory Administrative Resolution RAR ATT-DJ-RA-TL LP 32/201 establishes that the Telecommunications and Transport Regulation and Control Authority is required to grant a five years validity

accreditation for the provision of signature services and digital certification both for public and private Certification Entities.

Also, Article 47 of SD 1793 establishes that the five years validity accreditation may be renewed for the same period (five years) to natural or legal persons requesting it prior demonstration of the compliance with the requirements and conditions established in Administrative Resolution by the Telecommunications and Transport Regulation and Control Authority.

Auditing

Numeral 18 of Article 14 of Law 164 establishes that the Telecommunications and Transport Regulation and Control Authority has the responsible for carrying out technical audits of the certification entities at the national level.

Article 48 of SD 1793 establishes the minimum contents of the audit process, i.e.:

- Assessment of the reliability and quality of the systems used;
- Compliance with national and international standards on certification and digital signature;
- Integrity, confidentiality and availability of data, as well as compliance with the certification policies defined by the Telecommunications and Transport Regulation and Control Authority;
- Certification Entities Certification Practices Statement;
- Approved security and contingency plans.

According to section 4.5 of the Certification Entities authorisation process, included in the Resolution RAR 31, once a Certification Entity is duly authorised to operate:

- According to the presentation and personnel availability, the ICT Unit designates one or more analysts to carry on the compliance audit and an in-situ requirements verification. The audit is required to be done in a maximum period of forty-five days;
- The audit process begins with a communication note signed by the ICT Unit Manager stating the beginning of the review, including:
  - Start date and estimated duration;
  - Audit team identification data;
  - Administrative requirements for the development of the works as, for example, an office, a PC, a printer or a closed office availability;
  - Auditory programme to be developed during the review; and,
  - Certification Entity contact appointment requirement in order to coordinate the auditory works and to coordinate a list containing names and contact data (e-mail, phone numbers and role) of all the personnel involved with the certification activity in order to plan required interviews and visits.
- Once the review process is completed, the analyst(s) is required to prepare a report containing at least the following information:
  - Audit team name and identification;
  - Audit start and end date;
  - Completed tasks briefly description;
  - Detail in annex of the visited facilities and of the interviewed personnel;
  - Conformity statement of every Certification Entity requirements foreseen condition approved by the Telecommunications and Transport Regulation and Control Authority;
  - Certification Policy and Certification Practice Statement conformity statement as the assessment of the security and contingency plans and procedures effectiveness contained both in the Certification Practice Statement and required in the requirements annexes;

- Conformity related with used system trustworthiness and quality;
- Data reliability and availability; and,
- Signature of the analyst(s) that make up the appointed audit team.

- The audit review process is carried out based on what is indicated in SD 1793 and in the technical standard ISO 21188 [i.12], which establishes a series of PKI controls;
- The audit review process is required to include outsourced services, if any;
- If as a result of the audit observations are made, the assigned analyst(s) is required to prepare a report detailing the aspects to be amended and the corresponding note, which is required to be known by the ICT Unit Manager. These reports is required to
- indicate the maximum period of time for the Certification Entity to correct the audit observations. This period of time is required to not exceed, in any case, a thirty days period.
- the applicant Certification Entity is required to attach to the reply all the documentation and other evidence that allows the verification of the adoption of the required measures in order to correct the observed aspects, notwithstanding that the Head of the ICT Unit may carry out a new in situ review to corroborate the evidence submitted by the Certification Entity;
- Once the observations made have been amended and in situ reviews have been done, if applicable, the assigned analyst(s) is required to prepare the compliance audit report which is sent to the ICT Unit Central Office within a period of time that is required to not exceed fifteen days;
- On the other hand, if the observations made have not been duly amended, the analyst(s) is required to draw up within ten days a rejection report that is required to be accompanied by a note in which the Certification Entity is informed about the reasons for which the authorization process will not be continued. This rejection report is required to be sent to the TIC Unit. The ICT Unit Manager is required to have knowledge of the note that is sent to the applicant Certification Entity;
- Once the favourable reports covering technical, economic and legal aspects have been produced an the audit decisions has been made, and provided that all those reports agree on the achievement of the authorization process of the applicant Certification Entity, the Telecommunications and Transport Regulation and Control Authority is required to inform this entity about the economic obligations that has to be paid in this phase of the process;
- The Certification Entity is required to meet these economic obligations within 10 days and prior to the contract signing for the authorization of its operation. In case that the Certification Entity does not meet the economic obligations, the procedure is required to be dismissed unless the Certification Entity formally explains the reasons for the delay and the Telecommunications and Transport Regulation and Control Authority considers that those reasons may justify an extension.
- Once the economic obligations have been met, the ICT Unit will prepare a technical report on requirements with the requirements and the recommendation to the Telecommunications and Transport Regulation and Control Authority Legal Department for the preparation of the compliance contract and the administrative act to grant the authorization for the operation of the Certification Entity. This stage is required to be completed within fifteen days. Produced the actions indicated above, the root Certification Entity proceeds to the issuance of the Authorized Certification Entity digital certificate.

5.4.2.3 Best practice

Article 1 of Resolution RAR 32 establishes the technical standards to be adopted by the Certification Authorities, as well as designates the Telecommunications and Transport Regulation and Control Authority as the entity that has to establish the technical standards and other guidelines established for the operation of certified entities, both public and private.

Resolution RAR 876 approves time-stamp technical standards and, among them, the following ETSI standards applicable to an Authorised Certification Entity that want to provide time-stamping services:

- ETSI TS 102 023 [i.18] related with the policy requirements for time-stamping authorities; and,

- ETSI TS 101 861 [i.16] related with the time-stamping profile.

Annex 10 of Resolution RAR 32 describes three security levels:

- High security level: device that has the certification of NIST FIPS 140-2 [i.13] level 3or higher, recommended for the keys generation and the private key storage of the accredited Certification Authorities
- Medium security level: device that has the certification of NIST FIPS 140-2 [i.13] level 3or higher , recommended for the keys generation (public and private key) digital certificate storage recommended for:
  - those users (future signers) who have responsibility for identity accreditation and other conditions of the signers in the Registration Agencies;
  - those users (future signatories) that require a higher security level according to the type of document to be signed (type of information, role of the signer, application requirements, etc.)
- Normal security level: through software; it may be recommended for the keys generation and private key storage and protection of the digital certificate for the rest of uses and signers

5.4.2.4 Trust representation

There is not a trust list or any other trust representation for Bolivian Trust/Certification Service Providers

5.4.2.5 Reference Material

5.4.3 Brazil

5.4.3.1 Legal context

Brazilian Provisional Measure nº 2.200-2 (24/08/2001) by which establishes a Brazilian Public Key Infrastructure (ICP-Brasil); transforms the National Institute of Information Technology into autarky, and gives other measures (from now on: PM 2200) regulates:

- ICP-Brasil Management Committee competencies (article 4);
- Certification authorities competencies (article 6);
- Col authorities competencies (article 7);

"Accreditation criteria and procedures for ICP-Brasil entities v5.4" (Ref. DOC-ICP-03)":

- establishes the criteria and procedures to be followed for the accreditation, maintenance of accreditation and desaccreditation of Certification Authorities (CAs), Registration Authorities (ARs), Time Stamp Authorities (ACTs), Support Service Providers (PSSs), Biometric Service Providers (PSBios) and Digital Signature Service Providers (PSC) within the scope of the ICP-Brasil;
- defines Support Service Providers (PSSs) as a provider performing those activities described in the Certification Authority Certification Policies and Certification Practice Statement to which Support Service Provider is linked, directly or through the Registration Authority, or in the Time-Stamping Certification Policies and Time Stamp Practices Statement of the Time-stamp Authority to which Support Service Provider is linked, or still in the activities of Biometric Service Provider (PSBio). Support Service Provider can be classified in three categories according to the type of activities provided:
  - physical and logical infrastructure availability;
  - specialized human resources availability; or,
  - provision of physical and logical infrastructure and specialized human resources.
- establishes that a Biometric Service Provider (PSBio) applicant is required to be an entity with the technical capacity to perform biometric identification (1:N), turning a single registration or a single applicant into one or more biometric data bank/systems for all ICP-Brazil. This kind of provider also is required to have the technical capacity to perform biometric verification (1:1) of a digital certificate applicant through the comparison of a biometry that has a perennial and univocal characteristic according to the international usage standards, such as digital fingerprint, face, iris, voice, collected in the digital certificate issuing process with

another biometry that is stored with the same registry/indexer of this applicant in one or more biometric ICP-Brazil banks/data systems.

- establishes that Trust Service Providers related to digital signature and cryptographic keys storage services is required to be optional entities with the technical capacity to:
  - perform private key storage for end users within the scope of ICP-Brazil; or,
  - provide digital signature services, digital signature verification; or,
  - both, according to specific operating regulations.

According to article 4 of the Brazilian Provisional Measure 2.200-2 (24 august 2001) (from now on: PM 2200) the ICP-Brazil Management Committee is responsible for the identification and assessment of external PKI policies; for the negotiation and approval of bilateral certification agreements, cross-certification, interoperability rules and other forms of international cooperation.

Also, article 9 of PM 2200 set up the prohibition that any Certification Authority certifies a level different from the one immediately following to its level except in cases of cross-certification agreements previously approved by the ICP-Brazil Management Committee

According to section 1.1.2 of the "ICP-Brazil Trust Service Providers Certification Practice Statement minimum requirements" document (ref: DOC-ICP-17) defines an ICP-Brazil Trust Service Provider and the services provided by it as an entity accredited, audited and entity by ITI that provides:

- private key storage services to end users, pursuant to DOC-ICP-04; or,
- ICP-Brazil signature services and digital signature verification printed on electronic documents and electronic transactions, or both.

According to section 6.5 of the "Minimum operational procedures for ICP-Brazil Trust Service Providers" document (ref: DOC-ICP-17.01) establishes a trust service list of the available services related with private key storage services to end users provided by Brazilian Trust Service Providers. This services are classified in two categories: mandatory and optional trust services; i.e.:

- Mandatory trust services related with private key storage services to end users:
  - Provision of an authorization code service to obtain authorization from the title holder to use its private key;
  - Provision of Access token service: After obtaining authorization code, the access token will be requested with parameters in the format "application/x-www-form-urlencoded".
  - Provision of signature service: parameters with contents to be signed and signatures is required to contain values in Base64. If the scope of the token allows only one signature (single signature) and more than one content is informed, an error message will be returned.
  - Provision of application registration with ICP-Brazil SSL certificate: service used to register application with a Trust Service Provider. This application will use an ICP-Brasil SSL certificate to sign the submitted data replacing in this case the Application Registry Service.
  - Provision of certificate retrieval: Service to retrieve certificate stored by the Trust Service Provider. The application will have a valid User Token Access.
  - Provision of title holder position: service to find a title holder through CPF (natural person) or CNPJ (legal personal) information.
- Optional trust services related with private key storage services to end users:
  - Provision of application registration without ICP-Brazil certificate: service used to register application with a Trust Service Provider. It is mandatory for all applications that use authorization services without ICP-Brazil certificates
  - Provision of application registration maintenance service; this service is provided to maintain the stored information of a Trusted Service Provider application. This service is required for all applications that use authorization services not identified by ICP-Brazil SSL certificates.

- Provision de authorization by means of title holder certificate: this service is provided to obtain the title holder authorization to use its private key, with request for authentication factors.

According to section 1.1.5 of the "ICP-Brazil Time Stamp Authorities Certification Practice Statement minimum requirements" report (ref: DOC-ICP-12) states the use of the following ETSI technical specification related with the provision of time-stamping services:

- ETSI TS 101 861 [i.16] related with time-stamping profiles.

5.4.3.2 Supervision and auditing

Authorisation/accreditation process

"Accreditation criteria and procedures for ICP-Brazil entities v5.4" (Ref. DOC-ICP-03)" establishes the following accreditation criteria and procedures:

Accreditation Criteria

- All the accreditation applicants is required to meet the following requirements:
  - be a public law entity or body or a private law legal personal;
  - be exempt with all tax obligations and social charges established by law;
  - meet the economic and financial requirements established according to the activity to be developed (Annexes I, II, III, IV, V and VI); and,
  - comply with ICP-Brazil technical guidelines and standards related to the technical or contractual qualification contained in the documents listed in Annexes I, II, IV, V and VI, applicable to the services to be provided.
- Certification Authority applicants is required to also meet the following requirements:
  - present at least one operationally linked entity applying for accreditation to develop Registration Authority activities, or request their own accreditation to become a Registration Authority;
  - present a list of eventual candidates to be accredited to develop Support Service Providers (PSS) activities;
  - have the administrative headquarters located in the national territory; and
  - have operational facilities and physical and logical security resources, including a safe room compatible with the certification activity located in the national territory, or hire a Support Service Provider (PSS) to provide that facilities and resources.
- Registration Authority applicants is required to also meet the following requirements:
  - be operationally linked to at least one Certification Authority or applicant Certification Authority. The Registration Authority in operation is able to operate in all the Certificate Policies accredited by the linked Certification Authority;
  - have the administrative headquarters, operational facilities and physical and logical security resources compatible with the registration activity.
  - present the list of eventual Support Service Providers (PSS); and
  - If the technical facility is located at an address other than its administrative headquarters, present, cumulatively:
    a. In case of private entities:
       i. updated certificate of the commercial board or civil registry of legal entities according to their nature;
       ii. operating license, if any;
       iii. Legal Person National Register (CNPJ);

b. in the case of a direct or indirect administration legal entity, or public body:

i. administrative act authorizing the operation at that location;

c. in the case of notarial and registration services:

i. copy of the delegation granting act; and,

ii. Legal Person National Register (CNPJ).

- Time-stamp Authority applicants is required to also meet the following requirements:
  - present a list of eventual candidates to be accredited to develop Support Service Providers (PSS) activities;
  - have an administrative headquarter sited in the national territory;
  - have operational facilities and physical and logical security resources compatible with time-stamp issuance activities, located in the national territory, or hire a Support Service Provider (PSS) to provide that facilities and resources.
- Support Service Provider applicants is required to meet the following requirements:
  - be operationally linked to at least one Certification Authority or applicant Certification Authority or to a Registration Authority or applicant Registration or to a Time-stamp Authority or applicant Time-stamp Authority or to a Biometric Service Provider or applicant Biometric Service Provider;
  - have the administrative headquarters, operational facilities and physical and logical security resources compatible with the activities provided.
- Biometric Service Provider applicants is required to also meet the following requirements:
  - present a list of eventual candidates to be accredited to develop Support Service Providers (PSS) activities;
  - have an administrative headquarter sited in the national territory;
  - have operational facilities and physical and logical security resources compatible with biometric identification activities, located in the national territory, or hire a Support Service Provider (PSS) to provide that facilities and resources.
- Trust service Providers related to digital signature and cryptographic keys storage services is required to also meet the following requirements:
  - have an administrative headquarter sited in the national territory;
  - have operational facilities and physical and logical security resources compatible with cryptographic keys storage activities or with digital signature service activities or with digital signature verification service activities, or both, located in the national territory.

Accreditation Procedures

- Application:
  - The accreditation application to become an ICP-Brasil Certification Authority is required to be submitted to the root Certification Authority together with the following documents:
    - Certification Authority accreditation application form duly completed and signed by the legal representative of the applicant Certificate Authority;
    - Documents listed in Annex I;
    - Registration Authority accreditation application form duly completed and signed by the legal representative of the applicant Certificate Authority and Registration Authority;

  - Documents listed in Annex II, except in the event that the Registration Authority applicant is the same as the Certificate Authority applicant and indicate the same technical installation address; and,
  - If the Support Service Providers (PSS) accreditation is required:
    i. Support Service Providers accreditation application form duly completed and signed by the legal representative of the applicant Certificate Authority and of the applicant Support Service Providers, as well as of the applicant Registration Authority in case that the Support Service Providers intends to be operationally linked to the applicant Registration Authority;
    ii. Documents listed in Annex III; and,
    iii. report indicating the specific activities for which the Support Service Provider is making the accreditation application selecting one of the following options:

- physical and logical infrastructure availability;
- specialized human resources availability; or,
- provision of physical and logical infrastructure and specialized human resources.
  - The accreditation application is required to be registered in front of the root Certification Authority General Protocol and received within thirty days by means of a reasoned order; and,
  - If the accreditation application does not contain all the documents listed in Annexes I, II or III, if any, the root Certification Authority is required to determine a subpoena of the applicant so that under penalty of close the file on the applicant amend the irregularities within thirty days from the receipt of a letter sent by the root Certification Authority containing a proof of recipient reception.

- Preoperational audit:
  - After the publication of the reception order, the applicant Certification Authority is required to submit to the root Certification Authority within thirty days a duly completed audit request form stating that the applicant Certification Authority complies with all the requirements established by the resolutions of the ICP-Brasil Management Committee related to the activity of Certification Authority, and that is in place to be audited within fifteen days from that moment;
  - Such application is required to be completed and signed by the legal representatives of the applicant Certification Authority;
  - During the audits, the root Certification Authority may require additional documentation containing specifications on equipment, hardware and software products, technical and operational procedures adopted by the applicant Certification Authority;
  - In the case that the audit report indicates that any of the accreditation criteria required in the accreditation criteria section applicable to all accreditation applicant entity set forth before have not been met, the root Certification Authority is required to require the applicant to comply within the terms established by the Certification Authority upon the reception of a letter sent by root Certification Authority containing a proof of recipient reception.
  - After the communication to the applicant in order to fulfil the accreditation criteria not satisfied in the audit process, the root Certification Authority is required to require the applicant by means of a letter sent with proof of recipient reception the realization of a complementary audit in order to check the measures taken by the applicant Certification Authority;
  - The accreditation process withdrawal application may be requested until the date on which the audit application is received by the root Certification Authority;
  - Once the final audit report is presented, the root Certification Authority is required to express its opinion on the accreditation application acceptance or rejection within thirty days;
  - The decision to reject an accreditation application may be subjected to an administrative appeal by the applicant in front of the ICP-Brasil Management Committee.

- Accreditation act:

- The total or partial deferral, or the rejection of the accreditation, is required to be substantiated and communicated to the applicant Certification Authority. It is considered partial deferment the one that does not contemplate all Certification Policies proposed by the applicant Certification Authority;
- The Certification Authority accreditation act is required to determine the certificate issuance by the root Certification Authority or the Certification Authority of the next higher level, depending on the case:
  - to pay the fees established in the "Guidelines on ICP-Brasil root Certification Authority fees policy", in case the accredited member is a Certification Authority of a level immediately subsequent to the root Certification Authority;
  - the accredited Certification Authority has to submit to the root Certification Authority within ten days after the acceptance of the accreditation deferral, a contract insurance policy for coverage of civil liability arising from the digital certification and registration activities, with sufficient coverage and compatible with the risk of these activities.

The Direct Administration of the Union, the States, the Federal District and the Municipalities are exempt from paying the fee and also are exempt from submitting the insurance police.

- Accreditation is consumed with the Certification Authority certificate issuance. Upon the accreditation deferral, of the accreditation, the next higher-level Certification Authority is required to issue within ten days the certificate of the accredited CA, which is required to be operative within sixty days.

Besides the Certification Authority accreditation, ICP-Brasil regulations and technical documents provides accreditation procedures for the following entities:

- Registration Authorities;
- Time-stamp Authorities;
- Support Service Provider (PSS);
- Biometric Service Provider; and,
- Trust Service Providers related to digital signature and cryptographic keys storage services.

As all this entities accreditation procedures are very similar to the Certification Authority accreditation we have described before, we refer to the accreditation document ("Accreditation criteria and procedures for ICP-Brazil entities v5.4" (Ref. DOC-ICP-03)) in order to meet the specifications of the other entities accreditation procedures.

However there is one aspect related to Support Service Providers, Biometric Service Providers and Trust Service Providers related to digital signature and cryptographic keys storage services accreditation process. In particular it's this aspect is related to the following accreditation prohibition:

- Support Service Providers: The Support Service Provider (PSS) accreditation and recruitment by a Registration Authority to perform identification and authentication activities of the title holders identity and responsible for the certificates according to item 3 of the document "Minimum requirements for the Certification Practice Statement of ICP-Brasil Certification Authorities" is forbidden.
- Biometric Service Providers: it is forbidden to contract, subcontract or outsource all or any part of registration, updating or consultation activities for the purposes of applicant biometric data verification by the accredited Biometric Service Provider within the ICP-Brasil scope, except in case of companies that provide biometric solutions, identification (1:N) for a new register and verification (1:1) in on-line biometric requested queries provided that the Biometric Service Provider previously request it to the ITI, according to Annex V.
- Trust Service Providers related to digital signature and cryptographic keys storage services: It is forbidden to contract, subcontract or outsource all or any part of the activities of private key storage for end users by the accredited Trust Service Providers related to digital signature and cryptographic keys storage service within the ICP-Brasil scope, except in case of companies that provide solutions for cryptographic hardware and systems for digital signatures services and digital signatures verification services, according to Annex VI.

Auditing

Article 4 of PM 2200 establishes that one of the ICP-Brasil Management Committee competencies is to accredit, audit and supervise the Root CA and its service providers.

Section 2 of "Criteria and procedures for conducting audits in ICP-Brasil entities" (ref: DOC-ICP-08) document classifies audits in two groups:

a) **Pre-operational audit:** These are the audits carried out before the beginning of the activities of the applicant Trusted Service Provider, whether Certification Authority, Time Stamp Authority, Registration Authority, Support Service Provider, Biometric Service Provider or Digital Signature and Cryptographic Key Storage Trust Service Provider;

b) **Operational audit:** performed on an annual basis - considered the calendar year - over all Trust Service Providers to maintain the ICP-Brasil accreditation. Such audits will occur from the first calendar year following the date of the Trust Service Providers accreditation publication on the Official Journal of the Union.

5.4.3.3 Technical requirements

Article 1 of Resolution RAR 32 establishes the technical standards to be adopted by the Certification Authorities, as well as designates the Telecommunications and Transport Regulation and Control Authority as the entity that has to establish the technical standards and other guidelines established for the operation of certified entities, both public and private.

Section 1.1.5 of the "ICP-Brasil Trust Service Providers Certification Practice Statement minimum requirements" document (ref: DOC-ICP-17) states that the document is based on the following European standards and regulations, among others:

- Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) [i.4]
- ETSI TS 101 861 [i.16] related with the time-stamping profile [i.16].

Section 6.5.6 of the "Minimum operational procedures for ICP-Brasil Trust Service Providers" document (ref: DOC-ICP-17.01) defines the use of the following ETSI standard related with the Brazilian Trust Service Providers List which is encoded with XML format:

- ETSI TS 102 231[i.19] – on Provision of harmonized Trust- service status information;.

Section 6.6.5 of this document establishes that in ICP-Brazil, the format and structure to be used to create signature policies are been prepared based on ETSI TR 102 272 and ETSI TR 102 038 standards.

stamp technical standards and, among them, the following ETSI standards applicable to an Authorised Certification Entity that want to provide time-stamping services:

- ETSI TS 102 023 [i.18] related with the policy requirements for time-stamping authorities; and,
- ETSI TS 101 861 [i.16] related with the time-stamping profile.

5.4.3.4 Trust representation

Section 6.5 of the "Minimum operational procedures for ICP-Brasil Trust Service Providers" document (ref: DOC-ICP-17.01) defines the Trusted Service Providers List (LPSC in Portuguese) contains the accredited entities under ICP-Brazil as Trusted Service Providers. The list LPSC is required to be published by AC Root and updated within 180 days.

The LPSC list is required to be published in the root CA repository in textual format for human reading, and in XML format in order to process it by machine.

The authenticity and integrity of the machine-readable list compilation is ensured by means of an XMLDSig digital signature supported by an ITI digital certificate.

The LPSC list versions and the certificate that signs the list is required to be published in the Root CA repository, a link for which is available below in the reference table.

Trusted parties is required to verify the authenticity and integrity of the list before any use.

Finally, the LPSC list is encoded in XML format in accordance with the structure proposed by the standard ETSI TS 102 231, and contains the following data:

a) Information related with the scheme *(SchemeInformation)*, where the following data is presented: sender identification data, ITI data, and the date of the list next update *(NextUpdate)*;

b) The service providers list (*TrustServiceProviderList*), which contains an entry (*TrustServiceProvider*) for each Trust Service Provider accredited in front of ICP-Brasil; and,

c) Digital signature in XMLdSIG format.

5.4.3.5 Reference Material

5.4.4 Chile

5.4.4.1 Legal context

Chilean Law 19799/2002 on electronic documents, electronic signature and signature certification services (from here on: Law 19799) regulates:

- the use of electronic signature by Chilean public institutions (Title II);
- the Certification Service Providers (Title III);
- the electronic signature certificates (Title IV);
- the accreditation and supervision processes on Certification Service Providers (Title V);
- rights and obligations of electronic signatures users (Title VI);

Chilean Decree 181/2002 approves the Regulation on Chilean Law 19799 on electronic documents, electronic signature and signature certification services (from here on: Decree 181) and, besides the aspects regulated in the Law 19799, regulates:

- the use of electronic signature by individuals (paragraph 2º);
- the use of technical standards in these cases:
  - Certification Practices;
  - Security;
  - Certificate Profiles;
  - Data repositories;
  - Time-stamping;
  - Electronic DNI (i.e. a national document issued by a state identifying an individual) and biometrical identity;
  - Mobile signature services;
  - for a suitable use of certificate-based electronic signature policies (profiles, syntaxes, CRL and OCSP profiles, use of certain OID's).

Finally, Chilean Decree 24/2019 (from here on: Decree 24) approves an additional regulation for the provision of an advanced electronic signature certification service, and regulates:

- the conditions under which the Certification Service Providers will recognise the system "ClaveÚnica" (an IdP operated by the Government) as a verification method to check the identity of an advanced electronic signature certificate applicant; and,
- the technical specification of the devices that may contain advanced electronic signature certificates, allowing the provision of certificate with signature creation data generated and managed by the certification services provider on behalf of the signatory, thus allowing the remote creation of advanced electronic signatures.

As we said, Chilean providers are not called Trust Service Providers, as in the EU, but rather are known as Certification Service Providers or simply Certifier (somehow in line with EU Directive 99/93/CE).

According to Article 14 of the Decree 181, the Chilean Accreditation Entity function will be developed by the Undersecretary of Economy, Development and Reconstruction, which for this purpose may contract experts whose contracts will incorporate rules on administrative probity. In this sense, highlight that the Undersecretary of Economy, Development and Reconstruction functions are now the conducted by Undersecretary of Economy and Small Businesses.

According to Article 35 of the Decree 181, an accredited certification services provider may approve advanced electronic signature certificates issued by providers that are not established in Chile under their own responsibility. To that end, the accredited certification services provider is required to demonstrate to the Accreditation Entity that the certificates approved by it have been issued by a certification service provider not established in Chile that complies using technical standards equivalent to those approved in accordance the regulations.

Once the certificate approval or a group of advanced electronic signature certificates approval has been done, the accredited certification service provider is required to communicate this situation to the Accreditation Entity within three days and it is required to be published immediately in the registration of public access indicated in the Decree 181.

The homologation practices is required to be declared in the Certification Practices.

Chilean regulation considers the following services:

- Provision of advanced electronic signature certificate generation service (Title II of the Decree 181); there are four different modalities of the certification service:
  - Based in smartcard or HSM for remote signature (Decree 24).
  - Based in a mobile device. It is called “provision of mobile signature service” (First Transitory Disposition of the Decree 181);
  - Based in a smartcard with biometric capabilities. It is called “provision of biometrical certification services” (First Transitory Disposition of the Decree 181);
- Provision of time-stamping services (First Transitory Disposition of the Decree 181);

5.4.4.2 Supervision and auditing

Accrediting

According to Article 17 of Law 19799 to get the accreditation, Certification Service Provider has to comply at least the following:

a) Demonstrate the required reliability of the services provided;

b) Guarantee the existence of a secure service in order to consult the register of issued certificates;

c) Employ qualified personnel to provide the services offered within the scope of the electronic signature and the appropriate security and management procedures;

d) Use reliable systems and products that guarantee the security of the certification processes employed by the Certification Service Provider;

e) Have contracted an appropriate insurance in the terms indicated in Article 14 of Law 19799; and,

f) Have the required technological capacity for the development of the certification activity.

Article 18 of Law 19799 describes the accreditation process:

a) The Certificate Service Provider submits an application to the Accreditation Entity accompanied by the requirements of Article 17 of Law 19799 (see above) and the proof of payment of the accreditation cost. In order to verify the requirements of Article 17 of Law 19799, the Accreditation Entity may contract specialists to do so;

b) The Accreditation Entity is required to give a reasoned decision on the request within a period of twenty days counted from when, at the request of the interested party, it is certified that the request is in a state of resolution;

c) If the interested party denounces the breach of that deadline in front of the Accreditation Entity and this entity don't make any resolution/statement within the following month, the request is required to be understood as accepted;

d) Once the accreditation has been granted, the Certificate Service Provider is required to be registered in a public registry in the charge of the Accreditation Entity. During the validity of its registration in the registry, the accredited Certificate Service Provider is required to inform the Accreditation Entity about any modification of the conditions that authorised its accreditation;

Beside this general accreditation procedure, the Chilean Undersecretary of Economy and Small Businesses has edited four useful guidelines to accredit specific services of a Certificate Service Provider, i.e.:

- Accreditation Assessment Procedure Guidelines Advanced Electronic Signature Certification Service Provider version 2.0;
- Accreditation Assessment Procedure Guidelines Mobile Signature Certification Service Provider version 1.1;
- Accreditation Assessment Procedure Guidelines TSA Certification Service Provider version 1.0;
- Accreditation Assessment Procedure Guidelines Biometric Certification Service Provider version 1.0;

Auditing

Article 20 of Law 19799 establishes that in order to verify compliance with the obligations of the accredited providers, the Accreditation Entity is required to exercise the inspection authority over that providers and for that purpose the Accreditation Entity may request information and order visits to the providers facilities though specially hired public workers or specialists in accordance with the regulation.

Section 2.4 of annual inspection guidelines for Certificate Service Providers v.2.1 establishes that the auditing process is required to have an annual periodicity and is required to follow the next steps:

1) Through a resolution the Accreditation Entity is required to set within the first quarter of each year the fees related with the accreditation and the supervision processes.

2) Each accredited certification services provider is required to pay the supervision fee within 90 days from the date of the resolution that establishes the fees (article 24 of Decree 181);

3) Once completed, each Certification Service Provider is required to present to the Accrediting Entity the proof of payment of the annual supervision costs, duly individualized, through the following information:

    a. Name or business name of the applicant company;

    b. RUT of the applicant company;

    c. Name of the legal representative of the applicant company;

    d. RUT of the legal representative of the applicant company;

    e. Registered office; and,

    f. E-mail address.

4) To begin the annual supervision, the Accreditation Entity is required to request the Certification Service Provider to deliver the following documents:

    a. Procedure foreseen to ensure access to specialists or experts (article 14 Decree 181);

    b. If applicable, copies of outsourced service contracts dated after their accreditation or the last annual inspection;

    c. All the documentation defined in the Accreditation Assessment Guidelines for each specified requirement that have been modified from the accreditation date to the inspection date, or between one inspection and the next;

5) The Accreditation Entity is required to check that all the required background information is presented;

6) Once all the information has been received, the Accreditation Entity is required to proceed to assess compliance with the requirements expressed in the Law, the Regulations and its transitory provisions. The applicant Certification Services Provider is required to facilitate the access of the public workers or specialists that the Accreditation Entity designates to perform the assessments. Besides, providers is required to provide any additional information requested by them:

7) Once the assessment has been carried out, in order to maintain accreditation, the Accreditation Entity is required to proceed to pronounce on whether the requirements and obligations required in the Law, the Regulations and the corresponding Accreditation Assessment Guidelines are met;

8) The Accreditation Entity may revoke the accreditation through a well-founded resolution for the reasons provided in Article 6 of Decree 181. That resolution is required to order the cancellation of the Certification Services Provider registration on the public registry held by the Accreditation Entity;

9) In the event that the Accreditation Entity determines as a result of the supervision that the breaches presented by the applicant Certification Services Provider are rectifiable and do not affect the correct functioning of the system or the purposes set forth in the Law 19799 on electronic signature, the Accreditation Entity is required to proceed to deliver a document indicating the unfulfilled requirements that will be corrected and request the provider to submit a corrective measures plan and the deadlines established to do so;

10) Once the corrective measures plan proposed by the Certification Services Provider has been received, the Accreditation Entity will proceed to evaluate it. If the plan is not approved, the Accreditation Entity is required to proceed as indicated in numeral 8;

11) If the assessment is favourable, the Accreditation Entity is required to inform the Certification Services Provider about the maintenance of its registration in the public registry held by the Accreditation Entity.

5.4.4.3 Best practice

According to Article 47 of the Decree 181, the Ministry General Secretariat of the Presidency is the responsible for proposing the technical standards to be used in the Public Administration to the President of the Republic. To do so, the entity is required to adopt international technical standards issued by recognized entities in this subject. The entity is required to make a biannual revision in order to update the technical standards.

On the other hand, section 2.7.2 of the Accreditation Assessment Procedure Guidelines Advanced Electronic Signature Certification Service Provider version 2.0 establishes that the National Normalization Institute, at the request of the Accreditation Body, is required to proceed to the generation or homologation of standards depending on the case. Once the process is done, these standards will become part of the set of current technical standards.

Chilean Accreditation Assessment Procedure Guidelines establish the use of the following ETSI's standards:

- Related with the Advanced Electronic Signature:
  - ETSI TS 102 231 [i.19] (trust model);
  - ETSI TS 102 042 [i.17] (Business Continuity Plan and Disaster Recovery Plan; Keys Management Plan Assessment; Certification Service Provider Technologic Platform assessment and accreditation; physical security of the Certification Service Provider infrastructure; Advanced Signature Certificate Policy; Certification Practice Statement; and, full assessment of the personnel profiles at the Highly Reliable level);
- Related with the biometric service:
  - ETSI TS 102 042 [i.17] (physical security of the Certification Service Provider infrastructure providing biometric services)
- Related with time-stamp service:
  - ETSI TS 102 042 [i.17] (Business Continuity Plan and Disaster Recovery Plan; Time-Stamp Authority Technologic Platform assessment and accreditation; physical security of the Certification Service Provider infrastructure);
  - ETSI TS 102 023 (Time-stamp Policy; Time-Stamp Practice Statement; Time-Stamp Authority operational model; Time-Stamp Authority operation manual).

- Related with mobile signature service:
  - ETSI TS 102 023 (Use of mobile devices; Mobile signature generation procedure);
  - ETSI TS 102 206 (Level of protection offered for the mobile signature generation procedure);
  - ETSI TS 102 042 [i.17] (Business Continuity Plan and Disaster Recovery Plan; Mobile signature service technologic Platform assessment and accreditation; Mobile Signature Policy; Mobile Signature Practice Statement).

5.4.4.4 Trust representation

According to Article 18 of the Law 19799 once the accreditation has been granted, the Certification Service Provider is required to be registered in a public registry in the charge of the Accreditation Entity.

Also, according to Article 16 of the Decree 181 the Accreditation Entity is required to maintain a public registry of accredited certification service providers. This registry is required to contain the number of the resolution granting the accreditation, the name or registered name of the certifier, the registered office, the name of its Legal Representative, the phone number, its electronic domain site and email as well as the insurance company with which the provide has contracted the insurance policy.

Finally, section 2.7.5 of the Accreditation Assessment Procedure Guidelines Advanced Electronic Signature Certification Service Provider version 2.0 set out the name of the accredited service providers register: Accredited Certification Services Providers Register.

5.4.4.5 Identified enablers

- Adoption of ETSI TS 119 431-1 and ETSI TS 119 431-2 for the remote signature components, which does necessarily imply the adoption of CEN EN 419 241-1, but not of CEN EN 419 241-2, allowing using FIPS 140-2 [i.13] based solutions.
- Alignment of the current ETSI standards admitted in Chile to the last ETSI EN versions. The mobile based advanced electronic signatures certification is based in deprecated ETSI standards (to my knowledge).

5.4.4.5 Reference Material

5.4.5 Columbia

5.4.5.1 Legal context

Colombian Law 527 through which the access and use of data messages, electronic commerce and digital signatures is defined and regulated, and certification entities are established and other provisions are issued (18/08/1999) (from here on: Law 527) regulates:

- the use of digital signature and the requirements to fulfil to make it equivalent to a handwritten signature (Part III; Chapter I);
- the Certification Entities activities, requirements and obligations (Part III; Chapter II);
- some certificate related features, i.e. information to be included in the certificate; certificate acceptance; certificate revocation; record preservation (Part III; Chapter III); recognition of foreign certificates (Part III; Chapter VI);
- subscriber's liability and obligations (Part III; Chapter IV);

Colombian Decree 1747 through which the Law 527 is partially regulated in relation to certification entities, certificates and digital signatures regulates:

- the use of repositories;
- the use of time-stamps;
- the closed Certification Entities requirements, including the accreditation process (article 3);

- the open Certification Entities requirements, including the accreditation process; the Certification Practice Statement minimum contents; minimum capital; warranties; personnel, physical and technological infrastructure, security procedures and systems requirements; outsourced services; audit requirements; Certification Entities obligations and the (article 5 to 14);
- the use of digital certificates (article 15)
- the use of online certificate status information related with the certification revocation process, and also a register of certificates containing all the certificates issued, including its issuance expiration or revocation date (articles 23 and 24);
- the Superintendence of Industry and Commerce faculties, including the suspension or revocation of the Certification Entities accreditation (article 26); the establishment of technical standards (article 27)

Other aspects in the scope of these two regulations are:

- Electronic data Exchange;
- Data messages and documents preservation;
- Data messages and documents preservation through a third party;

Colombian Decree 2364/2012 through which Article 7 on electronic signature of Law 527 is regulated, and other dispositions are dictated, regulates the use of the electronic signature, including a technological neutrality statement (article 2); electronic signature trustworthiness (article 4); signer's obligations (article 6); and, criteria to establish the degree of security of electronic signatures (article 8);

Articles 5 and 6 of Colombian Decree 333/2014 through Article 160 of Decree 19/2012 is regulated establishes that Colombian National Accreditation Body is the accreditation authority for those Certification Entities, open or closed, that wants to achieve a national accreditation in order to provide its services.

Considering all the legal document revised, the denomination for Trust Service Providers as used in the EU context is unknown; Colombian regulation only mentions Certification Entities

According to Article 13 of the Colombian Decree 333/2014 the recognition of certificates issued by foreign certification entities carried out by certification entities accredited for this purpose in Colombia, is required to be recorded in a certificate issued by the accredited certification entities.

The effect of the recognition of each certificate is required to be limited to the features of the certificate recognized and during the period of its validity.

Recognized certificates subscribers and third parties is required to have identical rights as the subscribers and the third parties with respect to the certificates of the entity that makes the recognition.

According to Article 161 of Decree 019/0212, accredited Certification Entities may provide the following services:

- Provision of electronic signature certificate generation for natural or legal person service:
- Provision of certificate generation on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents service;
- Provision of certified digital signature data creation service;
- Provision of electronic signature data creation service;
- Provision of data messages generation, transmission and reception registration and time-stamping services;
- Provision of electronic transferable documents registration, preservation and recording services;
- Provision of data messages and electronic transferable documents archive and preservation services;
- Any other activity related to the digital and electronic signatures creation or usage;
- Electronic data exchange services (EDI)

For each service, there are specific rules to be fulfilled. There is also one specific document that is generally applicable for Certification Entities seeking the national accreditation issued by the Colombian National Accreditation Body:

- Digital Certification Entities specific accreditation criteria

5.4.5.2 Supervision and auditing

In case of closed certification entities, according to Article 5 of Colombian Decree 333/2014, those entities requesting an accreditation to operate as a closed certification entity is required to specifically indicate the activities in which they intend to be accredited in accordance with the provisions of article 161 of Decree 19/2012 and demonstrate to the Colombian National Accreditation Body, in addition to the requirements set forth in Chapter III of Decree 333/2014, the following requirements:

- That the certification entities administrators and legal representatives have not incurred in any of the incapacity causes foreseen un section c) of Article 29 of the Law 527;
- That the applying certification entity complies with current national and international technical standards and with the specific accreditation criteria that the Colombian National Accreditation Body determines.

In case of open certification entities, according to Article 7 of Colombian Decree 333/2014, those entities requesting an accreditation to operate as an open certification entity is required to specifically indicate the activities in which they intend to be accredited in accordance with the provisions of article 161 of Decree 19/2012 and demonstrate to the Colombian National Accreditation Body, in addition to the requirements set forth in Chapter III of Decree 333/2014, the following requirements:

- Legal status or notary or consul status;
- That the administrators and legal representatives are not involved in the causes of incompetence provided in letter c) of Article 29 of Law 527;
- Satisfactory Certification Practices Statement (CPD), in accordance with the requirements established by the Colombian National Accreditation Body;
- Minimum capital of 400 legal monthly minimum wages in force at the time of the accreditation application and during all the validity period of the accreditation;
- Constitution of the guarantees provided for in Decree 333/2014;
- Infrastructure and resources at least in the manner required in Article 11 of Decree 333/2014;
- An immediate revocation procedure to revoke at all levels the certificates issued to subscribers at their own request or when any of the events set forth in article 37 of Law 527 occurs;
- Comply with current national and international technical standards and with the specific accreditation criteria established by the Colombian National Accreditation Body for this purpose.

5.4.5.3 Best practice

According to the Article 14 of the Colombian Decree 333/2014 establishes that according to the provisions of Article 162 of Decree-Law 19/2012, the Colombian National Accreditation Body is required to be responsible for carrying out, directly or indirectly through third parties, audits on certification entities, in accordance with the accreditation rules provisions and regulations specific criteria set by the Colombian National Accreditation Body.

According to the technical annexes of the document “Digital Certification Entities specific accreditation criteria” the following ETSI standards are in force:

- Digital certificates issuance activities (digital signature):
  - ETSI TS 102 042 [i.17] (certificate life-cycle).
- Time-stamping services activities:
  - ETSI TS (EN) 102 023 Policy requirements for time-stamping authorities

5.4.5.4 Trust representation

Considering all the legal document revised, the existence of a trust representation list or an equivalent measure is unknown.

5.4.5.5 Reference Material

5.4.6 Paraguay

5.4.6.1 Legal context

Paraguayan Law nº 4017 on electronic signatures, digital signatures, data messages and electronic file legal validity, and regulates its use (from now on: Law 4017 on electronic signature).

First of all, Law nº 4017 distinguishes between electronic signatures and digital signatures. The main difference between them is that the digital signature is a certified electronic signature issued by an accredited Certificate Service Provider and that has been created using means that the owner keeps under its exclusive control, so that it is linked only to that owner and to the data to which it refers, allowing the subsequent detection of any modification, verifying the holder's identity and preventing that the integrity of the document and its authorship remain unknown.

In the Spanish terminology, the electronic signature will be equivalent to an ordinary electronic signature, and the digital signature, to an advanced electronic signature.

The law also regulates certification authorities, called certification companies, the provision of certification services, data messages, including its preservation, the consignment and receipt of data messages, the legal validity of electronic signatures, digital signatures, data messages and electronic files, certificate revocation services and accreditation and audit processes.

These providers are not called Trust Service Providers, as in the EU, but rather are known as Certification Service Providers (somehow in line with EU Directive 99/93/CE).

According to articles 38 and 39 of Law nº 4610 that modifies and expands the Law 4017 on electronic signature establishes that the Industry and Commerce Ministry, through the Vice Ministry of Commerce, will act as the Application Authority, and that one of its functions is to authorize the operation of certification entities in Paraguay and to supervise and audit these certification entities.

According to article 21 of the Decree 7369 establishes that the Application Authority may enter into mutual recognition agreements with similar entities, in order to recognize the validity of the digital certificates granted abroad and extend the validity of the digital signature. Mutual recognition agreements will guarantee equivalently the functions required by the Law in these regulations.

According to Article 36 of the Law nº 4017 on electronic signature establishes two conditions in order to recognise digital certificates issued by foreign certifiers under the same terms and conditions required by Law nº 4017 on electronic signatures. Those rules are:

a) Those digital certificates is required to meet the conditions established by Law nº 4017 on electronic signature and the corresponding regulations;

b) Those certificates is required to come from foreign suppliers that are recognized or approved by the regulatory authority, authorizing that authority to regulate the procedure for this recognition or approval.

Also, Article 8 of Decree 7369 establishes that in case of a foreign entities, compliance with the requirements contemplated in Law nº 4017, in the Decree and all the other requirements established by the Application Authority is required to be accredited (see Supervision & auditing to meet the accreditation requirements).

Paraguayan legislation considers the following services:

- Provision of electronic signature certificates generation service (articles 15 to 19 of the Law 4017 on electronic signature).
- Provision of digital signature certificates generation service (articles 20 to 24 of the Law 4017 on electronic signature).
- Provision of time-stamping service (article 2 of the Decree 7369 by which the general regulation of the law 4017 on electronic signature is approved) (from here on: Decree 7369);

- Provision of digital certificates in software module issuance service for individuals, legal entities, machines and applications data messages preservation service (article 1 of the Resolution 217 by which authorized certification service providers are authorized for the term of twelve months to carry out the issuance of digital certificates in software module for individuals, legal entities, machines and applications data messages preservation service).
- Provision of data messages and digital document preservation services (article 8 of the Law 4017 on electronic signature).
- Provision of public files digitalization service (article 11 of the Law 4017 on electronic signature), and its preservation (article 4 of the Decree 7369);
- Provision of original document reproduction through electronic means (article 2 of the Decree 7369);
- Provision of data messages delivery (articles 12 to 14 of the Law 4017 on electronic signature).

For each service, there are specific rules to be fulfilled. There are also two specific rules that are generally applicable for all types of certification service providers since they contain the audit requirements applicable to all the Paraguayan Certification Service Providers.

- Resolution nº 1105, of 29 of September of 2015, "by which the audit system to which the Certification Service Providers will be submitted to is established and approved, and by which the articles 3, 4 and 6 of the Resolution nº 164/14 are ineffective" (from now on: Resolution 1105)
- Resolution 1430/17 by which the annex of the Resolution nº 1105 is modified partially (from now on: Resolution 1430).

5.4.6.2 Supervision and auditing

According to Article 28 of the Law nº 4017 on electronic signature, the Certification Services Providers is required to meet the following requirements in order to obtain an accreditation to operate as a provider:

a) Guarantee the use of a fast and safe user guide service and a safe and immediate revocation service;

b) Ensure that the date and time when a certificate was issued or revoked can be accurately determined;

c) Duly verify, in accordance with national law, the identity and, if applicable, any specific attributes of the person to whom a recognized certificate is issued;

d) Employ personnel who have the specialized knowledge, experience and qualifications required for the services provided; in particular, competence in management, technical knowledge in the field of electronic signature and familiarity with the appropriate security procedures; they also is required to put into practice the appropriate administrative and management procedures compliant with the recognized standards;

e) Use reliable systems and products that are required to provide certification services and that are protected against any alteration and that can guarantee the technical and cryptographic security of the procedures with which they work;

f) Take measures against certificate forgery and, in the event that the Certification Service Provider generates signature creation data, guarantee confidentiality during the process of generating that kind of data

g) Have sufficient economic resources to operate in accordance with the requirements of the Law, in particular to deal with the risk of liability for damages, and may be used as deposits, guarantees, insurance or any other means;

h) Record all relevant information related to a certificate recognised for an appropriate period of time, in particular to provide evidence of certification in legal proceedings. This registration activity may be carried out by electronic means;

i) Not store or copy the signature creation data of the person to whom the Certification Service provider has provided electronic signature assignment services;

j) Use reliable systems to store certificates verifiably, so that:

- Only authorized persons can make annotations and modifications;

- The authenticity of the information can be checked;
- The certificates are available to the public for consultation only in those cases in which the consent of the certificate holder has been obtained; and
- The agent can detect all technical changes that call into question the aforementioned safety requirements;

k) Demonstrate the honesty of their legal representatives, administrators and officials, through police and judicial background certifications.

On another hand, article 7 of the Decree 7369 establishes the following accreditation process for Certificate Service Providers:

a) Submission of the application to the Application Authority, accompanied by proof of payment of the costs of the authorization and proof of the background that allows the verification of the accreditation requirements compliance with the exception of the insurance policy. In the application, the interested party is required to indicate: name or social reason, Unique Taxpayer Registry, name and identity document number of the legal representative, address, email address, and is required to expressly accepting that said electronic means as a form of communication;

b) The Application Authority is required to verify the admissibility of the required background within five working days;

c) Once the application is accepted, the Authority is required to examine compliance with the requirements and obligations of the Law and the regulations to obtain the certification/accreditation (30 days after admissibility, a period that may be extended once, for the same 30 days, and always with founded grounds to do so);

d) The interested party that meets the requirements to be qualified has 5 days to submit the insurance policy required by law (otherwise the application is denied);

e) The Authority is required to proceed to enable the interested party in order to operate its services. The Authority may, at any time, request additional documentation and/ or may visit the facilities of the interested party; and,

f) If the application is inadmissible, the interested party is required to be informed within 10 working days, so that the interested party will have 5 days to complete the background information (article 9 of the Decree 7369).

Finally, article 8 of the Decree 7369 establishes some other requirements for those Certification Services Provider that want to have the accredited condition; i.e.:

a) Proof of legal status;

b) Authenticated copy of the constitution of the company;

c) Minutes of the last assembly;

d) Document proving legal representation;

e) Tax compliance certificate;

f) Certificate of not being bankrupt, notice of creditors or interdiction;

g) Record of being up to date with social security;

h) Minimum capital of two hundred (200) minimum salaries for various activities not specified in the capital at the time of authorization;

i) Identification of a directory of current certificates and an immediate enforcement mechanism to revoke digital certificates;

j) Satisfactory document of certification policies in accordance with the requirements established by the Application Authority;

k) Proof that the provider has a team of people, a physical and technological infrastructure and security procedures and systems, to comply with the following obligations:

- Generate its own digital signatures and all the services for which the provider request authorization;
- Guarantee compliance with the requirements of the certification policies;
- Guarantee the existence of physical security systems in its facilities, permanent monitoring of all its physical plant, and restricted access to the equipment that manages the operation systems of the entity
- Ensure that the management of the private key of the entity is subject to a security procedure that prevents access to unauthorized personnel;
- Keep a record of all transactions carried out, which allows to identify the author of each of the operations;
- Ensure that the systems comply with the certification functions are only used for that purpose and can not perform any other function;
- Ensure that all systems that participate directly or indirectly in the certification function are protected by high-level protection and authentication systems and procedures, which will be updated according to technological advances to guarantee the correct provision of the service
- Constitute the guarantees provided in this document;

Article 42 of the Law nº 4017 the Application Authority is required to design an audit system to periodically audit the Paraguayan Certification Service Provider. That audit system may be implemented by the Application Authority or by a third party authorised for this purpose. The audits will at least evaluate the reliability and quality of the systems used, the integrity, confidentiality and availability of the data, as well as compliance with the regulations in force.

According to Article 20 of the Decree 7369 the authorities may performance verification visits to the accredited Certification Service Provider in order to verify the compliance with legal requirements.

The verification visits may have an ordinary or an extraordinary nature. The difference between one and another is that while the ordinary means an annual visit to the facilities of the accredited Certification Service Provider, as the faculty of requesting half-yearly information on the development of the activity, the extraordinary will be practiced ex officio or by a reasoned complaint on the provision of the service ordered by the Application Authority through a well-founded resolution.

Finally, specialized examiners may carry out inspections and, in the performance of their duties, they may require the certifier to provide additional information to the one provided.

5.4.6.3 Best practice

According to the articles 38 and 39 of the Law nº 4610 that modifies and expands the Law 4017 on electronic signature establishes that the Industry and Commerce Ministry, through the Vice Ministry of Commerce, will act as the Application Authority, and that one of the functions of the Application Authority the technological and operational standards for the implementation of the regulation.

Resolution 501/16, which approves and enforces the guide of technological standards and safety guidelines for the qualification and audit to Certification Services Providers, set up the standard ETSI TS 102 042 [i.17] as an assessment standard applicable to:

- Certification Statement Practice (CSP);
- Certification Policy (CP);
- Registration Authority Operation Model of the Certification Service Provider
- Certification Authority Operation Manual;
- Registration Authority Operation Manual;
- Personnel assessment; and,
- Key Administration Plan (Implementation and maintenance);

5.4.6.4 Trust representation

According to article 26 of the Law 4017 on electronic signature once a certification service provider has been enabled, he or she is required to self-assign a digital signature, and is required to submit the verification key to the regulatory authority, that will have a registry of certification service providers authorized in the Republic of Paraguay. That register can be used to verify the digital signature of the provider.

According to article 10 of the Decree 7369 that register is called: Public Register of Certification Service Providers.

5.4.6.5 Reference Material

5.4.7 Peru

5.4.7.1 Legal context

Peruvian Law N° 27269 of 8th of May 2000 (The Digital Certificates and Signatures Law) rules the usage of electronic signatures, with a special focus on digital signatures based on digital certificates. The law also regulates certification authorities, registration or verification authorities and repositories. These providers are not called Trust Service Providers, as in the EU, but rather are known as Digital Certification Service Providers (somehow in line with EU Directive 99/93/CE).

The Law, however, does not define other trust services, but the Supreme Decree N° 52/2008 of 18th of July 2008 defines Added Value Service Providers (AVSP) as public or private entities that offer services that include digital signatures and the use of digital certificates. The definition includes AVSPs acting in procedures without final users' digital signatures, such as issuing time stamps, or AVSPs acting in procedures with final users' digital signatures, such as intermediators between two parties (e.g. capturing final users' digital signatures).

According to Article 15 of Law N° 27269, the government is responsible for designating an administrative authority that defines the technical standards to be applied by the aforementioned entities. This designated administrative authority is the National Institute for the Defense of Free Competition and the Protection of Intellectual Property, also known as INDECOPI (Article 57 of Supreme Decree N° 52/2008).

According to Article 71 of Supreme Decree number 52/2008, INDECOPI may enter into mutual recognition agreements with foreign entities that perform similar functions, in order to recognize the validity of the digital certificates granted abroad and extend the interoperability of the supervision system called IOFE (Official Infrastructure of Electronic Signature). These mutual recognition agreements will guarantee equivalently the functions required by the Law and its respective Regulations.

According to Article 11 of Peruvian Law N° 27269, drafted by Law N° 27310 of 26th of June 2001 and Article 72 of Supreme Decree 52/2008, digital certificates issued by foreign entities will have the same validity and legal effect recognised by Peruvian law if these certificates are recognised by INDECOPI in the framework of the IOFE. This recognition process, which is different to the accreditation process applicable to national providers, is not subject to any reciprocity principle. The recognition process is also based in a set of policies and practices approved by INDECOPI, with the aim to guarantee the compliance of the provider's obligations and legal duties. This process also covers the situation in which a Peruvian provider uses the services of a foreign provider.

Finally, according to Article 73 of Supreme Decree number 52/2008, it is possible for a Peruvian provider, with a previous authorization by INDECOPI, to enter intro cross-certification agreements with foreign providers. In this case, the foreign certificates are recognised by the Peruvian provider and are incorporated to the IOFE. The Peruvian provider will guarantee that these foreign certificates have been issued in compliance with analogous requirements to IOFE certificates, and that the certificates comply with the functions described in Article 2 of Law N° 27269 (essentially equivalent to eIDAS advanced electronic signatures).

Thus, as far as other requirements of a digital signatures are met, a digital signature based in a foreign digital certificate that has been recognised by INDECOPI under the IOFE framework, in any of the three aforementioned cases, would be legally valid and effective in Peru.

Peruvian legislation considers the following services:

- Provision of digital certificates for digital signatures. This would be equivalent to the provision of eIDAS qualified certificates for qualified electronic signatures.

- Enrolment of subscribers for the provision of digital certificates for digital signatures. Contrary to the eIDAS model, under Peruvian legislation, this activity is considered as an independent service, even offered by a provider that does not issue certificates.
- Provision of added value services with final users' digital signatures, including the electronic delivery or archival of signed electronic documents.
- Provision of added value services without final users' digital signatures, limited to the provision of time stamps.

For each service, there are specific rules to be fulfilled. No rules currently exist that are generally applicable for all types of service providers.

5.4.7.2 Supervision and auditing

To be part of the IOFE, a Digital Certification Service Provider will be previously accredited or recognised by INDECOPI. The main difference between both processes is that accreditation is aimed at providers that are incorporated under Peruvian legislation or that are established in Peru, whereas recognition is aimed at foreign providers (Article 72 of Supreme Decree 52/2008).

The accreditation process may be seen analogous to the eIDAS qualification process. It requires the filing of an application by the service provider with INDECOPI, that will be accompanied by specific documents regarding compliance to legal requirements and an evaluation (audit), which will completed before accreditation is approved.

The audit is performed according to a scheme owned by INDECOPI (identified as PE-CFE-02), that establishes an audit procedure (identified as PE-CFE-01), criteria for the qualification of auditors, performance monitoring and training of evaluators, functions and compromises of auditors, profiles of auditors and a matrix for segregation of duties.

The accreditation is valid for five years, but the audit will be repeated on an annual basis.

Once a provider has been accredited or recognised, the provider is subject to the supervision process (Articles 74 and 75 of Supreme Decree N° 52/2008), which allows INDECOPI to verify the correct provision of services offered by the accredited providers, and to sanction any infringement by service providers of their legal obligations and duties, according to a specific Regulation (approved by Resolution of the Presidency of the Management Board of INDECOPI, number 39/2017 of 28th of February 2017).

5.4.7.3 Best practice

According to Article 21 of Supreme Decree N° 52/2008, INDECOPI is responsible for determining the standards compatible with the IOFE, applying the principle of technical neutrality and the criteria that will enable the interoperability between components, applications and digital signature infrastructures analogous to the IOFE.

According to Article 22 of Supreme Decree number 52/2008, in order to guarantee compliance with the security requirements necessary for the implementation of the components and applications of the IOFE, three levels are established: Medium, Medium High and High, which are defined by INDECOPI. The security level High is used, for example, in military applications.

In order to be accredited, it is mandatory that the aforementioned technical standards are fulfilled by the providers. Each accreditation process includes an annex listing the concrete applicable technical standards. It should be noted that these listings refer to a number of the ETSI and CEN standards for eIDAS.

5.4.7.4 Trust representation

Once a service provider is accredited or recognised, it is included in an official registry, known as ROPS, operated by INDECOPI, according to Article 3 of Supreme Decree N° 26/2016 of 28th of April 2016. This official registry is available below in the reference table. The ROPS is implemented as a Trusted List, using ETSI TS 102 231, offering XML and PDF versions.

5.4.7.5 Identified enablers

- ERDS
- TSA
- TSL update.

5.4.7.6 Reference Material

5.4.8 Uruguay

5.4.8.1 Legal context

Uruguayan Law 18.600 through which the validity and legal effectiveness of the electronic document and the electronic signature are recognized (21/09/2009) (from here on: Law 18.600) regulates:

- the use of electronic signature;
- the use of advanced electronic signature;
- the National Electronic Certification Infrastructure (Chapter II);
- the Electronic Certification Unit obligations (accreditation; control; regulation; sanction function) (Chapter III);
- Recognised Certificates (certificate content; applicant identity verification; certificate validity; certificate equivalency) (Chapter IV);
- Signers' rights and obligations (Chapter V);

This Law also defines:

- Electronic signature;
- Advanced electronic signature;
- Electronic time-stamp;
- Electronic Certificates;
- Electronic or digital document;
- Signature Creation/Verification Data;
- Signature Creation/Verification Device;

Uruguayan Decrees 436/2011 (19/12/2001) and 70/2018 (19/03/2018) regulates the following aspects:

- the use of centralised custody advanced electronic signature services (Chapter IV Decree 70/2018);
- the Trust Service Providers accreditation procedure (Chapter VI Decree 70/2018);
- the Certification Service Providers accreditation procedure (Chapter V Decree 436/2011)
- Accredited Certification Service Providers Register (Chapter VI Decree 436/2011)
- the accredited Trust Service Providers monitoring and control (Chapter VII Decree 70/2018);
- the accredited Certification Service Providers monitoring and control (Chapter VII Decree 436/2011);
- the relationship between Trust Service Providers and Certification Service Providers (Article 31 Decree 70/2018);

These providers are called Trust Service Providers (Decree 70/2018), as in the EU, but they also are known as Certification Service Providers (Law 18.600) (somehow in line with EU Directive 99/93/CE).

According to Article 24 of Uruguayan Law 18.600 recognised certificates may be issued by entities not established in the national territory and is required to be equivalent to recognised certificates issued by accredited Certification Service Providers, provide that there is an international in force agreement ratified by the Oriental Republic of Uruguay and is in force.

According to Uruguayan regulations trust services are defined as certification services. Article 12 of Decree 436/2011 defines the following certification services:

- Provision of Certification Authority services;
- Provision of Registration Authority services; and,
- Provision of Electronic Time-Stamping services.

On the other hand, section 1.8 of the natural person advanced electronic signature policy with centralized custody defines the following trust services:

- Provision of advanced electronic signature policy with centralized custody services;
- Provision of digital identification services;
- Provision of time-stamping services; and,
- Provision of other services established by the Electronic Certification Unit (from here on: ECU).

For each service, there are specific rules to be fulfilled.

5.4.8.2 Supervision and auditing

Accrediting

According to Article 13 of Uruguayan Decree 436/2011, the Certification Service Provider accreditation process begins submitting to the ECU an application containing the following information:

- For natural persons:
  - Name and surname;
  - Identity document;
  - Registered postal address, also being able to establish an electronic address in an electronic mail box;
  - Be legally registered in the Unique Tax Registry and in the Social Security Bank; and,
  - Good behaviour accreditation;
- For legal persons:
  - company name and trade name as applicable;
  - legal person accreditation, its validity and the invoked representation;
  - registered postal address, also being able to establish an electronic address in an electronic mail box;
  - Be legally registered in the Unique Tax Registry and in the Social Security Bank; and
  - Managers good behaviour accreditation;
- Accredit economic solvency;
- Proof of the existence of service contracts provided by third parties, if any;
- Models of contracts to be subscribed with the users and applicant privacy policy;
- Technical-legal audit report prepared by independent auditors chosen from those who were authorized by the ECU. The report is required to state that the applicant is able to act in accordance with the requirements established in the laws, regulations and other applicable technical regulations. The audit procedure is required to be carried out according to the protocol defined by the ECU.
- Describe in detail the technological platform including a detailed detail of hardware, software and communication devices with which it has, its characteristics and functionality;
- Inform the security plans and procedures that guarantee the provision of certification services;
- Present the declaration of certification practices; and,

- Comply with any other requirement that the ECU deems necessary.

According to Article 14 of Uruguayan Decree 436/2011, the requirements demanded in the accreditation application is required to be met while the accreditation is in force and be communicated to the UCE when there is a change in any of them within a maximum period of 10 calendar days since the modification is done.

Article 15 of Uruguayan Decree 436/2011 establishes the admissibility control: once the application has been received, its admissibility is required to be verified within the fifth working day. To do so it's required to check the submitted information.

If there are observations, these will be notified to the applicant who will have ten working days to correct them. In case of not doing so, the request is required to be considered rejected.

Once the application has been admitted, it will be analysed and assessed within sixty days, producing the necessary reports and the corresponding resolution project. This period may be extended once and for the same assessment period (sixty days).

If the result of the resolution is the denial of the accreditation application, the applicant is required to be notified, and is required to have ten working days to evacuate the corresponding view of discharges as established in article 75 of Decree Nº 500/991.

Once the accreditation application has been technically approved it is required to be communicated to the applicant who will have twenty calendar days counted from the day following to the notification date to present the guarantee provided for in Article 11 of Decree 436/2011.

The accreditation will be granted to the applicant for the term determined by the ECU and is required to be subject to the inspections and audits requires by the ECU as established in Chapter VII of Decree 436/2011.

The Certification Service Providers may request the accreditation renewal and, to do so, they is required to comply with the requirements that the ECU deems suitable such as the audit, the patrimonial status or the antecedents.

Auditing

Numeral 1 of the Resolution 2/2019 (23/01/2019) establishes that electronic signatures accredited Certification and Trust Service Providers is required to present assessment audits every two years without prejudice to extraordinary audits requested by the ECU. This numeral also establishes that the audit assessment framework is required to be the last WEBTRUST version.

Article 28 of the Decree 436/2011 establishes that audits and technical assessments is required to be ordered though a reasoned resolution ex officio or by users sustained complaints on the services provided. The resolution is required to indicate the systems or procedures that will be audited and assessed.

The ECU may at any time by itself or using the services of public bodies, individuals or legal entities accredited for this purpose, perform inspections of the facilities and perform technical assessments, order audits on systems and procedures, and require any documentation related with the provision of services that the ECU considers necessary to guarantee the correct provision of the services regulated by Law 18.600 and its regulations.

In both cases (accrediting and auditing) the entity designated to fulfil its functions is the ECU (Article 14 of the Law 18.600).

5.4.8.3 Best practice

According to section 5 of the natural person advanced electronic signature policy with centralized custody defines the use of the following ETSI qcStatements:

- Id-etsi-qcs-QcCompliance
- Id-etsi-qcs-QcSSCD

5.4.8.4 Trust representation

According to Article 18 of Decree 436/2011 the Certification Service Provider accreditation is required to produce the following effects: Incorporation to the Accredited Certification Services Providers Registry referred in Chapter VI of this Decree.

Also Article 18 of Law 18.600 determines the creation of an Accredited Certification Services Providers Registry in charge of the ECU.

Finally, Article 29 of Law 18.600 establishes a period of ninety days to carry out the transfer of the Certification Services Providers Registry, under the responsibility of the Communications Services Regulatory Unit, to the Accredited Certification Services Providers Registry, created by this law in the ECU.

5.4.8.5 Reference Material

5.5 The Middle East & Africa

5.5.1 AAECA Net

5.5.1.1 Legal context

The Arab Information and Communication Technologies Organization (AICTO) is a specialized Arab governmental organization working with support from the league of Arab States and is located in Tunis.

The Arab-African e-Certification Authorities Network (AAECA-Net) is an interregional multi-stakeholder network for electronic trust in the Arab and African regions. The overarching objectives of the AAECA-Net are the formation and maintenance of a common network of stakeholders in the Arab world, to see to the convergence of related legal frameworks, to open channels of interoperability and mutual recognition and to facilitate cooperation, both inter-regionally and internationally.

They are just building their internal framework and establishing practices to understand and adapt to the regional and international PKI and trust service environment.

AAECA-Net WG3 “E-Trust-L” (legal frameworks harmonization) is responsible for dealing with regulatory issues related to public keys and trust services management. This group will develop the regulatory framework under which the technical and supervisory standards and bodies will operate.

5.5.1.2 Supervision and auditing

At present, no information about an auditing scheme or framework.

5.5.1.3 Best practice

AAECA-Net WG2 “E-trust-T” (technical aspects) is responsible for the investigating the possibilities for introducing PKI and electronic trust services into the two regions, assessing best practices from regional and international stakeholders. By the first quarter of 2020 is expected the production of various studies including a Region Report, a white book entitled "PKI implementation in the Arab and African regions" and a capacity-building and training programme.

5.5.1.4 Trust representation

At present, no information about trust representation.

5.5.1.5 Reference Material

5.5.2 Israel

5.5.2.1 Legal context

Israel established its Electronic Signature Law, 5761-2001originally in 2001. This was last amended in 2010. This law is similar to the EU Electronic Signatures Directive 1999/93 and includes features such as Certified Signing Device, Registration of Certification Authorities, Revocation, Secure Electronic Signature, Certified Electronic Signature which may be related to requirements for advanced and qualified electronic signatures under eIDAS.

The certificates issued under this regulation can be used to support electronic identities as well as electronic signatures.

The trust services are used mainly to support citizen to government and citizen to business.

The Electronic Signature Law includes specific provisions for the inclusion of "foreign" certification authorities in Israel's register.

5.5.2.2 Supervision and auditing

Certification Authorities (TSPs) are audited against CEN Workshop Agreement – CWA 14167-1, a risk analysis and a review of certification practice statement based on RFC 3647

Auditors are approved by the Ministry of Justice but with no specific accreditation requirements.

5.5.2.3 Best practice

Other than – CWA 14167-1, and the high-level requirements in the Electronic Signature Law, there are no specific requirements placed on TSPs.

5.5.2.4 Trust representation

Only 2 CAs are registered under the Electronic Signature Law in Israel. A list of approved CA are listed on the ministry of justice web site with information on their root certificates published in a national newspaper.

5.5.2.5 Reference Material

5.5.3 Oman [In progress]

5.5.3.1 Legal context

5.5.3.2 Supervision and auditing

5.5.3.3 Best practice

5.5.3.4 Trust representation

5.5.3.5 Reference Material

5.6 Asia / Pacific

5.6.1 China

5.6.1.1 Legal context

The legal context in China for electronic trust services is predicated on the 2004 "Electronic Signature Law of the People's Republic of China", in which TSPs are referred to as "electronic verification service providers". Regional trust services are established based within this legal environment; banks and other organizations, however, can develop and deploy their own PKI systems. In fact, the banking industry is required to use PKI-based electronic authentication and/or electronic signatures for transactions above a specified limit, though interoperability is limited and customers should use private keys specific to their own bank.

5.6.1.2 Supervision and auditing

Presently no information about supervision and auditing.

5.6.1.3 Best practice

Presently no information about best practice.

5.6.1.4 Trust representation

Presently no information about trust representation.

5.6.1.5 Reference Material

5.6.2 Hong Kong

5.6.2.1 Legal context

The "Electronic Transaction Ordinance" of 2000 comprises at least part of the Hong Kong legal context for electronic trust services, with the root certificate operated by Hong Kong Post. Specific implementations include an electronic identification scheme project, e-governance and e-commerce applications, with optional usage for banking applications. No third-party trust providers are currently part of the PKI ecosystem; Hong Kong Post electronic certificates services is operated by "Certizen", a private-sector enterprise (a link to which is provided below).

5.6.2.2 Supervision and auditing

Presently no information about supervision and auditing.

5.6.2.3 Best practice

Presently no information about best practice.

5.6.2.4 Trust representation

Presently no information about trust representation.

5.6.2.5 Reference Material

5.6.3 India

5.6.3.1 Legal context

For the PKI scheme managing Digital Signature Certificates (DSC) in India, the Root Certificate Authority is operated by the Government of India, a regulatory branch called the Controller of Certifying Authorities (CCA). Certificates are used for governmental, enterprise and personal uses, including: tax-filing, company legal filings, e-tendering, import/export, banking, financial institutions, digital locker, corporate/enterprise document-signing, e-invoicing, among others. The basis for trust decisions lies in the licensing process, including qualification and audit criteria as well as the audit results themselves.

The CCA has established the Root CA of India (RCAI) under section 18(b) of the IT Act to digitally sign the public keys of CAs in the country. The RCAI is operated as per the standards laid down under the Act. The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The CCA certifies the public keys of CAs using its own private key, which enables users to verify that a given certificate is issued by a licensed CA.

The scheme functions similarly to ETSI TS 119 612 [i.20] on trusted lists in that the certificates are similar to EU qualified certificates. India has a root certificate authority-based trust chain; all relying parties trust this root. Identity vetting happens only through internal RAs or CAs as India does not permit external RAs to fulfil this function. Identity vetting is similar to ETSI, though it is perhaps more stringent due to the physical form requirement, for which vetting documents are not allowed to originate from electronic form. However, the national ID is a digital ID and is hence accepted in electronic forms. Video vetting is mandatory for all cases. Cloud signatures are permitted in India in the form of online electronic signatures, but they come with a short-lived key pair, which is based on online authentication made by the user.

For operating as a licensed CA under the IT Act, an application has to be made to the CCA as stipulated under Section 21 of the IT Act. The application form for grant of license prescribed under Rule 10 of the IT Act has to be submitted to the CCA. Before submitting the application however, the applicant is expected to have the entire infrastructure – technical, physical, procedural and manpower – in place. CAs can then apply for different services such as issuing different classes of certificates: time-stamping, e-signatures, SSL and code-signing, for example.

5.6.3.2 Supervision and auditing

The audit scheme, approvals and controls in India have several similarities with the eIDAS regulation, and is seen to have equivalence with ETSI EN 319 403.

On receipt of the application to become licensed Certifying Authority under the IT Act 2000, and after examination of the same along with the supporting documents, CCA will depute an empanelled auditor based on whose audit report a decision will be taken on whether a license can be granted to the applicant to operate as a Certifying Authority under the IT Act 2000.

Auditors are empaneled and accredited through a process conducted by the CCA; accreditation criteria is customized in individual scope and published by the CCA.

While these criteria equally cover similar to that of both ETSI and WebTrust criteria, the detailed report is not published for public viewing and is only released to trained, empanelled auditors. The criteria may also currently not be descriptive as a checklist, as for the other audit schemes, but is undergoing a transition to a more sophisticated version, which should be available in a year. No concrete timescale has yet been given.

The Indian CCA follows the following criteria for audits:

- Adequacy of security policies and implementation,
- Existence of adequate physical security,
- Evaluation of functionalities in technology as it supports CA operations,
- A CA's services administration processes and procedures,
- Compliance to relevant CPS as approved and provided by the Controller, and
- Adequacy of contracts/agreements for all outsourced CA operations.

Adherence to Information Technology ACT, 2000, the rules and regulations thereunder, and guidelines issued by the Controller from time-to-time.

5.6.3.3 Best practice

The CCA certificate practice statement (CPS) contains controls on the CAs that are similar or equivalent to ETSI EN 319 411-1 [i.24]: general provisions, liability, financial responsibility, fees, audit, identification and authentication, operational requirements, security audit procedures, physical and personnel security controls, technical security controls and others.

5.6.3.4 Trust representation

No requirements specified.

5.6.3.5 Identified enablers

One suggestion is to initiate an interoperability project to analyse how the certificates issued under the Indian CCA can be validated by eIDAS QTSPs.

5.6.3.6 Reference Material

5.6.4 Japan

5.6.4.1 Legal context

The Japanese PKI infrastructure is enveloped within an overarching legal framework, and separate advisory groups or standards institutes, acting under ministerial oversight, supervise individual branches of trust services and their providers.

The Act on Electronic Signatures and Certification Business (hereafter e-Signature Act) and the Law Concerning the Use of Information and Communication Technology for the Storage of Documents by Private Companies and Other Similar Purposes (hereafter e-Document Law), for example, set guidance for the provision of electronic trust services.

According to paragraph 1 of article 17 of the e-Signature act, a competent minister can require a designated investigative organization (DIO) to investigate all or part of the application process for a certification business. According to paragraph 4 of article 17, if the DIO performs this investigation, it is required to immediately notify the minister of the results. Additionally, the DIO may conduct investigations of new applications for the accreditation of

specified certification business, perform annual investigations of already issued accreditations and changes to an accredited certification business. The investigation methods used include both a document-based and an on-site audit. A review of documentation comprises a review of the CPS policies, an accreditation conformance criteria checklist, operation manual review, for example. The on-site audit comprises a facilities check as well as a review of the management and system tests, for example.

The Japanese Certification Authority Network (JCAN) Trusted Service Registration is a cloud service used to publish a list of reliable trust services, often for e.g. registered email and electronic contracts because these services are usually based on remote e-signature models. This service is exclusively specific to companies and individuals in Japan.

As the competent authority making trust decisions, JIPDEC oversees the JCAN Trusted Service Registration Assessment Committee, which provides auditing for applicant companies.

The primary differences between ETSI EN 319 411-1 [i.24] and EN 319 411-2 [i.25] and the e-Signature Act's Implementation Ordinance include:

- Accredited Certification Business CA of the e-Signature Act does not allow key escrow,
- The e-Signature Act does not specify concrete procedures at the time of CA termination,
- The e-Signature Act does not specify tamper prevention until receiving HSM,
- In the e-Signature Act, there is no financial status criterion for a CA (the CA submits the Specified Certification Business's closing notification to the competent ministry), and
- The CP/CPS of each Accredited Certification Business is created in compliance with RFC 2527.

The e-Documents Law permits private companies electronic storage of both electronic documents and computerized (digitized paper) documents, for which storage is mandatory as a record of evidence. Electronic signatures and time stamps are required to assure the integrity of these documents and their electronic storage.

5.6.4.2 Supervision and auditing

The basis for the "Accreditation of Specified Certification Business" scheme lies in the e-Signature Act and is managed by the Japanese Institute for the Promotion of Digital Economy and Community (JIPDEC); auditor accreditation requirements can be found in Articles 17 through 29. Criteria developed for the audit are based on the e-Signature Act, as well as its complementing "Implementation Ordinance" and "Guidelines on the Accreditation of Specified Certification Business".

As shown in Figure 4 below, the accreditation entity of e-Signature Act is Ministry of Internal Affairs and Communication (MIC), Ministry of Justice (MOJ) and Ministry of Economy, Trade and Industry (METI). These ministries certify a Specified Certification Business (SCB) and Designated Investigative Organization (DIO), which audits (the language of the original author is "investigates") the SCB. The DIO then reports the audit report to the competent ministry, who then receive and make a decision to or not to accredited the SCB. It should be noted that the DIO will be established in Japan.

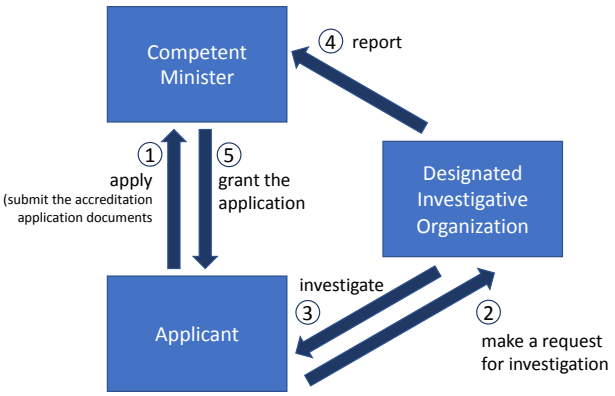


Figure 4 Accreditation scheme (derived from JIPDEC)

JIPDEC also oversees the Japanese Certification Authority Network (JCAN) Trusted Service Registration, a cloud service used to publish a list of reliable trust services, often for e.g. registered email and electronic contracts because these services are usually based on remote e-signature models. This service is exclusively specific to companies and individuals in Japan.

JADAC runs the accreditation program for time authorities (TA) and time stamping authorities (TSA), which is a voluntary program for time-stamping services. The program can approve the accreditation of the services of a TA and a TSA if they meet a set of required criteria which represent input from five distinct fields: (i) Technical issues, (ii) management and operation, (iii) facilities, (iv) network security and (v) disclosure and notification.

Accreditation is only awarded to TAs and TSAs with established businesses, including facilities and equipment for time business in Japan and presently submit an application for renewal every two years.

The basis for auditor accreditation requirements, according to the "JCAN Trusted Service Registration", is the JCAN Trusted Service Assessment Practice; the criteria used during an audit come from independent standards developed by JIPDEC, but are based on the following:

- Act on Electronic Signatures and Certification Business
- CA/B Forum Baseline Requirements
- WebTrust for Certificate Authorities
- ETSI TS 102 042 [i.17]
- ETSI EN 319 411-1 [i.24] and
- ETSI EN 319 411-2 [i.25]

Furthermore, and although not able to compare perfectly, JCAN Trusted Service Registration and ETSI EN 319 403 are about the same criterion and therefore can assume a level of equivalence in scope.

5.6.4.3 Best practice

Accreditation under JADAC of TA and TSA services references ISO/IEC standards, including :

- ISO/IEC 18014 parts 1 to 3 on time-stamping services [i.9]
- ISO/RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- ETSI TS 102 023 [i.18] Policy requirements for time-stamping authorities

With a view towards equivalence with ETSI EN 319 403, no information is yet available, though a study is currently underway to map existing Japanese standards to those in the EU for interoperability.

Reference of "JCAN Trusted Service Registration" to ETSI is made in preparation of the trust management criteria; therefore, there is a built-in equivalence to e.g. ETSI TS 119 612 [i.20] on trusted lists.

5.6.4.4 Trust representation

Upon accreditation, a certificate is issued by JADAC to the accredited service provider, who can then use the logo (a link to which can be found below), respective of the service provided.

Information about accredited JCAN trusted services is published to the Cyber Business Registry (ROBINS).

5.6.4.5 Identified enablers

Because the eSignature Act is Japanese law and is more in line with a legal framework than a set of specific standards, it is not related to ETSI TS 119 612 [i.20] concerning trusted lists. However, it may be possible to imagine reference within the legal framework to trusted lists for interoperability.

Experts interviewed suggested that conducting studies in consideration of typical use cases, mutual understandings should be developed in various aspects. Further information is needed, however, cited was the expectation that JADAC will move towards inter-operability with the EU LoTL according to ETSI TS 119 612 [i.20].

Only the “registration certificate” (PDF) means to announce accredited CAs and the “registration certificate” is not suitable for digital processing. A coherent set of certificate policies like ETSI EN 319 411-1 [i.24] and EN 319 411-2 [i.25], according to some interviewed experts, should be established in Japan.

5.6.4.6 Reference Material

5.6.5 Asia PKI Consortium

5.6.5.1 Legal context

Present members of the Asia PKI Consortium, which was established in 2001 and covers trust services across many Asian countries, include members from 10 countries with an additional 10 countries undergoing the application process of membership. Current membership details can be found on the Consortium webpage, a link for which is included below.

Trust services in the applicable Asian countries are mostly regulation-driven and are based on the 2001 UNCITRAL Model Law on e-Signatures described above.

5.6.5.2 Supervision and auditing

Most of the countries appoint a national regulator to operate the root CA and appoint issuing CAs under the root or to accredit / empanel issuing CAs. WebTrust principles are accepted for assessment, though individual countries may also deploy their own customized assessment policies and procedures.

5.6.5.3 Best practice

Types of membership include principal members, enterprise members, NPO members and individual members. Meetings include a general assembly, a steering committee meeting and a special steering committee meeting. Several working groups offer activities in pursuit of strengthening the PKI ecosystem between members across the Asian continent. For example, the business application working group aims to address cross-domain and cross-region issues, promote exchange and collaboration and develop IT-enabled services. The legal and policy working group aims to influence interoperability initiatives, to collaborate with government and related industries and to produce policy papers and raise awareness about regulations among and between members. The technology and standards working group produces white papers and case studies, addressing topics such as the standardization of technological advancements, emergent technologies in public key cryptography and seeks to bring technological platforms together for the benefit of all members.

5.6.5.4 Trust representation

Presently no information about trust representation.

5.6.5.5 Reference Material

Note: A report by the Asia PKI consortium is in progress describing the approach taken by members of the Consortium members which will be taken into account in later versions of this report. This covers the following countries: India, China, Hong Kong, Korea, Taiwan, Thailand, Macau, Malaysia and Saudi Arabia.

5.7 North America

5.7.1 Canada [Planned]

5.7.1.1 Legal context

5.7.1.2 Supervision and auditing

5.7.1.3 Best practice

5.7.1.4 Trust representation

5.7.2 México

5.7.2.1 Legal context

Mexican Advanced Electronic Signature Law of 11th of January 2012 rules the usage of electronic signatures, with a special focus on advanced electronic signatures (also named "reliable electronic signature" based on digital certificates. The law also regulates certification authorities, electronic documents. Repositories are ruled by the General Rules to which the Certification Services Providers is required to be subject, as a required technological element in order to get the accreditation as a Certification Service Provider in the following services: digital certificates and digital time stamp issue; data conservation evidence service issued in accordance with NOM-15-SCFI-2016; and, document digitalization service in physical format in accordance with NOM-15-SCFI-2016. The General Rules also regulates Certification Authorities, Registration Authorities, HSM devices and certificate status services; i.e. Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP).

The Mexican Advanced Electronic Signature Law, and other regulations like the General Rules to which the Certification Services Providers is required to be subject or the Mexican Commerce Code also defines other trust services, as the digital time stamp issuance service. These regulations also detail some other services like data messages preservation and document digitalization in physical format, as to act as a Third Party Legally Authorised, but these services cannot be considered as trust services from an eIDAS Regulation point of view.

These providers are not called Trust Service Providers, as in the EU, but rather are known as Certification Service Providers (somehow in line with EU Directive 99/93/CE).

According to the Whereas of the General Rules to which the Certification Services Providers, the Mexican Federal Government seeks to strengthen policies, strategies and guidelines on the use of advanced electronic signature as a factor in electronic government and the simplification of the interaction between traders and government. In that sense, the Whereas establishes that to reach this goal, the Economy Department is required to issue General Rules on Certification Services so that the practices and policies that are applied guarantee the continuity of the service, the security of the information and its confidentiality through clear and defined procedures, as well as establish the standards in computer security related to electronic commerce and advanced electronic signature; and issuing accreditation of Certification Services Providers for the issuance of digital certificates and other additional services of advanced electronic signature.

According to Article 114 of the Mexican Commercial Code when, notwithstanding the provisions of the preceding paragraphs, if the parties agree among themselves the use of certain types of Electronic Signatures and Certificates, this agreement is required to be recognized as sufficient for the purposes of cross-border recognition, unless that agreement is not valid or effective according to the applicable law.

According to Article 114 of the Mexican Commercial Code any certificate issued outside the Mexican Republic will produce the same legal effects as a certificate issued in the Mexican Republic if that certificate presents a degree of reliability equivalent to those contemplated by the Mexican Republic. In the same way, this Article establishes that any Electronic Signature created or used outside the Mexican Republic will produce the same legal effects as an Electronic Signature created or used in the Mexican Republic if it presents an equivalent degree of reliability.

Finally, the Article 114 of the Mexican Commercial Code establishes that in order to determine whether a Certificate or an Electronic Signature presents an equivalent degree of reliability for the purposes of the preceding paragraph, the international standards recognized by Mexico and any other pertinent means of conviction is required to be taken into consideration.

Mexican legislation considers the following services:

- Provision of digital certificates for advanced digital signatures. This would be equivalent to the provision of eIDAS qualified certificates for qualified electronic signatures.
- Provision of digital time stamp issuance service.
- Provision of data messages preservation service.
- Provision of document digitalization in paper support.

For each service, there are specific rules to be fulfilled. There are also two specific rules that are generally applicable for all types of certification service providers:

- General Rules to which the Certification Services Providers.
- Mexican Commercial Code Regulation regarding Certification Services Providers

5.7.2.2 Supervision and auditing

To act as a Certification Services Provider offering the following services: Digital Certificates issuance, digital time stamps issuance, data Message conservation, document digitalization in physical format, as well as to act as a Legally Authorized Third Party, it is necessary to obtain an accreditation by the Mexican Economy Department (numeral 1, Title I of the General Rules to which the Certification Services Providers is required to be subject)

The accreditation process may be seen analogous to the eIDAS qualification process. According to article 5 of the Mexican Commercial Code Regulation regarding Certification Services Providers, and to article 102 of the Mexican Commercial Code, the accreditation process begins with the filling and presentation of an application by the service provider in a format determined by the Economy Department, which will be accompanied by specific documents regarding compliance the provision of certain resources (human, material, economical and technological), that will be checked by the Economy Department.

Also, the provider is required to attach to the application a declaration of each individual who intends to operate or have access to the systems that will be used in case of being accredited, in which that individual manifests, under protest of telling the truth and warned of the penalties incurred by those who falsely declare to an authority other than a judicial authority, that was not condemned for crime against the individuals patrimony and much less disqualified for the exercise of the profession, or to perform a position in the public service, in the financial system or to exercise trade activities.

The provider has to have a bond policy for the amount and conditions that are determined in the Regulations and in the General Rules issued by the Economy Department.

Finally, the provider has to include in the application a written agreement to be subject to be audited by the Economy Department at all times, so that it verifies compliance with the requirements to obtain and maintain accreditation as a Certification Services Provider. Once this is done, the provider has to register the certificate at the Economy Department.

According to article 7 of the Mexican Commercial Code Regulation regarding Certification Services Providers, in order to complete the accreditation process made by the Certification Service Provider, a resolution on the accreditation request is required to be provided following these steps:

1.- Consignment of certain information (name, nationality, profession, etc.) about the interested applicant (or a representative) to certain authorities to be evaluated by them;

2.- Review and preliminary assessment, within twenty days as of the request receipt, of the information and documentation received for possible corrections of errors (20 days after its notification at the registration window);

3.- Conduct a visit at the address indicated by the interested party within twenty-five working days following the date of the application presentation, in order to carry out an audit to verify the requirements to obtain accreditation as a Certification Services Provider, requirements determined by Mexican Commercial Code and its Regulation regarding Certification Services Provider;

4.- Resolve within forty-five working days following the submission of the application whether or not to grant accreditation as Certification Services Provider; resolution that will be notified to the interested party through a registration window. The Economy Department may not grant more than one accreditation to the same interested party; and,

5.- Publish in the Federation Official Journal the accreditations granted within thirty days following the resolution that determines its applicability.

According to article 22 of the Mexican Commercial Code Regulation regarding Certification Services Providers, the audits performed by the Economy Department to the Certification Services Providers is required to be carried out in accordance with the provisions of the Federal Administrative Procedure Law for verification visits, which is required to be carried out ex officio or at the request of the Certificate Holder, the signatory or a trust party.

According to eleventh chapter of the Third Title of the Federal Administrative Procedure Law the authorities may perform verification visits, which may have an ordinary or an extraordinary nature. The difference between one and another is that, while the ordinary will be carried out in working days and working hours, the second ones may be performed any time.

In order to be able to practice visits, the verifiers is required to be provided with a written order with an autograph signature issued by the competent authority, specifying the place or area to be verified, the purpose of the visit, the scope that it will have and the provisions legal grounds that support it.

The owners, managers or responsible of establishments subject to verification will be required to allow access and provide ease and reports to the verifiers for the development of their work.

At the beginning of the visit, the verifier is required to show a valid credential with photograph, issued by a competent authority accrediting the verifier to perform that function, and he/she will leave copy to the owner, responsible, manager of the establishment.

From every verification visit, a circumstantial record is required to be drawn up, in the presence of two witnesses proposed by the person with whom the proceeding was understood or by the person who practices it if the latter has refused to propose those witnesses.

Finally, a copy of any minutes is required to be left to the person with whom the procedure was understood, even if he/she refused to sign, which is required to not affect the validity of the procedure or document in question, provided that the verifier indicates such circumstance in its own minutes.

The Mexican acts and regulations do not determine the validity of the Certificate Services Provider accreditation, as we do not know the basis of the audit repetition.

5.7.2.3 Best practice

According to the Whereas of the General Rules to which the Certification Services Providers, the Mexican Federal Government, through the Economy Department, is required to establish the standards in computer security related to electronic commerce and advanced electronic signature, applying the principle of technical neutrality

In order to be accredited, and to maintain that accreditation, according to several numerals contained in the General Rules to which the Certification Services Providers is required to be subject, it is mandatory that the providers fulfil the following technical standards whatever the service they are providing (digital certificates and digital time stamp issue; data conservation evidence service issued in accordance with NOM-15-SCFI-2016; and, document digitalization service in physical format in accordance with NOM-15-SCFI-2016):

ETSI TS 102 042 [i.17] applicable to:

- Physical security (section 7.4.4 ETSI TS 102 042);
- Business Continuity Plan (section 7.4.8 ETSI TS 102 042);
- Certificate Policy;
- Key Administration Plan (section 7.2 ETSI TS 102 042);

5.7.2.4 Trust representation

According to article 3 of the Mexican Commercial Code Regulation regarding Certification Services Providers, the Economy Department will draw up a list of the accredited or suspended Certification Service Providers and of the individuals or corporations acting on their behalf in accordance with the provisions of article 104, section I of the Mexican Commercial Code. The relationship will also include the natural persons who are part of the personnel of the aforementioned subjects. The Economy Department is required to keep this relationship updated and available for all users.

5.7.2.5 Reference Material

5.7.3 US Federal PKI

5.7.3.1 Legal context

In contrast to the Trusted List framework of eIDAS, the US Federal PKI is a bridge CA framework. At the centre of this trust framework is the Federal Bridge CA (FBCA), which acts as a trust hub for disparate PKI domains. The Federal Policy Management Authority (FPKI Management Authority) is the organization that operates and maintains the FBCA on behalf of the US Government, US Federal PKI Policy Authority (FPKIPA) shows the trust framework of FPKI.

To be more precise, the FBCA is not an autonomous service as such, but rather consists of a framework of specific norms and standards to determine the reliability of TSPs, based on a standardized methodology for assessing compliance with these norms and standards, and a cross-certification platform allowing TSPs to cross-certify with the US Federal PKI Architecture at seven pre-defined assurance levels. The FBCA functions as a non-hierarchical hub allowing relying parties to create certificate trust paths from their PKI domains back to the PKI domain of the cross-certified TSPs, so that the levels of assurance honoured by disparate TSPs can be more easily reconciled. The FBCA itself operates under the FBCA CP, which specifies seven different levels of assurance.

5.7.3.2 Supervision and auditing

All TSPs have to demonstrate their compliance with the predefined assurance levels, by regular independent audits in accordance with the published procedure. When a TSP cross-certifies with the FPKI architecture, and is an affiliate in good standing, a relying party operating an online application that utilizes digital certificates for electronic identity authentication may choose to trust that PKI's digital certificates at the Level(s) of Assurance asserted by those certificates. The purpose of the FBCA is to ensure that no other trust requirements are needed for the relying party to make that determination. While designed specifically with the benefit to US federal government services, the cross-certification approach is not inherently restricted to any sector, application or domain. In fact, there are additional sectors using the same approach and requesting the same conditions (e.g. SAFE Bio-pharma, etc.).

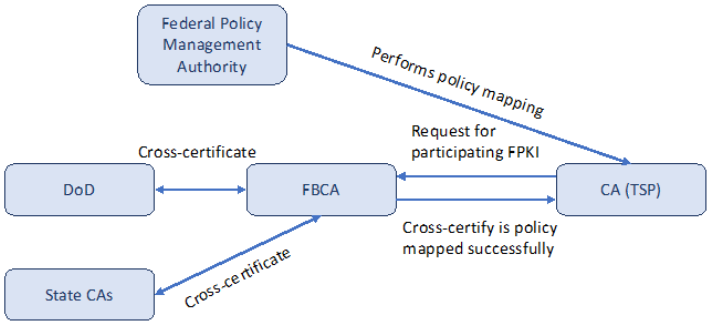


Figure 5: The trust framework of US Federal PKI

Cross-certification with FBCA can demonstrate that the TSP operation and its security level is equivalent to what the US government requires for their PKI system, which hence guarantees harmonization. However, one notable problem with the system, as it currently stands, is that it is not updated very often and sometimes includes TSPs that are still trusted, though without reason.

5.7.3.3 Best practice

At present, no information about best practice.

5.7.3.4 Trust representation

At present, no information about trust representation.

5.7.3.5 Reference Material

5.8 Other

5.8.1 Russia [In progress]

5.8.1.1 Legal context

5.8.1.2 Supervision and auditing

5.8.1.3 Best practice

5.8.1.4 Trust representation

5.8.1.5 Reference Material

5.8.2 Switzerland

5.8.2.1 Legal context

This PKI-based trust service scheme is for the community of providers established in Switzerland, and falls under the purview of the "Law on certification services in the area of the electronic signature and other applications of digital certificates" (hereafter the Law on the Electronic Signature).

5.8.2.2 Supervision and auditing

The basis for the auditing scheme is the Law on the Electronic Signature, including federal law on technical obstacles to trade and the corresponding implementing provisions. The auditor (also referred to as the "recognition body" in the Law on the Electronic Signature or as the "certification body" in ISOIEC 17021-1) is presently accredited by the Swiss Accreditation Service (Art. 1). Recognition bodies according to Art. 16 of the Law on the Electronic Signature are responsible for the audit. The recognition body is accredited by the Swiss Accreditation Service (Art. 1). The recognition body is comparable to the CAB according eIDAS. There is currently only one recognition body: KMPG.

The recognition body notifies the accreditation body of the providers they recognise. The accreditation body then adapts the list of recognized providers and makes it available to the public. In Switzerland there is no national supervisory body like in other EU countries.

The Federal Office of Justice (FOJ) and the Federal Office of Communications (OFCOM) are responsible for the regulation. They are not involved in the audit scheme. OFCOM is also responsible for overall coordination.
The basis for trust decisions rests on the Assessment Report of the recognition body.

The audit is based on the rules regarding the process defined in ISO/IEC 17021-1 and on the technical requirements defined in the technical and administrative regulations. This process is more or less equivalent to the process described in EN 319 403 under chapter 7.4.5 except that the full re-assessment takes place every three years with annual surveillances. In the future, in case EU Member States globally accept EN 319 403 as a reference point for the audit process, it could likewise be considered as a reference in order to harmonize Swiss rules with those of other EU states.

A PDF list of recognized Certification Service Providers is published on the Swiss Accreditation Service website. This is currently the only reliable public information useful to identifying the recognised certification provider.

5.8.2.3 Best practice

The recognised provider will implement a certificate policy that complies with the law, the decree and technical and administrative regulations concerning certification services in the area of electronic signatures and other applications of digital certificates. The technical and administrative regulations refer directly to EN 319 411-2 [i.24] and indirectly to EN 319 411-1 [i.25].

The regulations also refer to other ETSI and CEN standards such as ETSI EN 319 412-x (certificate profiles), ETSI EN 319 421 and EN 319 422 (time-stamping) and EN 419211-x (protection profiles).

Additionally, Switzerland plans to implement a machine-readable Trusted List according to TS 119 612 [i.20] in 2019.

5.8.2.4 Trust representation

At present, no information about trust representation.

5.8.2.5 Identified enablers

To ensure cross recognition, the conclusion of an agreement between the EU and Switzerland would be necessary, according to Art. 20 from the Law on Electronic on the Electronic Signature.

Users, providers and the administration are of course interested in an agreement between EU and Switzerland concerning the mutual recognition of electronic signatures and services. The conclusion of an agreement depends on the general programme of negotiations between Switzerland and the EU and the priorities set. The Directorate for European Affairs (DEA) is the centre of expertise for Switzerland's European policy.

5.8.2.5 Reference Material

6 Analysis of Enablers and Barriers to Mutual Recognition

6.1 Introduction

The following text summarises the main approaches taken by existing national and international PKI based trust services as described in clause 5, and then the respondents to the question, information gathered through desktop investigations. This is followed by consideration of the enablers and barriers that have been identified for each pillar.

Editor's Note: This information is based on an initial analysis of information collected so far. This may be subject to change having collected further information through the workshops.

6.2 Legal context

6.2.1 General Approaches

From a legal perspective, there exist different approaches to regulating trust services. These can be group in two general categories: Regulatory and agreement-based approaches.

Regulatory approaches are based in the existence of formal legislation regarding the provision of trust services, by private and/or public entities. This legislation frequently defines specific legal effects to one or more trust services, and to the electronic evidence supported by them, specifically when the trust service complies with certain rules. This approach has been generally adopted following UNCITRAL's Electronic Signature Model Law of 2001, in some cases extended to other trust services. Following the principle of functional equivalence, under Article 6 of UNCITRAL's Electronic Signature Model Law, when any law requires the signature of a persona, this requirement will be fulfilled using an electronic signature that is trustworthy and appropriate for the purposes for which an electronic data message was created or communicated. Article 6 (3) of the Model Law sets forth the criteria to consider an electronic signature as trustworthy – these criteria correspond to the EU legal concept of and "advanced electronic signature" –, and Article 7 of the Model Law allows for the establishment of a public or private body in charge of determining which electronic signatures comply with that criteria. This process is required to be compatible with recognised international norms or criteria.

Also, according to the technological non-discrimination principle, the Model Law mandates that all forms of electronic signature receive the same legal effect (Article 3), except in case of a valid and enforceable agreement by the parties using the electronic signature (Article 5).

While being a Model Law addressed to international electronic commerce, a majority of national laws following it have also regulated the legal effects of electronic signatures and other trust services in a horizontal way, including the usage of these technologies in electronic government procedures.

The EU regulatory approach has been used to foster the international recognition, in the European Economic Area, of electronic signatures (Directive EC/99/93) and, nowadays, also legal person electronic seals, time stamps, certified electronic delivery evidences and web authentication certificates (EU Regulation 910/2014). The approach has been similar to UNCITRAL's Model Law, but explicitly defining different legal concepts for each electronic evidence and corresponding trust service – qualified and non-qualified –, with the aim to define explicit legal effects to qualified ones, while mandating that the non-qualified ones may not be denied legal effects solely on the grounds they are in electronic form and do not comply with all the requirements to be qualified. Possibly the main regulatory difference between the EC/99/93 Directive and Regulation (EU) 910/2014 consists in the mandatory, previous and continued supervision of any provider offering qualified services, as a way to generate enough trust as to impose Member States the legal obligation of accept foreign qualified trust services in their territory, even when used in electronic government processes.

Regulation (EU) 910/2014 does not preclude the legal competence of Member States to define the legal effects of the non-qualified instruments and services, even limiting their usage in specific cases (i.e. to protect consumers, workers, or when strict form requirements apply), but respecting the autonomy of the will of contracting parties, following partially the UNCITRAL's approach.

Many national laws have formally adopted UNCITRAL's approach, allowing the usage of all forms of electronic signatures under the principle of autonomy of the will of contractual parties, but in many cases have fostered or imposed the adoption of specific electronic signature technologies, mainly based in digital signatures based in PKI certificates issued by licensed certification service providers complying with very specific technical standards imposed by a supervisory body. In many cases, national laws have been extended to cover other certification services (trust services), applying the same regulatory approach and are, thus, similar to current Regulation (EU) 910/2014.

Additionally, some national laws – including some EU Member States – have also created national PKI operated by public bodies, aiming to provide services to public authorities, employees, devices, etc.; or as a way of controlling the corresponding licensed service providers; or even to be able to permanently verify a digital signature based in a certificate.

Finally, some legislators have regulated the use of electronic signature or electronic seal certificate as an electronic identification means, allowing its usage in the context of electronic government processes, due to the legal value of the digital certificate to confirm its holder's identity. Apart from this possibility, several countries have ruled the issuance of certificates that are exclusively used for identification purposes, in some cases included inside a national ID document or electronic passport.

Contrary to regulation, agreement-based approaches are based on agreements between the parties representing the use and provision of trust services. Such approaches can be based on the negotiation power of one party, or can be based in the autonomy of the will of parties, normally organised through associations with different governance models.

In the first case, there's a party with a very strong power of negotiation that allow this party to impose its requirements (i.e. Adobe. Google…), based in non-negotiable agreements, to the rest of the parties.

In the second case, there are a number of parties, within a more equilibrated scenario, that set forth multilateral agreements to regulate trust services in a specific domain. In this second case, parties also create associations between one or more trust services, in users in a business domain (i.e. SAFE-BioPharma) or for a specific usage, such as Internet trust embedded in applications (i.e. CA/Browser Forum).

In both cases, agreement-based approaches tend to re-use international standards to foster interoperability and ease adoption, specially from a technological perspective. The agreement-based approach may also leverage on legal concepts such as advanced electronic signatures to give them fully legal effect in their domain, based in the corresponding agreements, but always considering any legal limitations on the autonomy of the will of the parties.

6.2.2 Enablers

The eIDAS aligned ETSI trust services standards provide a framework supporting both regulatory and agreement-based approaches, that could act as an enabler for global transactions.

A first enabler is the existence of legal concepts for non-qualified electronic evidence and corresponding trust service, as it eases their reuse as foundational basis for comparing different regulations or defining multilateral contractual frameworks. This enabler is especially relevant in the context of ETSI standards, which generally set forth best practices independently of the EU concept of qualification.

In example, the legal concept of an advanced electronic signature may act as a basis both for the recognition of cross-border transactions according to different regulatory framework or in a particular application of domain supported by agreements.

A second enabler is precisely the legal concept of qualification, because it is constructed around a set of specific requirements, thus allowing the legal comparison between institutions in different regulatory and agreement-based approaches and easing recognition. I.e. SAFE-BioPharma could consider that an EU qualified electronic signature complies with their requirements for advanced electronic signatures, or Argentina's supervisory body could consider that an EU qualified electronic signature is equivalent to a digital signature according to Argentinian law.

6.2.3 Barriers

From a legal perspective, some barriers need also be considered, as they may hinder cross-border recognition, especially in the case of regulatory approaches.

One barrier that should be considered is the different set of trust services regulated in the different legislation, as not all trust services or even electronic evidence institutions are not considered in all legal systems (i.e. legal persons seals).

A second legal barrier affecting cross-border recognition can be found in the legal conditions set forth for that recognition, and any inherent limitation contained in the applicable law. I. e. Article 14 of Regulation (EU) 910/2014 requires the signature of an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU, but that agreement requires that (1) a foreign trust service complies with all the requirements for the corresponding EU qualified trust service; and (2) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded (bilateral approach).

Apart from these constraints, in some cases recognition may be additionally limited by Member States, as in the case of electronic signatures and seals. According to Article 25 (3) of Regulation (UE) 910/2014, are member states are required recognised as a qualified electronic signature in all other Member States.

Due to the principles of international law, especially reciprocity principle, we can assume that any recognition will be constrained by the limitations of Regulation (UE) 910/2014.

These barriers do not necessarily affect the potential recognition of trust services in the agreement-based approaches.

6.3 Supervision / Audit

6.3.1 General Approaches

In most of the non-EU countries, the provisioning of trust services is subject to a supervision regime that includes an initial audit (pre-authorisation) and regular audits throughout the lifecycle of the provided trust services.

However, there is a certain diversity in terms of the requirements applicable to the auditors for them to be eligible to conduct those audits. If in all cases where auditing is required, approved auditors are mandated to

be independent from the assessed TSP/TS, the accreditation requirements may come from three different sources:

- A nationally defined scheme, as for the majority of 3rd countries (e.g. Brazil, India, Japan, Australia, South Korea, …);
- An accreditation scheme where national accreditation bodies, signatories of the International Accreditation Forum (IAF) & ILAC multilateral agreement (MLA), are accrediting CABs under a standardised framework. This framework is either ISO/IEC 17065 supplemented by ETSI EN 319 403, like in Europe as the EA promoted accreditation scheme for eIDAS accredited CABs, or ISO/IEC 17021 (e.g. Switzerland); or
- An ad hoc commercial scheme, namely the WebTrust for CA certification scheme, requiring the auditors to be WebTrust practitioners licensed by Chartered Professional Accountants (CPA) Canada

ISO/IEC 17065 supplemented by ETSI EN 319 403 framework

ISO/IEC is an accreditation framework already benefiting from the IAF/ILAC MLA and is widely available worldwide. ETSI has supplemented this framework for requirements on CABs assessing trust service providers and the trust service they provide. The European cooperation for Accreditation (EA) has promoted the ISO/IEC 17065 framework supplemented by EN 319 403 as the eIDAS accreditation framework dedicated to the assessment of QTSP/QTS against the eIDAS Regulation, used as the normative reference against which the QTSP/QTS conformance is assessed.

That same ISO/IEC 17065 framework supplemented by EN 319 403 is widely used for assessing conformance of TSP/TS with standard specifications, including ETSI standards establishing best practices specifications for a wide range of trust services, including issuance of digital certificates, provision of time-stamps, preservation of digital signatures, validation of digital signatures, provision of electronic delivery services.

WebTrust for CA accreditation and certification framework

WebTrust for CA is an internationally well-know and used audit scheme for TSPs issuing digital certificates as a trust service. WebTrust audits are conducted by independent accountant firms (practitioners) that are licensed by Chartered Professional Accountants (CPA) Canada.

As a rule-based assurance audit, the WebTrust scheme aims to review the implementation and operational effectiveness of controls over a period of time in the past (to make sure the systems have been adequately operating, with the assumption that they will continue to do so). This is a major difference with schemes that are reviewing the organisational and operational set-up making sure that not only past operations were conducted as expected but are in place to ensure that future operations will confidently be operated as expected.

The WebTrust scheme does not actually meet the requirements of eIDAS conformity assessment bodies in Article 3 (18) as falling out of the scope of Regulation (EU) 765/2008 where accreditation of CABs is performed by NABs. However, the confidence in the WebTrust licensed practitioner to conduct audits with the same rigour and qualifications as Regulation (EU) 765/2008 accredited CABs, under ISO/IEC 17065 supplemented by ETSI EN 319 403 in particular, is comparable.

The WebTrust scheme has the advantage to be self-contained and benefiting from a clearly identifiable set of licensed auditors. There is no centralised or formal list of ETSI accredited auditors and ETSI standards are sometimes difficult to embrace as they are relying on many external references without sometimes the formal assurance that all relevant criteria coming from external sources are included (e.g. no formal assurance that

CA/Browser requirements are included in relevant standards, no formal assessment that complying with ETSI standards ensure compliance with eIDAS requirements).

The WebTrust scheme is however limited to the assessment of TSP issuing digital certificates as a trust service and is not directly applicable to the assessment of other types of trust services.

6.3.2 Enablers

The accreditation framework based on ISO/IEC 17065 supplemented by ETSI EN 319 403 is a framework dedicated to the assessment of TSP/TS but agnostic of the actual set of criteria against which the audit will be conducted. When those criteria are standards such as ETSI standards, this makes it a very powerful tool to strengthen the confidence in the assessed TSP/TS to meet the requirements of the concerned standard.

As a general principle, all certifications issued by CAB having been accredited by signatories of the IAF MLA under a recognised framework (like ISO/IEC 17065 is) will benefit from international recognition under the "certified once recognised everywhere principle".

It is believed that the IAF MLA driven accreditation scheme based on ISO/IEC 17065 (potentially supplemented by ETSI EN 319 403) is a very natural and interesting candidate for any country to base their national TSP/TS certification scheme on. By nature, this framework allows assessing conformance to any set of criteria, be it standards (e.g. ETSI standards on TSP/TS), be it legal provision (e.g. eIDAS requirements on QTSP/QTS), be it Industry specifications (e.g. CA/Browser Forum requirements), etc.

The European cooperation for Accreditation (EA) has promoted the ISO/IEC 17065 framework supplemented by EN 319 403 as the eIDAS accreditation framework dedicated to the assessment of QTSP/QTS against the eIDAS Regulation. As those requirements are functional and technology neutral, and as no standard has been referenced by the eIDAS Regulation for giving conformant implementation with presumption of compliance with part or all eIDAS requirements, it de facto requires CAB willing to be eIDAS accredited to define their own eIDAS certification scheme for each type of QTSP/QTS defined by the eIDAS Regulation. Furthermore, very few of the conformity assessment scheme documents used in practice today are made publicly available by CABs. As a result, relying parties are hampered in their legitimate quest for trust and accountability, and cannot obtain a reasonable confirmation that QTSP/QTS meet the requirements of the eIDAS Regulation.

However, despite the peer review mechanism imposed at the level of NABs by Regulation (EC) 765/2008, there is no assurance on the quality of the currently accredited CAB certification schemes to effectively confirm that assessed QTSP/QTS meet the eIDAS requirements. There can be not only a difference in the formal approach, but also and more importantly a diversity in terms of quality in such assessments.

Nevertheless, it is not impossible nor unusual for such 3rd countries to expand and finalise such a scheme by the establishment of a harmonised, specific and complete certification scheme laying down, to a sufficient level of technical details, the exact set of controls and control objectives that the CAB will have to use to conduct a conformity assessment of QTSP/QTS against more generic legal provisions. This may be facilitated by the fact that national legislations may reference standards as binding normative documents (contrary to the eIDAS Regulation). However, the EA promoted scheme being incomplete and falling short of a harmonised eIDAS certification scheme is often pointed out by 3rd countries as jeopardizing the mutual recognition of EU QTSP/QTS.

6.3.3 Barriers

The lack of globally adopted accreditation scheme for CABs assessing PKI based trust services aimed is still a barrier to the general global cross recognition of trust services.

When the normative document against which accredited CABs have to assess TSP/TS for conformance are not standards or clearly identified technical specifications (e.g. laws or functional and technology neutral requirements), the lack of harmonised conformity assessment (certification) scheme not only creates friction in the internal market – with CABs in different Member States interpreting (e.g. eIDAS) requirements slightly differently – but also jeopardizes international interoperability.

There is a need for a harmonised set of certification schemes for ISO/IEC 17065, supplemented by ETSI EN 319 403, accredited CABs to assess QTSP/QTS against the eIDAS requirements.

There is a need for formally adopting the ISO/IEC 17065, supplemented by ETSI EN 319 403, accreditation framework at the European level and to further promote it at international level for the accreditation of CAB assessing TSP/TS.

6.4 Best practice

6.4.1 General Approaches

All known general-purpose PKI trust services are based on the ITU X.509 standard or the IETF equivalent RFC 5280.

The structure (table of content) of most PKI trust services are based on trust service policies and practices statements which follow RFC 3647.

Some PKI services are based on the earlier ETSI specifications TS 101 456 [i.15] and TS 102 042 [i.17]. These "historical" specifications which are used as the basis for the ETSI EN 319 411-1 [i.24] & -2 Policy Requirements, the latter being aimed to support based on the eIDAS Regulation (EU) 910/2014 [i.4] EN 319 411-1 [i.24] & 319 411-2 [i.25].

6.4.2 Enablers

The use of generally adopted standards, such as X.509 and the definition of a certificate policy RFC 3647 will facilitate comparison of the audit criteria used for assessing the acceptability of PKI systems.

If the technical approaches are based on the detailed technical standards as adopted in the EU such as EN 319 411-1 [i.24] & 319 411-2 [i.25], then technical comparison between PKI systems under different regimes should be straight forward. If non-EU PKIs are based on the earlier standards (TS 101 456 [i.15] or TS 102 042 [i.17]) then it may be necessary to upgrade the PKI to use the latest standard to assure equivalence or at least apply those aspects required by the eIDAS regulation. For Webserver authentication the CA/Browser baseline or extended validation guidelines provides a common set of policy requirements, with extended validation guidelines being necessary for the Qualified level. Where other standards provide generally acceptable practices, such as ISO 21188 [i.12] (or its potential derivative which is taking into account general information security practices to be ISO 27009) this may assist in comparison.

6.4.3 Barriers

If there is no other common basis comparison of the certificate or trust service policies used as the basis for PKI systems comparison to identify equivalence of acceptance criteria used to assess a PKI service can be a difficult and lengthy process.

The lack of globally adopted standards for PKI based trust services aimed at the particular needs of the trust services as identified in the eIDAS is still a barrier to the general global cross recognition of trust services.

6.5 Trust Representation

6.5.1 General Approaches

Four main models for representation of trust are widely used:

- The national root-signing by a national root CA with ability to cross-certify other CAs for mutual or unilateral recognition;
- Trust stores for listing the approved issuing CAs or root-CAs operated by an application or software platform provider
- The usage of trusted lists as specified in TS 119 612 [i.20] or sometimes in the older version of the specifications (ETSI TS 102 231 [i.19]).

- Cross certification between CAs or root-CA through a bridge CA which approves the cross certified CA as meeting basic policy criteria as set by the bridge policy authority

SafeBiopharma and Adobe have demonstrated that it is possible to map representations between an ETSI TS 119 612 [i.20] based trusted list representation of trust and a trust representation based on cross certificate with the bridge. Moreover, Adobe has demonstrated that consumption of trusted lists into a trust store at a large scale was possible and pretty efficient.

Trusted list-based model may facilitate independence from GAMMOA trust stores and root-signing models as demonstrated by Adobe recognition of EU trusted lists for verifying EU qualified electronic signatures.

6.5.2 Enablers

Trusted lists are a powerful tool for representing trust in approved trust service providers and the trust services they provide. If the technical identifiers for expressing the levels of reliability are shared between trust domains and those levels being similarly defined then then technical cross recognition should be straight forward. When those identifiers and levels are different then technical means for expressing a mapping between equivalent identifiers and levels may be required to be specified.

In particular, ETSI EN 319 412-5 [i.26] QcCompliance statement specifications should be updated to extend its scope to non-EU countries.

6.5.3 Barriers

Extended specifications for TL-to-TL mapping between different approval systems (using different identifiers and levels of reliability definitions) and expressing mutual recognition between selected levels may require further development of the EU Trusted List standards.

7 Initial Conclusions

Note: The following are initial thoughts towards the report's conclusions and do not necessarily represent the final results of this study.

a) In order to establish cross recognition between separate PKI based trust services comparison need to be made for each of the 4 pillars:

   1: legal context,

   2: supervision

   3: audit and policy requirement of the PKI based systems.

   4: trust representation

b) The adoption of common standards, such as those defined by ETSI, as the basis for the provision of trust services will assist significantly in cross recognition.

Annex A:
Study Questionnaire

ETSI Study on Globalisation of European Trust Services

Questionnaire on Globally Relevant PKI and Trust Services

V2.1

Introduction

ETSI has tasked a group of experts (reference STF 560) to study existing PKI-based trust services schemes that operate in different regions of the world, and their possible mutual recognition / global acceptance. In particular, the study aims to identify further steps which could be taken to facilitate cross recognition between EU trust services, based on ETSI standards supporting the eIDAS Regulation (EU) No 910/2014, and trust services from other schemes.

A key element of the study will be an exploratory mapping between:

- ETSI standards (ETSI standards may be downloaded from: https://www.etsi.org/standards-search entering the document number as above without spaces) related to EU trust services for:
    - Policy requirements, defined in ETSI EN 319 4xx series (e.g. EN 319 411-2) and EN 319 5xx series;
    - Assessment scheme, defined in ETSI EN 319 403;
    - and
- Corresponding information on other PKI-based trust services schemes.

This information will be collected through desktop research, the present questionnaire, interviews and other investigations, and put in perspective based on results from joint workshops to be held on the same topic at a number of locations around the world

Note: ETSI standards may be downloaded from: https://www.etsi.org/standards-search
entering the document number as above without spaces.

To assist us in carrying out this study we request that you provide some basic information about your PKI-based trust schemes with links to any further details that may be available. We request the questionnaire is responded to by all those who are concerned with running a PKI-based trust scheme operated outside the European Union and may be interested in achieving cross recognition with the EU. The scheme may operate across a country, or internationally to meet the requirements of a market sector. A PKI-based trust scheme may involve one or more service providers within a coherent set of certificate policies.

Information on PKI Scheme

Topic	Information
Name scheme generally known by:	
Person or persons assisting providing the information	Name(s): Organisation(s): Role(s): Contact email(s):
Geographical scope of PKI scheme	
Community / application	
Other information	

General Reference material

Ref number	Title	URL

Trust Management

Feature	Information
Represented as Trust List or Bridge CA certificate or other (please describe)	
Authority making trust decision	
Basis of trust decision	
Geographical scope of trust management scheme	
Community / application	
Other information	
Views on relationship to ETSI TS 119 612 trusted lists	

Trust Management: Reference material

Ref number	Title	URL

Audit

Feature	Information
Basis of Audit scheme	
Auditor accreditation requirements	
Criteria used for audit	
Views on equivalence to ETSI EN 319 403 based audit scheme	

Audit: Reference material

Ref number	Title	URL

Certificate Policy or equivalent

Name	Description	URL or other reference

Views on equivalence to certificate polices defined in ETSI EN 319 411-1 & ETSI EN 319 411-2

Comments

Other relevant information

Topic	Information

What are main impediments to cross recognition with EU trust services

Comments

What steps could be taken to improve cross recognition

Comments

Other comments

Comments

Annex B: Example of mutual recognition process flow

A general process for conducting a comparison between two trust models for TSP/TS in the view of a recognition agreement could be, at high level, described as follows:

(a) Establish the scope and objectives of the mutual recognition project:

a. The objective can be to achieve the mutual recognition of the equivalence of the levels of reliability of the TSP/TS irrespectively whether they are originating from one model or another;

b. The scope may range from the recognition of one specific type of trust service, up to the recognition of as many types as possible of trust services, including the recognition of the equivalence of the trust services outputs, such as digital signatures, time stamps, delivery service evidence, digital certificate, etc., originating from both models.

(b) Identify the approach to be used to conduct the mutual recognition process: The definition of this approach should take into account aspects like:

a. The level of preparation and of preliminary analysis or studies on the feasibility of a mutual recognition;

b. The nature of the commitment of the parties: this may range from a simple expression of interest to the establishment of a joint working group, formal or informal;

c. The readiness of the respective models;

d. The phasing of the process: It is likely that starting with a feasibility study, be it informal in a first step when engaging resources from both parties, would be an interesting approach in many cases.

e. The tentative calendar and deadline, be it ambitious, realistic, conservative, if and when it can be estimated.

(c) Execute the comparison:

a. For each of the comparison pillars identified and illustrated in Figure 1, the comparison process is executed in line with the four steps illustrated in Figure 2.

b. The complete comparison process may require for each of the pillar several iterations before coming to a conclusion.

c. The results and conclusions of those processes should be consolidated, in such a way to allow the drafting of the mutual recognition agreement (MRA) and its draft execution plan.

(d) MRA preparation and signing:

a. In case of positive conclusion on the, partial or complete, comparison process between QTSP/QTS from both models, the mutual recognition agreement should be drafted, finalised and signed.

b. The corresponding MRA execution plan should be drafted, finalised and signed.

(e) MRA execution: The MRA should be executed and its execution monitored according to the agreed plan.

(f) MRA maintenance/revision: From its execution and implementation monitoring, after an agreed period of time or as a result of changes in the respective compared models, or at the occasion of an incident or for any other applicable reason, the MRA may be reviewed.

(g) MRA termination: The consequence of the termination of the MRA should likely be anticipated at the conclusion of the MRA and subject to a termination plan. At the time of its termination, the plan should be updated and executed in accordance with the agreed provisions.

Each step of the above process can be confronted to issues in their realisation that can be addressed using the four steps method illustrated in Figure 2 above aiming to come to a solution, involving potentially several iterations before coming to a positive conclusion.

As a general remark, this process may be a lengthy process and tentative planning should take this into account.

Annex C:
The Model of eIDAS used as reference for Comparison

[Note: This annex has yet to be reviewed by the STF and is likely to be subject to change.]

C.1 Introduction

C.1.1 Overview

The eIDAS Regulation [i.5] (hereafter eIDAS) provides a regulatory environment for electronic identification of natural and legal persons and for a set of electronic trust services, namely electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication. It sets the principle of non-discrimination of the legal effects and admissibility of these trust services as evidence in legal proceedings.

Since 1 July 2016, most provisions of eIDAS are directly applicable in the 28 EU Member States' legal framework overcoming problems of fragmented national regimes. It provides legal certainty and fosters the usage of eID means and trust services for online access and online transactions at EU level.

To further enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the EU internal market and to promote the use of trust services and products, eIDAS introduces the notions of qualified trust service (QTS) and qualified trust service provider (QTSP) with a view to indicating requirements and obligations that ensure high-level security of whatever QTS or product is used or provided and, as a consequence, are granted a higher presumption of their legal effect.

C.1.2 General principles for mutual recognition

Article 14 "International aspects" of eIDAS rules the mutual recognition principles between trust services provided by trust service providers established in a third country and QTSs provided by QTSPs established in the Union.

As per Article 14(2).a of eIDAS, the mutual recognition of their legal equivalence is only applicable to third country TSP/TS that meet the eIDAS requirements applicable to EU QTSP/QTS, hence de facto limiting Art.14 mutual recognition to the various types of EU QTSP/QTS foreseen in eIDAS.

In order to be validly executed the recognition of the legal equivalence of 3rd country TSP/TS with EU QTSP/QTS is required to be recognised in an agreement concluded between the European Union and the 3rd country in question (or an international organisation) in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU).

As per Article 14(2).a of eIDAS, such agreements are required to ensure a reciprocity in the legal equivalence recognition, i.e. that the QTSs provided by QTSPs established in the Union are recognised as legally equivalent to trust services provided by TSPs in the third country or international organisation with which the agreement is concluded.

C.1.3 Mutual recognition of qualified electronic signatures

It should also be noted that, while the mutual international recognition foreseen in Article 14 of eIDAS is limited to the legal equivalence between QTSP/QTS and their 3rd country TSP/TS counterparts, the mutual international recognition between qualified electronic signatures (QESig) and their 3rd country electronic signatures is made possible by definition in eIDAS in combination with Art.14.

Indeed, QESig is defined in Article 3(12) of eIDAS as *an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures*. Provided a 3rd country electronic signature is meeting the advanced electronic signature requirements set out in Article 26 of eIDAS, is created by a QSCD and is based on an electronic signature certificate that is issued by a 3rd country TSP/TS recognised under an Article 14 agreement concluded with the EU for being legally equivalent to a qualified certificate (QC) for electronic signatures issued by an EU QTSP/QTS, this 3rd country electronic signature will be deemed legally equivalent to an EU QESig.

Requirements set out in Article 26 of eIDAS for advanced electronic signatures are functional requirements that are likely met by state-of-the-art PKI based digital signatures, in particular when meeting e.g. the standards referred to in CID (EU) 2015/1506 [i.6], and a fortiori when based on QC for electronic signature (or 3rd country equivalent).

The mechanisms, or the absence of mechanisms, for (mutual) recognition of 3rd country signature creation devices as (legally) equivalent to EU QSCD are presented in section A.2.4.

C.1.4 Mutual recognition of qualified electronic seals

The mutual recognition principle developed in the previous section is mutatis mutandis applicable for the mutual recognition of the legal equivalence of 3rd country electronic seals to EU qualified electronic seals (QESeals).

C.1.5 (Mutual) recognition of qualified signature/seal creation devices

The mechanisms for (mutual) recognition of 3rd country signature/seal creation devices as (legally) equivalent to EU qualified signature/seal creation devices (QSCDs) as they are specified in eIDAS are peculiar.

In order to be considered as an EU QSCD, an electronic signature creation device is required to:

- meet the requirements laid down in Annex II of eIDAS, and
- be certified by an appropriate public or private body designated by an EU Member State to confirm such a compliance with requirements laid down in Annex II of eIDAS.

EU Member States is required to notify to the European Commission (EC) the names and addresses of those designated certification bodies. The EC makes that information available, together with the list of QSCDs certified by those bodies on its website (https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds)

The certification of QSCD in the context of eIDAS considers two types of devices:

- For "Type 1" devices where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment, the certification is required to be based on a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list of the Annex of CID (EU) 2016/650 [i.7];
- For "Type 2" devices where a QTSP manages the electronic signature creation data or electronic seal creation data on behalf of a signatory or of a creator of a seal, the certification is required to be based on an alternative process:
  - that, pursuant to Article 30(3)(b) of [eIDAS], uses security levels comparable to those required for Type 1 devices, and
  - that is notified to the EC by a designated certification body.

Today CID (EU) 2016/650 [i.7] does not include a list of standards for the certification of Type 2 devices. The alternative processes currently in application for Type 2 devices (https://ec.europa.eu/futurium/en/content/list-alternative-processes-notified-commission-accordance-article-303b-and-392-eidas) may be used only in the absence of such standards referred to in CID (EU) 2016/650 [i.7] or when a security evaluation process referred to in CID (EU) 2016/650 [i.7] is ongoing.

This means that the only way for a 3rd country signature creation device to be recognised as (legally) equivalent to an EU QSCD is to be certified as an EU QSCD, i.e. the 3rd country signature creation device is certified under [eIDAS] as a Type 1 or Type 2 device using the appropriate method described here above. Such a certification is required to be done by a body designated by an EU Member State. However, nothing would prevent an EU Member State, in particular in absence of delegated acts concerning the establishment of specific criteria to be met by such designated bodies, to designate an appropriate body from a 3rd country certifying devices in accordance with CID (EU) 2016/650 [i.7].

C.2 Regulatory provisions for QTSP/QTS

C.2.1 Nine types of EU QTSP/QTS

In its Article 3(16), [eIDAS] defines a 'trust service' as an electronic service normally provided for remuneration which consists of:

a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

b) the creation, verification and validation of certificates for website authentication; or

c) the preservation of electronic signatures, seals or certificates related to those services.

Only those trust services listed in Article 3(16) of eIDAS for which there are applicable requirements in the Regulation can benefit from the qualified status. eIDAS regulates the following nine qualified trust services:

1) **The provision of qualified certificates for electronic signatures**
Certificates for electronic signature are electronic attestations which link electronic signature validation data to a natural person and confirm at least the name or the pseudonym of that person. Since 1 July 2016, an electronic signature can only be used by a natural person to sign, i.e. mainly to express consent on the signed data/document. Therefore, certificates for electronic signature cannot be issued to legal persons. Instead legal persons can use certificates for electronic seals (see below).
A qualified electronic certificate for electronic signatures is an essential element for a signatory to create qualified electronic signatures that is required to have the equivalent legal effect of a handwritten signature all over the EU.

2) **The provision of qualified certificates for electronic seals**
As explained above, since 1 July 2016, legal persons cannot create legally valid (qualified) electronic signatures anymore and cannot be issued (qualified) certificates for electronic signatures. Instead legal persons can use certificates for electronic seals, which are electronic attestations that link electronic seal validation data to a legal person and confirm the name of that person. The aim of an electronic seal is not to sign but to serve as an evidence that an electronic data/document was issued by a legal person, ensuring certainty of the data/document's origin and integrity.
A qualified electronic certificate for electronic seals is an essential element for a legal person to create qualified electronic seals that is required to enjoy, all over the EU, the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

3) **The provision of qualified certificates for website authentication**
Certificates for website authentication are issued to ensure the users (in particular citizens and SMEs) that behind the website there is a legal or natural person identifiable by trustworthy information.

4) **Qualified preservation service for qualified electronic signatures**
Such a qualified trust service aims to ensure the legal validity and trustworthiness of qualified electronic signatures over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

5) **Qualified preservation service for qualified electronic seals**
Such a qualified trust service aims to ensure the legal validity and trustworthiness of qualified electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.

6) **Qualified validation service for qualified electronic signatures**
Validation of electronic signature is an ancillary service to electronic signatures whose process aims to confirm the validity of an electronic signature.
Qualified validation services for qualified electronic signatures entail the verification by a qualified trust service provider that the requirements of eIDAS are met by a qualified electronic signature in order to confirm its validity.

7) **Qualified validation service for qualified electronic seals**
Validation of electronic seal is an ancillary service to electronic seals whose process aims to confirm the validity of an electronic seal.
Qualified validation services for qualified electronic seals entail the verification by a qualified trust service provider that the requirements of eIDAS are met by a qualified electronic seal in order to confirm its validity.

8) **Qualified electronic time stamps services**
Electronic time stamps are issued to ensure the correctness of the time linked to data/documents.
Qualified electronic time stamp is required to enjoy, all over the EU, the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

9) **Qualified electronic registered delivery services**
Relying on a qualified electronic registered delivery service will benefit, all over the EU, from the presumption of the integrity of the registered data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by that qualified trust service.

eIDAS sets requirements for all such qualified trust services to be considered trustworthy together with obligations for their qualified trust service providers with regard to the security of their operations, their liability and their supervision regime.

C.2.2 eIDAS regulatory requirements for EU QTSP/QTS

eIDAS foresees a set of requirements and obligations for QTSP/QTS in order to ensure high-level security of the qualified trust services. Those obligations include in a nutshell (with an indication of the relevant articles of eIDAS):

- General requirements for all types of QTSP/QTS: are given in eIDAS
  - (Art.5) relating to Processing and protection of personal data
  - (Art.13.2 & 13.3) relating to Liability and burden of the proof.
  - (Art.15) relating to Accessibility for person with disabilities.
  - (Art.19.1) relating to Implementing appropriate technical and organisational measures to manage the risks.
  - (Art.19.2) relating to Security and personal data breach notification:.
  - (Art.20.1) relating to Completion and internal procedures.
  - (Art.23) relating to Use of the EU trust mark for QTS.
  - (Art.24 points (a) to (j)) relating to Additional requirements on QTSP operations and practices:

- **Specific requirements** from the provisions laid down in eIDAS with regards to the provision of a specific type of qualified trust service, with the relevant articles of eIDAS as illustrated in Figure 3 below, for the nine types of QTSP/QTS.

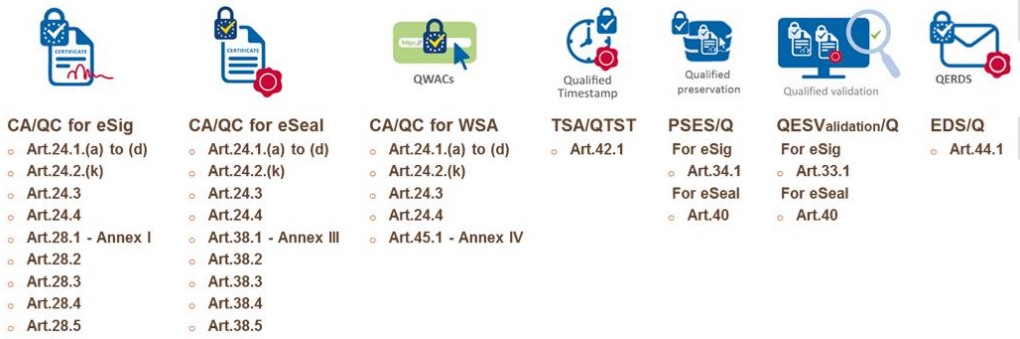


Figure 6: EU QTSP/QTS specific requirements as laid down in eIDAS [i.3]

C.3 Supervision & auditing of EU QTSP/QTS

C.3.1 Supervision of EU QTSP/QTS

In order to ensure high-level security of qualified trust services, eIDAS foresees an active supervision scheme of QTSP and the QTS they provide (hereafter referred to as a QTSP/QTS by the national competent supervisory body (SB) that supervises, ex ante and ex post, fulfilment of the QTSP/QTS requirements and obligations. All those requirements is required to be met by the QTSP/QTS before providing the very first qualified trust service output, e.g. before issuing the very first qualified time stamp in the case of QTSP providing qualified time stamping services.

Before a TSP/TS is granted a qualified status (QTSP/QTS), it will be subject to a pre-authorisation process – the so-called initiation process. QTSPs may only begin to provide the qualified trust service after the qualified status has been granted by the competent supervisory body and indicated in the national trusted list. From there, the supervision scheme covers the full life cycle of each QTS and each QTSP, from its genesis until its termination.

In practice, where TSPs without qualified status intend to start providing qualified trust services, they are required to submit to the supervisory body a notification of their intention together with a conformity assessment report issued by an "eIDAS accredited" conformity assessment body (CAB). Before notifying the competent supervisory body of their intention to start providing qualified trust services, the future QTSP/QTS is required to hence successfully pass an external assessment (audit) to confirm it fulfils the requirements from eIDAS. That audit is required to be conducted by a conformity assessment body specifically accredited to carry out assessments of QTSP/QTS against eIDAS. The audit results in a formal conformity statement confirming - if such is the case - that the QTSP/QTS meets all the applicable requirements of eIDAS. Based on the notified information including the report of such an audit, the competent SB will formally verify that the candidate QTSP/QTS meets the applicable eIDAS requirements and, in case of positive verification, it will undertake the publication of the grant of the qualified status for that QTSP/QTS in the national trusted list.

It is only when its qualified status is published in the corresponding national trusted list that the QTSP/QTS is authorised to provide the corresponding QTS.

Once granted a qualified status, QTSPs and their QTSs have the obligation to pass, and submit to the competent supervisory body a conformity assessment report (CAR) issued by an accredited CAB confirming at least every 24 months, that the QTSP and the QTSs it provides fulfil the requirements laid down in [eIDAS]. Competent supervisory bodies are also allowed, at their own discretion and at any time, to audit themselves any QTSP/QTS for which they are competent or to request an accredited CAB to perform an ad hoc audit.

QTSPs and their QTSs are supervised for their entire lifecycle, from their genesis to their termination. In particular, in order to ensure sustainability and durability of QTSs, as well as to ensure proper termination and user's confidence in their provision, QTSPs is required to maintain, at all times, an up-to-date termination plan. That plan is to be agreed by the SB upon initiation and regularly checked for compliance during the life of the QTSP/QTS.

C.3.2 Auditing of QTSP/QTS

Art.3.18 of eIDAS [i.3] requires CABs to be accredited in accordance with Regulation (EC) No 765/2008 [i.9] in a way that such accreditation ensures the accredited CABs are competent to carry out conformity assessment of a QTSP/QTS against the requirements of eIDAS.

The European cooperation for Accreditation (EA), is the body recognised under Regulation (EC) No 765/2008 that manages a peer evaluation system among NABs from the EU Member States and other European countries. That rigorous and transparent peer evaluation system ensures the equivalence of the accreditation services delivered by NABs and thus the equivalence of the level of competence of CABs. This mandatory peer evaluation system facilitates the mutual recognition and promotes the overall acceptance of accreditation certificates and conformity assessment results issued by accredited bodies. National authorities are required to recognise the equivalence of the services delivered by those accreditation bodies (i.e. the NABs) which have successfully undergone such peer evaluation, and thereby accept the accreditation certificates of those bodies and the attestations issued by the CABs accredited by them. All European NABs are signatories of the IAF MLA.

The EA is also the recognised body, under Regulation (EC) No 765/2008, as competent to develop sectoral or specific accreditation schemes. This may be done on request of the Commission but in the context of eIDAS this has not been the case. eIDAS does not specify any specific accreditation scheme or any conformity assessment (or certification scheme) against which the CAB is required to be accredited but requires the resulting conformity assessment scheme to be eIDAS specific, i.e. such that CAR confirms that the QTSP/QTS meet the requirements of eIDAS.

Nevertheless, the EA has promoted the ETSI EN 319 403 [i.10] standard on requirements for CABs to carry out conformity assessment of TSPs as one route to demonstrate conformity with relevant requirements of eIDAS through assessment by accredited CABs. The EN 319 403 defined accreditation scheme is such that:

(i) It requires the accreditation of the CAB to be based on ISO/IEC 17065 [i.11];

(ii) It supplements the general requirements provided in ISO/IEC 17065 to provide additional dedicated requirements for CABs performing certification of TSP/TS towards defined criteria against which they claim conformance.

It does not, however, specify those criteria nor the certification scheme and needs to be considered as an accreditation "framework" for the conformity assessment of TSP against audit criteria. Those criteria need to be defined in such a way that they should:

(a) take into account specificities of the type of trust service to be assessed;

(b) ensure that all aspects of the TSP activity are fully covered; and

(c) be based on standards, publicly available specifications and/or regulatory requirements.

Consequently the EA promoted accreditation scheme (ISO/IEC 17065 completed by ETSI EN 319 403) cannot be implemented unless such effective criteria, the related control objectives and controls are clearly defined in a way that the NAB can evaluate the competency of the CAB to conduct an assessment of a QTSP/QTS against them in order to assess its conformity with the eIDAS requirements and so that the accreditation cannot be contested. Their definition will be the purpose of the conformity assessment scheme that may be defined by the CAB itself, the EU MS supervisory body, or any other body possessing the necessary technical competence.

It is a paramount importance to clearly understand that such conformity assessment is required to be conducted against the requirements of eIDAS and not against a specific standard. Furthermore, no standard may be imposed to a QTSP/QTS as a condition for them to be recognised as qualified. Of course, standards may be of great help in order for QTSP to establish their practices and design their QTS in order to achieve best practices and to maximise interoperability. They also may significantly help CAB to design their certification scheme for conducting assessment of QTSP/QTS against the requirements of eIDAS.

Today, there are actually as many different eIDAS certification schemes as there are eIDAS accredited CABs (https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation). This results in the fact that there are chances that divergences may exist between these schemes. The fact that these schemes currently used by eIDAS accredited CABs are not easily available, when available at all, does not make it easy for relying parties to be convinced that they do fulfil a minimum set of requirements outside the eIDAS context. The absence of implementing act referencing standards allowing for presumption of compliance with a set of requirements of eIDAS, the problems due to the possible divergent interpretations of relevant standards aimed to support eIDAS implementation further contribute to the divergence issue.

It would plead for the definition of a European wide eIDAS conformity assessment scheme (or actually one for each one of the 9 types of qualified trust services defined by the eIDAS Regulation) against which the CAB could be accredited and the QTSP/QTS assessed to confirm they meet the eIDAS Regulation requirements.

C.4 Technical standards & best practices for EU QTSP/QTS

As already stressed above, no standard may be imposed to a QTSP/QTS as a condition for them to be recognised as qualified. Of course, standards may be of great help in order for QTSP to establish their practices and design their QTS in order to achieve best practices and to maximise interoperability. They also may significantly help CAB to design their certification scheme for conducting assessment of QTSP/QTS against the requirements of eIDAS.

C.5 Trust representation of EU QTSP/QTS

C.5.1 EU trust mark for QTS

For marketing purposes, once qualified, a QTSP/QTS may use the EU Trust Mark for QTS when promoting its QTS in compliance with the provisions laid down in eIDAS and its related secondary legislation (Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (Text with EEA relevance). OJ L 128, 23.5.2015, p. 13–15). That trust mark shown in Figure 7 can only be used by a QTSP to “label” its QTS.

Figure 7: EU trust mark for qualified trust services

C.5.2 EU national trusted lists

Trusted lists are signed XML files, as specified by ETSI TS 119 612 [i.20], which enable in practice any interested party to determine whether a trust service is or was operating in compliance with relevant requirements, currently or at a given time in the past (e.g. at the time the service was provided, or at the time at which a transaction reliant on that service took place). In order to fulfil this requirement, trusted lists need to contain information from which it can be established whether the TSP's service is, or was, known by the Trusted List Scheme Operator (TLSO) and if so the

status of the service at a given time. Trusted lists therefore contain not only the service's current status, but also the history of its statuses.

EU MS have the obligation to include in their national trusted list the information related to the grant of a qualified status to a TSP/TS and to maintain over time the information on any change of that status. This information is required to be kept and maintained forever from the date of the grant of a qualified status. Trusted lists

On a voluntary basis EU MS can include, on the basis of a national scheme in accordance with national laws, approval information about non-qualified trust services and the non-qualified TSP they provide them.

In order to validate that a trust service is a qualified one under Regulation (EU) No 910/2014 [i.5], a relying party would need to check the qualified status of the given trust service and that it is provided by a qualified trust service provider. Provided a trust service is included in the trusted list, it provides the relying party with the necessary information about the given trust service, its status and status history and potentially additional relevant information helping the relying party to validate the trust service or its outputs (e.g. certificate, signature or seal, time-stamp).

In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission publishes a central list with links to the locations where the national trusted lists are published as notified by Member States. This central list, called the List Of Trusted Lists (LOTL), is available in both a human readable format and in a format suitable for automated (machine) processing XML.

LOTL also plays an important role in authenticating EU MS trusted lists. Each national trusted list is electronically signed/or sealed by its MS scheme operator and the certificate to be used to verify such a signature/seal is included in the LOTL after notification to the European Commission. The authenticity and integrity of the machine processable version of the LOTL is ensured through a qualified electronic signature or seal supported by a qualified certificate which can be authenticated and directly trusted through one of the digests published in the Official Journal of the European Union.

ETSI TS 119 612 [i.20] provides specifications for trusted lists in two contexts, namely the European Union legislative context as set by Regulation (EU) No 910/2014 [i.5] and the context of countries outside the European Union and the EEA countries, or of international organizations willing to issue trusted lists in accordance with the present document.

The benefits from the adoption of the present document by non-EU countries or international organizations are twofold:

- This can be used to enable in practice any interested party to determine whether a trust service from a non-EU country or an international organization is or was operating under an approval scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place.

- This can facilitate the declaration of mutual recognition between trust services and their outputs (e.g. between EU and other nations/organizations outside the EU, within or between groups of nations/organizations outside the EU).

Would there be an agreement concluded between the EU and a 3rd country with regards to the mutual recognition of trust services, the specifications for the LOTL, based on ETSI TS 119 612 [i.20], allows for pointing to the trusted list of that 3rd country or to a trusted list representation of the trust representation in use in that 3rd country with respect the recognised equivalent TSP/TS.

Annex:
Change History

Date	Version	Information about changes
August 2019	V0.0.4	Draft for public availability

History

Document history		
<Version>	<Date>	<Milestone>