ETSI TR 103 684 V1.1.1 (2020-01)

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

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 Report (TR) 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

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 present document 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: legal context, supervision and audit, technical standards, and trust representation. This methodology is used to analyse 37 PKI standard, global, sector and national PKI schemes.

In addition, workshops covering 4 regions of the world were held in Dubai, Tokyo, Mexico City and New York to discuss the local approaches to PKI based trust services and how these may be related to the EU trust services established under eIDAS.

The study concludes with 18 recommendations to facilitate acceptance between EU trust services and other non-EU based trust services.

There is strong interest with achieving mutual recognition of trust services with the EU in all the regions of the world visited. However, there remain significant issues to be overcome, as outlined in the conclusions, before this can become a reality.

Introduction

Since the year 2000, ETSI has developed and enhanced a number of standards for trust. This began with policy requirements standards supporting the Electronic Signatures Directive [i.64], ETSI TS 101 456 [i.38], with a variation of this policy not specifically aimed at this Directive with associated profiles of the X.509 certificate format based on Recommendation ITU-T X.509 [i.65]. From 2014, with the publication of the eIDAS Regulation (EU) No. 910/2014 [i.4] on electronic identification and trust services, ETSI published a whole new series of standards aimed at supporting the eIDAS regulation. This new set of standards were not only updated to meet the new requirements of the eIDAS regulation and replace the existing ETSI standards supporting electronic signatures, but also served to extend the standards to support the new types of trust services adopted under eIDAS. These include electronic seals, aimed at identifying organizations (legal persons rather than individual natural persons), website authentication and registered electronic delivery where authenticated identity is supported through proofs provided by the information delivery service rather than certificates provided by a Public Key Infrastructure (PKI).

Around the world, a number of countries have since followed the lead of Europe and have adopted use of electronic signatures primarily based on the Electronic Signatures Directive and the earlier ETSI standards, in some cases moving towards equivalence with eIDAS. Furthermore, globally used commercial applications for viewing signed documents and securing transport level communications to websites have adopted the more recent eIDAS-based ETSI standards for assuring the security of these trust services.

The eIDAS Regulation and the earlier Electronic Signature Directive use the term "qualified" to apply to trust service providers which support the most stringent requirements of the Regulation. Article 14 of eIDAS Regulation (EU) No. 910/2014 [i.4] provides for trust service providers established in non-EU countries to be recognized as legally equivalent to EU qualified trust service providers. However, whilst some trust services may be considered as an operating and equally trustworthy service outside the EU, there is currently no agreement between the EU and other countries - or international organizations - that allows for trust services to be considered as legally equivalent.

This lack of international agreement regarding equivalence to EU qualified trust services and trust service providers, even though they may be based on the same ETSI standards, is one substantial barrier to achieving trust in support of global electronic commerce. The present document presents the results of a study into the barriers and enablers for mutual recognition of EU and non-EU trust service providers in support of global security of electronic systems.

1 Scope

The present document presents the results of a study examining existing trust services and trust service providers 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 present document first 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: legal context, supervision and audit, best practice and trust representation. Then the information collected concerning major PKI-based trust service schemes around the world and how they relate to the European trust service scheme based on eIDAS and ETSI standards is presented. The approaches to PKI across the globe are analysed to identify enablers and barriers to mutual recognition. Finally, conclusions are presented on steps that could be taken to facilitate mutual recognition.

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".

NOTE: Available at 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.8] EU Regulation 765/2008 for Accreditation and Market Surveillance (RAMS).

[i.9] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with European Economic Area relevance).

[i.10] IETF RFC 2527: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.11] IETF RFC 3126: "Electronic Signature Formats for long term electronic signatures".

[i.12] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol".

[i.13] IETF RFC 3628: "Policy Requirements for Time-Stamping Authorities (TSAs)".

[i.14] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.15] IETF RFC 5019: "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments".

[i.16] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.17] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.18] IETF RFC 5652: "Cryptographic Message Syntax".

[i.19] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.20] IETF RFC 6962: "Certificate Transparency".

[i.21] 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.22] ISO/IEC 17021-1:2015: "Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements".

[i.23] ISO/IEC 17065: "Conformity assessment -- Requirements for bodies certifying products, processes and services".

[i.24] ISO/IEC 27001: "Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements".

[i.25] ISO/IEC 27002: "Information Technology Security Techniques Code Of Practice For Information Security Controls".

[i.26] ISO/IEC CD 27099: "Information Technology -- Security techniques -- Public key infrastructure -- Practices and policy framework".

[i.27] ISO/IEC 27701: "Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines".

[i.28] ISO 21188: "Public key infrastructure for financial services -- Practices and policy framework".

[i.29] NIST FIPS 140-2: "Security Requirements for Cryptographic Modules".

[i.30] NIST SP 800-63-3: "Digital Identity Guidelines".

[i.31] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

[i.32] CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates.

[i.33] CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".

[i.34] CEN EN 419 211 Parts 1 to 6: "Protection profiles for secure signature creation device".

[i.35] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements".

[i.36] CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing - Part 1: Protection profile for QSCD for Server Signing".

[i.37] CEN EN 319 221-5: "Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services".

[i.38] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[i.39] ETSI TS 101 861: "Electronic Signatures and Infrastructures (ESI); Time stamping profile".

[i.40] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.41] ETSI TS 102 023: "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities".

[i.42] ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".

[i.43] ETSI TR 102 206: "Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework".

[i.44] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information".

[i.45] ETSI TS 102 778-1: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

[i.46] ETSI TS 102 778-4: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile".

[i.47] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.48] ETSI TR 102 272: "Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies".

[i.49] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

[i.50] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

[i.51] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

[i.52] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

[i.53] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.54] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.55] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.56] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.57] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.58] 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.59] 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.60] ETSI EN 319 412 (all parts): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles".

[i.61] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.62] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.63] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.64] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.65] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.66] ETSI TR 102 458 (V1.1.1) (2006-04): "Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456)".

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.55] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.55] and the following apply:

AAECA	Arab-African e-Certification Authorities Network
AATL	Adobe® Approved Trust List
ACS	Botswana Accreditation Certification Service Standards
AICPA	American Institute of Certificate Public Accountants
AICTO	Arab Information and Communication Technologies Organization
AVSP	Added Value Service Providers
BOCRA	Botswana Communications Regulatory Authority
CA	Certification Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CFR	Code of Federal Regulations
CICA	Canadian Institute of Chartered Accountants
CID	Commission Implementing Decision
CP	Certificate Policy
CPA	Certificated Public Accountant
CPS	Certification Practice Statement CCA Indian Controller of Certifying Authorities
CRL	Certificate Revocation List
CSP	Certification Service Provider

NOTE: Equivalent to TSP under Directive 1999/93/EC [i.64].

CWA	CEN Workshop Agreement
DIO	Japan Designated Investigative Organization
EA	European Cooperation for Accreditation
ECC	Elliptic Curve Cryptography
ECU	Electronic Certification Unit of Uruguay
eIDAS	Regulation (EU) 910/2014 [i.4] on electronic identities and trust services (for authentication and signatures)
ENISA	European Union Agency for Agency for Network and Information Security
ETO	Hong Kong Electronic Transactions Ordinance
FBCA	US Federal Bridge Certification Authority
FDA	US Food and Drug Administration
FIPS	US Federal Information Processing Standards
FPKI	US Federal PKI
GCIO	Hong Kong Government Chief Information Officer
HSM	Hardware Security Module
IAF	International Accreditation Forum
ICT	Information and Communication Technologies
IdM	Identity Management
IETF	Internet Engineering Task Force
ILAC	International Laboratory Accreditation Cooperation
IMRT	The International Mutual Recognition Technical Working Group
IOFE	Peruvian Official Infrastructure of Electronic Signature
IT	Information Technology
ITA	Information Technology Authority of Oman
JADAC	Japan Data Communications Association
JCAN	Japanese Certification Authority Network
JIPDEC	Japanese Institute for the Promotion of Digital Economy and Community
LOTL	List Of Trusted Lists
LTV	Long-Term Validation as applied by PAdES and other related signature formats
MLA	Multilateral Agreement
MLEC	UNCITRAL Model Law on Electronic Commerce [i.2]
MLES	UNCITRAL Model Law on Electronic Signatures [i.3]
MRA	Mutual Recognition Agreement
NAB	National Accreditation Body
NIST SP	Special Publication of the US National Institute of Standards and Technology

OCSP Online Certificate Status Protocol

NOTE: As defined in IETF RFC 6960 [i.19] or earlier equivalents.

PIN Personal Identification Number
PIV Personal Identity Verification (US federal identity credential)
PKI Public Key Infrastructure

NOTE: The generic term for a trust service infrastructure based on use of public key certificates.

PM Provisional Measures
PMA Policy Management Authority
QSCD Qualified Signature Creation Device as defined in eIDAS, or equivalent, Regulation [i.4]
QTS Qualified Trust Service
QTSP Qualified Trust Service Provider
QTSP/QTS Qualified Trust Service Provider and the Qualified Trust Service it provides
RA Registration Authority
RSA Cryptographic algorithm developed by Rivest, Shamir and Adleman
SB Supervisory Body
SCB Japanese Specified Certification Business
SD Supreme Decree
SIM Subscriber Identification Module of mobile phone
SSL Secure Socket Layer
TC ETSI Technical Committee
TLS Transport Layer Security
TLS/SSL Transport Layer Security/Secure Socket Layer protocol

NOTE: As specified in IETF RFC 5246 [i.16] or earlier equivalent Secure Socket Layer protocol.

TRA United Arab Emirates Telecommunications Regulatory Authority
TS Trust Service
TSA Time-stamping Authority
TSL Trust Status List
TSP Trust Service Provider
UAE United Arab Emirates
UNCITRAL United Nations Commission on International Trade Law
URL Uniform Resource Locator
US United States of America
XML eXtensible Markup Language

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 recognized 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 globalization of those services and by there, the globalization of electronic transactions supported by them.

NOTE: In order to avoid confusion, the present document refers to levels of reliability when addressing trust services, to make a clear distinction with the term "levels of assurance" that is used only when referring to electronic identification schemes (or systems). The notion of levels of assurance is not 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. Whilst the levels of assurance of electronic identification means/schemes and levels of reliability of a trust service may be related these are defined independently in the eIDAS regulation [i.4]. 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).

4.2 Areas of comparison between trust service schemes

The present clause 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 that 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.

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 and the trust services it provides 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 and the trust services it provides.

d. The approval and oversight systems applicable to auditing bodies for them to be eligible to conduct audits on the TSP and the trust services it provides.

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 a TSP and the trust services it provides. 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 institutionalized 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, 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 and the trust services it provides) 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 the best practices for PKIs operating in different legal contexts needs to confirm:

1) the ability of the practices to meet the requirements for a trust service to be mutually recognized as specified in both legal contexts;

2) that the practices achieve an equivalent level of security;

3) 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 standardized table of contents for the declaration of trust service practices or policies like IETF RFC 3647 [i.14] 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 and the trust services it provides, 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.53]), 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 and from the agreed trust representation when exchanged.

4.3 Comparison process

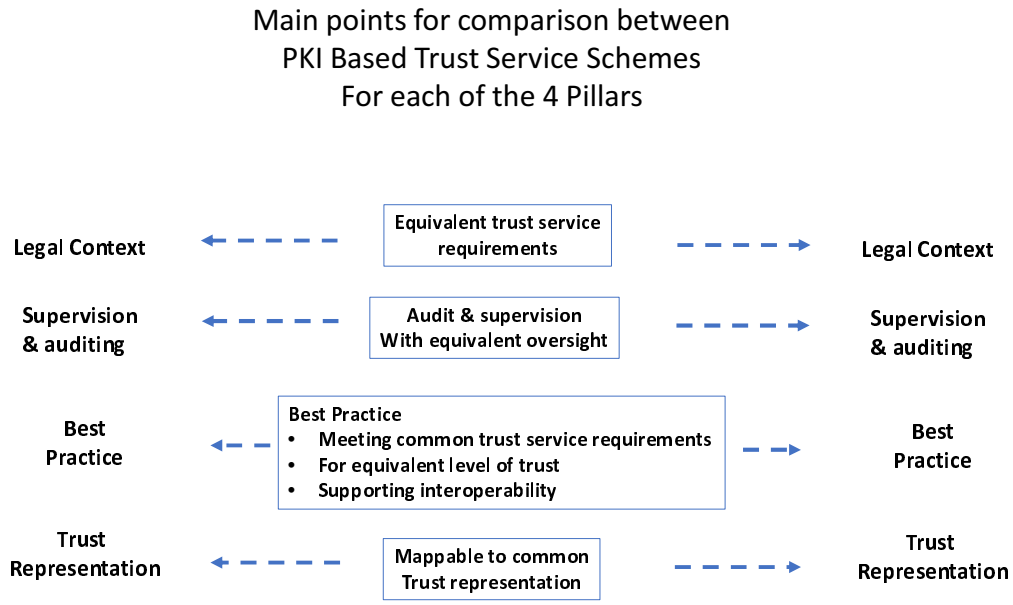

Figure 1: Main points for comparison between PKI-Based Trust Service Schemes for each of the 4 Pillars

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 potentially 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 and 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.

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 unsolvable 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's similar model or between any PKI-based (qualified) trust service provided by an EU QTSP and any third country TSP. However, Annex B 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 and the trust services it provides 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 and the trust services it provides 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 and the trust services it provides from a trust model would satisfactorily meet the requirements for a TSP and the trust services it provides 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 and the trust services it provides 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 the present document aimed to:

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

b) For each scheme, present the information collected along the four comparison areas described in clause 4.2.

c) Give a short analysis identifying, for each areas of comparison, how the specific non-EU PKI-based trust service scheme is described and compared against a scheme based on eIDAS regulation and related ETSI standards (see clause 5).

d) Identify the general issues that could act as a barrier or enabler to mutual recognition in considering the different schemes identified in clauses 5 and 6.

e) Identify, when applicable, potential solution at the technical and standardization level that can facilitate the resolution of identified issues to mutual recognition (see clause 7).

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 the present document aims to provide correct and up-to-date information, it is based on an understanding of information provided coming from a variety of sources and its correctness is not guaranteed. Reference should be made to the sources cited for more accurate information.

This survey includes information of specific products from major software suppliers that could have significant impact on the global adoption of EU standards for trust services. This does not mean that there is any endorsement of these specific products but is included as an indication of the global impact of EU trust service standards on the global market.

5.2 International Legal Framework & Standards

5.2.1 UNCITRAL

5.2.1.1 Introduction

The present clause summarizes the notes [i.1] 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. 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 harmonizing 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, 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 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)	https://uncitral.un.org/en/working_groups/4/electronic_commerce
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
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

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

5.2.2.1 Legal context

ISO 21188 [i.28] 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, has specific recognition under EU legislation.

5.2.2.2 Supervision and auditing

No requirements specified, but see WebTrust.

5.2.2.3 Best practice

Many of the provisions in ISO 21188 [i.28] are equivalent to requirements in ETSI EN 319 411-1 [i.58] 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.38].

5.2.2.4 Trust representation

No requirements specified.

5.2.2.5 Reference material

Title	URL
ISO 21188 [i.28]	https://www.iso.org/standard/63134.html

5.2.3 ISO/IEC 27099 PKI -- Practices and policy framework

5.2.3.1 Legal context

ISO/IEC CD 27099 [i.26] is committee draft of an international standard currently under development for PKI practices and policy framework. Though it is not presently published, it is expected to be ratified in 2020 or 2021. It is based on ISO 21188 [i.28] 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.28] and being an International Standard, has specific recognition under EU legislation.

5.2.3.2 Supervision and auditing

No requirements specified.

5.2.3.3 Best practice

Many of the provisions in ISO/IEC CD 27099 [i.26] are equivalent to requirements in ETSI EN 319 411-1 [i.58] and they both make use of general requirements for information security management in ISO/IEC 27002 [i.25].

5.2.3.4 Trust representation

No requirements specified.

5.2.3.5 Reference material

Title	URL
ISO/IEC CD 27099 [i.26]	https://www.iso.org/standard/56590.html

5.2.4 WebTrust for CAs

5.2.4.1 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 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, CPA Canada 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 CPA Canada 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.

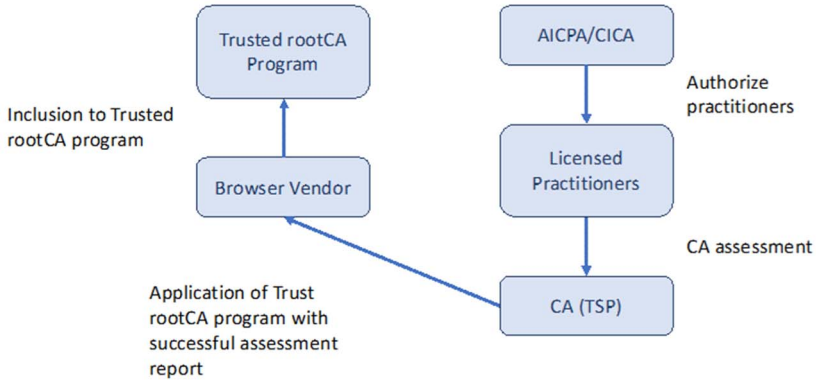

Figure 2: The trust framework of WebTrust for root CA program

5.2.4.2 Supervision and auditing

WebTrust operate its own qualification scheme for acceptance of certification authorities.

Because the requirements for non-European/North American TSPs do not currently extend to the eIDAS/EU qualified level, the functional philosophy behind WebTrust is the provision of assurance that TSP's services have, until the point of time the assessment is conducted, verifiably met a rigorous set of defined criteria. The operating assumption 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 EN 319 403 [i.54], which 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.28] and all other offerings are based on controls that have been specified by the CA/Browser Forum Baseline Requirements [i.31].

WebTrust currently offers a product for each service, as stated above, that is informed or based on ISO 21188 [i.28] and by CA/Browser Forum Baseline Requirements [i.31].

5.2.4.3 Best practice

WebTrust publishes its own criteria for Certification Authorities. This is based on ISO 21188 [i.28].

5.2.4.4 Trust representation

Used as the basis for root stores included 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. CPA Canada 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 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.

5.2.4.5 Reference material

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

5.2.5 CA/Browser Forum

5.2.5.1 Legal context

The CA/Browser Forum defines a set of standards for PKIs primarily aimed at website authentication the most significant being its baseline requirements [i.31] and extended validation guidelines [i.32]. It operates as an agreement between certification authorities (called certificate issuers) and providers of applications such as web browsers, which rely on certificates (called certificate consumers). The agreement is not binding on application providers (such as Google®, Apple®, Microsoft® and Mozilla®) who apply the CA/Browser Forum standards as they wish.

The CA/Forum standards are primarily aimed at webserver authentication, though they also support secure email and code signing.

5.2.5.2 Supervision and auditing

The CA/Browser Forum standards require either an audit based on WebTrust (see previous clause) or ETSI standards (ETSI EN 319 403 [i.54] and ETSI EN 319 411-1 [i.58]).

The providers of the applications relying on certificates audited against the CA/Browser Forum standards act as the equivalent to supervisory authority for CAs. Based on the results of an audit the application providers and applying their own acceptance criteria establishing their own list of CAs (i.e. trust service providers) considered as meeting their acceptance criteria in a "Root Store". Application providers can accept or reject CAs at their own discretion.

5.2.5.3 Best practice

The CA/Browser Forum has two main documents defining requirements for:

a) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [i.31].

b) Guidelines for the Issuance and Management of Extended Validation Certificates [i.32].

The ETSI standards are consistent with both the CA/Browser standards. The extended validation guidelines [i.32] are consistent with the ETSI standards for qualified certificates for website authentication.

5.2.5.4 Trust representation

The application providers represent trusted CAs in a root store.

5.2.5.5 Identified enablers

There is close alignment between the ETSI standards and the CA/Browser Forum best practices.

5.2.5.6 Identified barriers

The application providers using CA/Browser Forum standards do not recognize qualified certificates as meeting the requirements per se. A CA issuing certificates which are qualified needs to meet both the requirements of qualified certificates under the eIDAS regulation as well as the requirements as specified in the CA/Browser forum documents.

5.2.5.7 Reference material

Title	URL
CA / Browser Forum website	https://cabforum.org/
Baseline Requirements	https://cabforum.org/baseline-requirements-documents/
Extended Validation Guidelines	https://cabforum.org/extended-validation/

5.2.6 IMRT-WG

5.2.6.1 Legal context

The International Mutual Recognition Technical Working Group (IMRT-WG) is an information group of experts representing interests in Japan, North America and Europe to achieving global interoperability. The group is chaired by Japan. The group aims to identify a methodology for achieving mutual recognition and set up case studies for some specific use cases requiring mutual recognition.

It has been proposed that the IMRT-WG methodology for achieving mutual recognition is based on the four areas identified in the present document.

The group brings together PKI schemes based on a range of agreements and regulatory environments but all have keen interest in establishing mutual recognition with Europe.

5.2.6.2 Supervision and auditing

This is an area which is to be most exercised by the case studies with differing approaches to supervision and audit between the parties.

5.2.6.3 Best Practices

Some work has already been done with some of the parties with comparison with ETSI standards.

5.2.6.4 Trust Representation

The use cases are expected to involve both bridge certificate and trusted list forms of trust representation and mapping between the two is likely to be necessary.

5.2.7 Kantara Initiative®

5.2.7.1 Legal context

Kantara Initiative® is a commercial consortium.

5.2.7.2 Supervision and auditing

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

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

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

5.2.7.3 Best practice

The Kantara Initiative Identity Assurance Framework complies with the United States Federal Identity, Credential, and Access Management program and is based on the requirements of NIST SP 800-63-3 Digital Identity Guidelines [i.30] (Base and Volumes a, b and c).

5.2.7.4 Trust representation

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

5.2.7.5 Identified enablers

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

5.2.7.6 Reference material

Title	URL
Kantara Initiative Trust Framework Operations program	https://kantarainitiative.org/trustoperations/
Trust status list	https://kantarainitiative.org/trust-registry/trust-status-list/
NIST SP 800-63-3 Digital Identity Guidelines	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

5.3 Global Sector/Platform-specific PKI

5.3.1 Adobe® Approved Trust List

5.3.1.1 Legal context

The Adobe® Approved Trust List is a proprietary list of trusted root certificates, allowing Adobe's global user-base to create digital signatures that can be trusted whenever signed documents are opened with Adobe's Acrobat and Acrobat Reader® software. Electronic signatures that are viewed in these applications and have been created with a high-assurance, trustworthy certificate on this list is trusted by Acrobat® and Acrobat Reader®. Such trusted electronic signatures can support signatures created by both natural and legal persons, or applications or devices, such as electronic signatures or electronic seals defined in the eIDAS Regulation.

5.3.1.2 Supervision and auditing

The basis of trust decisions is a self-assessment of compliance to the technical requirements, supported by audits and certificate policy and certification practice statement documentation. The following audit schemes are recognized:

1) ETSI EN 319 411-1 [i.58] normalized certificate policy;
2) ETSI EN 319 411-2 [i.59] qualified certificate policy for natural or legal persons;
3) WebTrust v.2.0 or later; and
4) ISO 21188:2006 [i.28].

Conformity assessment bodies that are to carry out assessments against the accepted standards above are independent from the member's organization and are formally accredited or recognized for the applicable scheme. In particular:

1) the auditor conducting ETSI audits is be accredited against ISO/IEC 17065 [i.23] and ETSI EN 319 403 [i.54] for audits against ETSI EN 319 411 standards series [i.58] and [i.59];
2) the auditor conducting WebTrust audits is a WebTrust licensed Practitioner for WebTrust audits; and
3) the auditor conducting ISO 21188 audits is accredited against ISO/IEC 17065 [i.23] for ISO 21188 audits.

The member makes any applicable audit report available to Adobe® no later than three months after the end of the audit period. In the event of a delay greater than three months, the member provides an explanatory letter signed by the qualified auditor.

5.3.1.3 Best practice

The AATL implements a similar concept to ETSI TS 119 612 [i.53] regarding trusted lists but uses a proprietary XML format attached to a signed PDF file.

Accreditation against ETSI EN 319 403 [i.54] for audits against ETSI EN 319 411 standards [i.58] and [i.59] is required.

ETSI EN 319 411-1 [i.58] Normalized Certificate Policy and ETSI EN 319 411-2 [i.59] qualified Certificate Policies for Natural or Legal persons are considered compatible with AATL Technical Requirements. Other levels as Lightweight Certificate Policy may not be enough to meet compliance.

5.3.1.4 Trust representation

The Adobe AATL represents trusted CAs in the form of a list managed by Adobe. PKI Certificates recognized by the Adobe AATL used for electronic signatures are shown as "trustworthy" by all installed pdf-Reader programs, estimated 500 Mio installations. Additionally the Adobe Software is able to import the European Trust Service Status Lists, so that qualified trust services for electronic signatures and seal are recognized as trustworthy too.

5.3.1.5 Identified enablers

One particular enabler identified by Adobe is improved support for clearer and more objective requirements for non-qualified trust services. Additionally, beneficial would be further support of more granular type of service identifiers e.g. remote electronic signature services, code-signing and privileged execution.

5.3.1.6 Reference material

Title	URL
AATL Technical Requirements v.2.0	https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf
Adobe Global Guide to Electronic Signature Law	https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/document-cloud-global-guide-electronic-signature-law-ue.pdf

5.3.2 CertiPath®

5.3.2.1 Legal context

CertiPath® Public Key Infrastructure (PKI) Bridge enables cross-organizational trust for its members, who operate high assurance identity credentialing systems known as Enterprise PKI, and several of whom are providers of Personal Identity Verification - Interoperable credentials to other organizations. This bridged trust is characterized by a hub-spoke peer-to-peer environment where all of the members retain control over their individual trust domain policies and technical solutions, but agree to a common set of overarching requirements embodied in Federated Trust. Each member establishes parity with the Federated Trust's requirements, which in turn enables the trust between them.

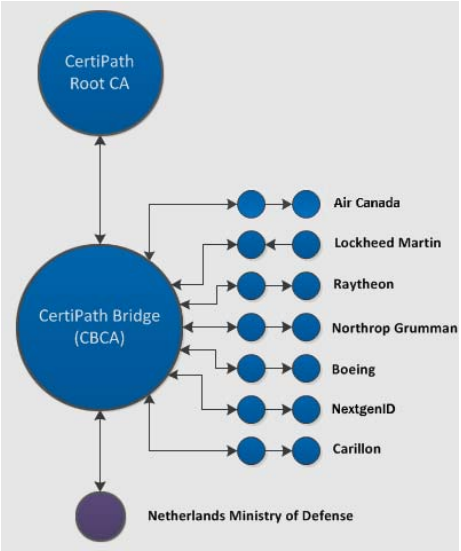

Figure 3: Illustration of CertiPath current trust network

CertiPath extends the same trust fabric that US Department of Defense and Federal Agencies rely on to Commercial Entities. CertiPath provides Best Practices, classified by Certipath as medium software, medium hardware, high hardware and IceCAP levels of assurance through Federated Trust.

5.3.2.2 Supervision and auditing

The CertiPath High Assurance Trust Environment is governed by the CertiPath Policy Management Authority (PMA), a member-driven committee chaired by CertiPath. Each CertiPath Bridge member organization has voting membership on the CertiPath PMA. All prospective members undergo review by the PMA and a vote before being admitted to membership in the trust framework. In this manner, the CertiPath trust community maintains its high level of integrity and the current membership is directly involved in the decision-making.

CertiPath reviews the certification practice statements of CAs to be cross-certified with the bridge for compliance with CertiPath certificate policies. Also, third party auditor attestation is required for the adherence of the applicant's PKI operations to its certificate policy and certification practice statement. The full requirements are specified in Certipath's PKI Criteria and Methodologies.

5.3.2.3 Best practice

The requirements of practices of the cross-certified CA are specified in the CertiPath X.509 Certificate Policy. This policy is consistent with IETF RFC 3647 [i.14].

5.3.2.4 Trust representation

Trust is represented by a bridge certificate issued by CertiPath's bridge CA.

5.3.2.5 Reference material

Title	URL
CertiPath federated trust	https://www.certipath.com/FederatedTrust.html
CertiPath Policy Management Authority	https://www.certipath.com/FederatedTrust_PolicyManagementAuthority.html
CertiPath PKI Criteria and Methodologies	https://www.certipath.com/downloads/CertiPath_Criteria_and_Methodologies_v1.2.pdf

5.3.3 SAFE-BioPharma®

5.3.3.1 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 Food and Drug Administration requirements, Drug Enforcement Administration requirements, European Medicines Agency requirements, Health Insurance Portability and Accountability Act of 1996 requirements.

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.

5.3.3.2 Supervision and auditing

In order to become cross-certified with SAFE-BioPharma Bridge CA, 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 [i.54]. The audit will be repeated on annual basis.

5.3.3.3 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: ETSI EN 319 401 [i.57], ETSI EN 319 411-1 [i.58], ETSI EN 319 411-2 [i.59].

5.3.3.4 Trust representation

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

5.3.3.5 Identified enablers

A study has been carried out into comparing the SAFE-BioPharma bridge certificate policy requirements with those in ETSI EN 319 411-1 [i.58] and it has been found that these are comparable. Also, it has been found possible to map the Bridge certificates to the EU trusted list.

The operation of the SAFE-BioPharma policy management authority has some similarities with the oversight provided by the EU supervisory bodies although it does not operate in the same regulatory environment, and is not totally independent of the CAs being overseen.

5.3.3.6 Identified Barriers

The main barrier to cross recognition is that this scheme operates through agreement. It does not operate in the same regulation-based environment as the EU.

5.3.3.7 Reference material

Title	URL
SAFE-BioPharma	http://safe-biopharma.org/index.html
FDA 21 CFR (Code of Federal Regulations) Part 11 - Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application	https://www.fda.gov/media/75414/download
Trusted lists	http://safe-biopharma.org/SAFE_Trust_Lists.html

5.3.4 Google Chrome®

5.3.4.1 Legal context

Google Chrome® attempts to use the root certificate store of the underlying operating system to determine whether a website certificate is indeed trustworthy, with a few exceptions. Google® reserves the right to distrust root certificates present in the operating system's root certificate list. Underlying operating system root programs recognized by Google are: Microsoft®, Apple®, Linux® using Mozilla® root program and Android®.

Google currently maintains its own hard-coded list in the binary of which root certificates are "EV-Qualified". It is assumed that this refers to CAs that follow the CA/Browser Forum EV guidelines [i.32]. It requires all EV certificates to use Certificate Transparency. However, recent reports indicate that Google will not indicate that a site is protected by EV certificates.

Moreover, Google has aimed to avoid use of organizational identifiers, as adopted in ETSI standards, as part of the primary name of the subject of a certificate difficult by requiring that an alternative name form also be included in CA/B Forum guidelines.

5.3.4.2 Supervision and audit

Generally, decisions are made by the supplier of the underlying operating system as described above.

5.3.4.3 Best practice

Google is an active participant in the definition of best practices developed in the CA/Browser Forum.

5.3.4.4 Trust representation

Trust is generally based on use of the underlying operating system root store.

5.3.4.5 Identified barriers

Google's approach to use of EV certificates and proposals to integrate features of the EU approach into the CA/Browser Forum guidelines may be seen as a barrier to the general adoption of EU certificates in Google Chrome.

5.3.4.6 Reference material

Title	URL
Google Chrome root certificate policy	https://www.chromium.org/Home/chromium-security/root-ca-policy
Certificate Transparency	https://goo.gl/chrome/ct-policy#chromium-certificate-transparency-policy.
Report on Google support for EV certificates	https://www.theregister.co.uk/2019/08/12/google_chrome_extended_validation_certificates/

5.3.5 Apple®

5.3.5.1 Legal context

The use of certificates is defined in Apple®'s root certificate program.

5.3.5.2 Supervision and audit

CA providers are required to complete a WebTrust audit or equivalent. Apple acts as the final decider on certificates included in its root program.

5.3.5.3 Best practice

CAs are required to follow the CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates or the Guidelines For The Issuance And Management Of Extended Validation Certificates.

5.3.5.4 Trust representation

Trust is represented by a root store managed by Apple on its operating system platforms.

5.3.5.5 Reference material

Title	URL
Apple root certificate program	https://www.apple.com/certificateauthority/ca_program.html

5.3.6 Microsoft®

5.3.6.1 Legal context

The use of certificates on Microsoft® platforms is controlled under its root program.

Microsoft program supports certificates for: website authentication, code signing, TLS/SSL client certificates, document signing (electronic signature) and secure email.

5.3.6.2 Supervision and audit

Microsoft accepts audits under WebTrust, ETSI EN 319 403 [i.54] or government approval.

Microsoft acts as the final decider on certificates included in its root program.

5.3.6.3 Best practice

Microsoft requires that CAs follow WebTrust or ETSI standards following the CA/Browser Forum documents.

5.3.6.4 Trust representation

Trust is represented by a root store managed by Microsoft on its operating system platforms.

5.3.6.5 Reference material

Title	URL
Microsoft root certificate program	https://aka.ms/RootCert

5.3.7 Mozilla®

5.3.7.1 Legal context

When distributing binary and source code versions of Firefox™, Thunderbird® and other Mozilla®-related software products, Mozilla® includes with such software a set of X.509v3 root certificates for various CAs. The included certificates have their "trust bits" set for various purposes, so that the software in question can use the CA certificates to anchor a chain of trust for certificates used by TLS/SSL servers and S/MIME email users without having to ask users for further permission or information.

The use of certificates on Mozilla platforms is controlled under its root program.

5.3.7.2 Supervision and audit

As specified in CA/Browser Forum documents, which require audits based on WebTrust or ETSI standards.

5.3.7.3 Best practice

CA/Browser Forum baseline or extended validation requirements.

5.3.7.4 Trust representation

Trust is represented by a root store managed by Mozilla on its platforms.

5.4 South America

5.4.1 Argentina

5.4.1.1 Legal context

Among some other aspects, Argentinian Law nº 25.506 on digital signatures (11/12/2001) regulates digital certificates, including the validity period and requirements and foreign certificates recognition, the licenced certifiers, the licence requirements and licenced certifiers activity cessation, the digital certificate title holder rights and obligations, the Application Authority, the Argentinian audit system, including subjects to be audited, and accreditation requirements for third parties that may carry out an audit process.

Argentinian Decree 182/2019 (11/03/2019) that regulates the Law nº 25.506 regulates the Digital Signature Infrastructure, including its composition, the root Certification Authority, the audit system types and report, digital certificates (validity, in case of issuance by non-licenced certifiers, and revocation), licence obtaining (requirements, effects, duration, licence expiry reasons), foreign certificates recognition and unique certification policy requirements. It also covers aspects related to Registration Authorities and TSPs, including the definition of Argentinian trust services.

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, the digitalisation of documents, the electronic notification of the Electronic Document Management System.

Law nº 25.506 distinguishes between electronic and digital signatures. According to article 3, 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 or licenced certifiers when those providers are accredited.

According to article 22 of Decree 182/2019, the Modernization Government Secretariat, depending on the Central Office of Cabinet of Ministers, will act as the Application Authority and, among its functions, it is responsible for the authorization of the operation of certification entities in Argentina and also supervises and audits these certification entities.

According to article 16 of the Decree 182/2019, the Modernization Government Secretariat is authorized to elaborate on 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 compliance with the conditions established by Law n° 25.506 is verified.

Article 36 of the Argentinian Decree 182/2019 defines the provision of the following trust services: digital documents digitally signed preservation services, 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, storage of intention statements made in electronic format, 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 accreditation, a certifier is required to comply with the following steps: Application submission, application admissibility, documentation analysis; conformity audit, ability report, granting the license; issuance of the certifier digital certificate and operations start of the licensed certifier.

According to article 14 of Decree 182/2019, the accreditation validity is for five 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.

5.4.1.3 Best practice

According to article 23 of the Decree 182/2019, the Administrative Modernization Secretariat, depending on the Modernization Government Secretariat, depending on Central Office of Cabinet of Ministers, will act as the Application Authority. 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 2019) set up the following ETSI standards that are applicable to:

- ETSI TS 102 023 [i.41] related with the policy requirements for time-stamping authorities; and
- ETSI TS 101 861 [i.39] 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 the Internet or on a public access network data transmission/dissemination that substitutes the 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 the 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	https://www.argentina.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 164 regulates the legal and evidentiary validity of the digital document, the electronic data message and the digital signature; the certification authorities (called "certification entities"), the legal status of digital certificates issued by foreign certification authorities, the attributions of the Bolivian accreditation entity, the entity that will provide the public sector certification service and for general Bolivian population and the Value-Added Services accreditation requirements.

The Bolivian Administrative Regulatory Resolution RAR ATT-DJ-RA-TL LP 32/2015 (9 January 2015) (from now on: Resolution RAR 32) regulates the approval of technical standards and other guidelines established for certification entities, digital certificate types, usage and formats, the Certification Entities and Registration Agency authorization requirements, digital certificate and certificate revocation list format (CRL and OCSP), minimum contents of Certification Entities terms and conditions, Certificate Policy minimum contents for an accredited Certification Entity, Certificate Policy Statement minimum contents for a Certification Entity, minimum contents of an accredited Certification Entity disaster recovery plans and procedures; minimum contents of an accredited Certification Entity security and risk assessment plans and procedures; minimum contents of the procedures and the conditions that is required to be complied by Certification Entities for the preservation of physical and digitized documents and the security levels.

The Bolivian Supreme Decree nº1793 (from here on: SD 1793) regulates digital certificates and digital signatures, the National Digital Certification Infrastructure framework, 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 and other related aspects such as TSA terms and conditions minimum contents or the TSA digital certificate format.

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.

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 SD 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; provision of digital signature validation service; provision of time-stamping service; provision of registration service for natural and legal persons, including digital certificate approval or revocation request. Finally, this legislation establishes the provision of other related certification services.

5.4.2.2 Supervision and auditing

Accreditation

According to the Certification Entities authorization process, included in the Regulatory Administrative Resolution ATT-DJ-RA-TL LP (from now on referred to as RAR) 31/2015, to obtain the accreditation to operate the interested Certification Entity is required to submit the authorization application to the Telecommunications and Transport Regulation and Control Authority.

The documentation received is reviewed by the ICT Unit Central Office. This entity verifies the compliance of economic and technical requirements both for public and private certification entities. If the assessed entity is authorized, the Telecommunications and Transport Regulation and Control Authority Legal Department is required to verify the compliance with legal requirements established in the applicable regulations.

Article 7 of the Regulatory Administrative Resolution RAR 32/2015 establishes that the Telecommunications and Transport Regulation and Control Authority is required to grant a five-year 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-year validity accreditation may be renewed for the same period (five years) to natural or legal persons requesting it prior to 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 responsibility 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.

According to section 4.5 of the Certification Entities authorization process, included in the Resolution RAR 31, the audit review process is carried out based on what is indicated in SD 1793 and in the technical standard ISO 21188 [i.28].

5.4.2.3 Best practice

Article 1 of Resolution RAR 32/2015 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 876/2016 approves time-stamp technical standards and, among them, the following ETSI standards applicable to an Authorized Certification Entity that want to provide time-stamping services:

- ETSI TS 102 023 [i.41] related with the policy requirements for time-stamping authorities; and
- ETSI TS 101 861 [i.39] related with the time-stamping profile.

5.4.2.4 Trust representation

There is presently no trust list or any other trust representation for Bolivian Trust/Certification Service Providers.

5.4.2.5 Reference material

Title	URL
Bolivian Law nº 164 on telecommunications and information and communication technologies	https://www.wipo.int/edocs/lexdocs/laws/es/bo/bo052es.pdf
General Regulation on Law nº 164	https://cites.org/sites/default/files/common/docs/informes_ACTO/Bolivia/ANEXO_A2_DECRETO%20SUPREMO_BO-RE-DSN_1391.pdf
General Regulation on Law nº164	https://cites.org/sites/default/files/common/docs/informes_ACTO/Bolivia/ANEXO_A2_DECRETO%20SUPREMO_BO-RE-DSN_1391.pdf
Supreme Decree nº 1793	https://www.lexivox.org/norms/BO-DS-N1793.html
Regulatory Administrative Resolution ATT-DJ-RA-TL LP 31/2015	https://ecrb.att.gob.bo/images/PDF/Normativa/ATT-DJ-RA%20TL%200031.PDF
Regulatory Administrative Resolution ATT-DJ-RA-TL LP 32/2015	https://att.gob.bo/sites/default/files/archivospdf/ATT-DJ-RAR%20TL%20LP%20202%202019.pdf
Regulatory Administrative Resolution ATT-DJ-RA-TL LP 876/2016	https://ecrb.att.gob.bo/images/PDF/Normativa/ATT-DJ-RAR-TL-LP-8732016.PDF
Regulatory Administrative Resolution ATT-DJ-RA-TL LP 272/2017	https://ecrb.att.gob.bo/images/PDF/Normativa/RARAR2017.PDF

5.4.3 Brazil

5.4.3.1 Legal context

Brazilian Provisional Measure nº 2.200-2 (27/07/2001) which establishes a Brazilian Public Key Infrastructure (ICP-Brazil), transforms the National Institute of Information Technology into autarky and gives other measures (from now on: PM 2200) to regulate ICP-Brazil Management Committee competencies, Certification Authorities competencies and Registration Authorities competencies.

"Accreditation criteria and procedures for ICP-Brazil entities v5.4" establishes the criteria and procedures to be followed for the accreditation, maintenance of accreditation and disaccreditation of Certification Authorities (CAs), Registration Authorities, Time Stamp Authorities, Support Service Providers, Biometric Service Providers and Digital Signature Service Providers within the scope of the ICP-Brazil.

This document also defines Support Service Providers and classifies them in three categories according to the type of activities provided.

Finally, the accreditation criteria and procedures document establishes that Trust Service Providers related to digital signature and cryptographic key storage services are 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 and 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 its level except in cases of cross-certification agreements previously approved by the ICP-Brazil Management Committee.

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. These services are classified in two categories: mandatory and optional trust services.

5.4.3.2 Supervision and auditing

Authorization/accreditation process

"Accreditation criteria and procedures for ICP-Brazil entities v5.4" (Ref. DOC-ICP-03) establishes the accreditation criteria and procedures for all the accreditation applicants, for Certification Authority applicants, Registration Authorities applicants, Time-stamp Authority applicants, Support Service Provider applicants, Biometric Service Provider applicants and Trust service Providers related to digital signature and cryptographic keys storage services.

Accreditation Procedures

The accreditation application to become an ICP-Brazil Certification Authority is required to be submitted to the root Certification Authority together with some specific documents such as the specialized human resources availability among others.

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-Brazil Management Committee related to the activity of Certification Authority, and that is in place to be audited within fifteen days from that moment.

The total or partial deferral, or the rejection of the accreditation is required to be substantiated and communicated to the applicant Certification Authority.

Auditing

Article 4 of PM 2200 establishes that one of the ICP-Brazil 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-Brazil entities" (ref: DOC-ICP-08) document classifies audits in two groups: pre-operational audits and operational audit (performed on an annual basis).

5.4.3.3 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.

Section 1.1.5 of the "ICP-Brazil 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.39] related with the time-stamping profile.

Section 6.5.6 of the "Minimum operational procedures for ICP-Brazil 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.44] - on the Provision of harmonized Trust-service status information.

Section 6.6.5 of the document referenced above (ref: DOC-ICP-17.01) establishes that in ICP-Brazil, the format and structure to be used to create signature policies have been prepared based on ETSI TR 102 272 [i.48] and ETSI TR 102 038 [i.42] standards, stamp technical standards and, among them, the following ETSI standards applicable to an Authorized Certification Entity that want to provide time-stamping services:

- ETSI TS 102 023 [i.41] related with the policy requirements for time-stamping authorities; and
- ETSI TS 101 861 [i.39] related with the time-stamping profile.

5.4.3.4 Trust representation

Section 6.5 of the "Minimum operational procedures for ICP-Brazil Trust Service Providers" document (ref: DOC-ICP-17.01) defines the Trusted Service Providers List which contains the accredited entities under ICP-Brazil as Trusted Service Providers. The Trusted Service Providers List is required to be published by CA Root in textual format for human reading, and in XML format in order to process it by machine, and is required to be updated within 180 days.

Finally, the Trusted Service Providers List is encoded in XML format in accordance with the structure proposed by the standard ETSI TS 102 231 [i.44].

5.4.3.5 Reference material

Title	URL
Brazilian Provisional Measure nº 2.200-2 (27/07/2001) by which establishes a Brazilian Public Key Infrastructure (ICP-Brazil); transforms the National Institute of Information Technology into autarky, and gives other measures	https://presrepublica.jusbrasil.com.br/legislacao/100256/medida-provisoria-2200-01
Accreditation criteria and procedures for ICP-Brazil entities v5.4	https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/03/DOC-ICP-03_-_v.6.0_-_CRIT._E_PROCED._PARA_CRED._DAS_ENT._INTEG._DA_ICP-BRASIL.pdf
Brazilian Provisional Measure 2.200-2 (24 August 2001)	https://www2.camara.leg.br/legin/fed/medpro/2001/medidaprovisoria-2200-2-24-agosto-2001-391394-publicacaooriginal-1-pe.html
Minimum operational procedures for ICP-Brazil Trust Service Providers (DOC-ICP-17.01)	https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/17.1/DOC-ICP-17.01-vers%C3%A3o_2.1_PROCEDIMENTOS_OPERACIONAIS_M%C3%8DNIMOS_PARA_OS_PRESTADORES_DE_SERVI%C3%87O_DE_CONFIAN%C3%87A_DA_ICP-BRASIL.pdf
Criteria and procedures for conducting audits in ICP-Brazil entities	https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/08/DOC-ICP-08_Versao_4.5.pdf
ICP-Brazil Trust Service Providers Certification Practice Statement minimum requirements	https://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/17/DOC_ICP_17_-_verso_1.0_REQUISITOS_MINIMOS_PARA_AS_DECLARACOES_DE_PRATICAS_DOS_PRESTADORES_DE_SERVICO_DE_CONFIANCA_DA_ICP-BRASIL.pdf

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, the Certification Service Providers, the electronic signature certificates, the accreditation and supervision processes on Certification Service Providers and the rights and obligations of electronic signatures users.

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 and the use of technical standards.

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 recognize 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.

Chilean providers are not called Trust Service Providers as in the EU, but rather are known as Certification Service Providers or simply Certifier.

According to article 14 of the Decree 181, the Chilean Accreditation Entity function will be developed by the Undersecretary of Economy, Development and Reconstruction whose functions are now 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.

Chilean regulation considers the provision of the following services: advanced electronic signature certificate generation service. In that sense, there are four different modalities of the certification service: based in smartcard or HSM for remote signature; based in a mobile device (also called provision of mobile signature service); and, based in a smartcard with biometric capabilities, also called "provision of biometrical certification services". Chilean regulation also provides for time-stamping services.

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 with some specific requirements such as to guarantee the existence of a secure service in order to consult the register of issued certificates or have the required technological capacity for the development of the certification activity, among other requirements.

Article 18 of Law 19799 describes the accreditation process. 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 audit and is required to follow some specific steps.

5.4.4.3 Best practice

According to article 47 of the Decree 181, the Ministry General Secretariat of the Presidency is 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 standards:

- Related with the Advanced Electronic Signature:
  - ETSI TS 102 231 [i.44] (trust model);

  - ETSI TS 102 042 [i.40] (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.40] (physical security of the Certification Service Provider infrastructure providing biometric services).

- Related with time-stamp service:
  - ETSI TS 102 042 [i.40] (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 [i.41] (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 [i.41] (Use of mobile devices; Mobile signature generation procedure);
  - ETSI TR 102 206 [i.43] (Level of protection offered for the mobile signature generation procedure);
  - ETSI TS 102 042 [i.40] (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 provider 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 sets 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 [i.49] and ETSI TS 119 431-2 [i.50] 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 the use of FIPS 140-2 [i.29] based solutions.

- Alignment of the current ETSI standards admitted in Chile to the last ETSI EN versions. The mobile-based advanced electronic signatures certification however is believed to be based on old ETSI standards.

5.4.4.6 Reference material

Title	URL
Chilean Law 19799/2002 on electronic documents, electronic signature and signature certification services	https://www.leychile.cl/Navegar?idNorma=196640
Chilean Decree 181/2002 approves the Regulation on Chilean Law 19799 on electronic documents, electronic signature and signature certification services	https://www.leychile.cl/Navegar?idNorma=201668
Chilean Decree 24/2019 approving an additional regulation for the provision of an advanced electronic signature certification service	https://www.leychile.cl/Navegar?idNorma=1130382
Accreditation Assessment Procedure Guidelines Advanced Electronic Signature Certification Service Provider version 2.0	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2010/11/FEA.pdf
Accreditation Assessment Procedure Guidelines Mobile Signature Certification Service Provider version 1.1	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2019/01/Gu%C3%ADa-de-Evaluaci%C3%B3n-Procedimiento-de-Acreditaci%C3%B3n-PSC-FMO-v1.11-1p.pdf
Accreditation Assessment Procedure Guidelines TSA Certification Service Provider version 1.0	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2010/11/TSA.pdf
Accreditation Assessment Procedure Guidelines Biometric Certification Service Provider version 1.0	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2010/11/BIO.pdf
Annual inspection guidelines for Certificate Service Providers v.2.1	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2013/02/Gu%C3%ADa-para-Inspecci%C3%B3n-Anual-de-Servicios-de-Certificaci%C3%B3n-v2.1.pdf

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 signatures and the requirements to fulfil to make it equivalent to a handwritten signature; the Certification Entities activities, requirements and obligations; certificate requirements such as certificate revocation, record preservation or recognition of foreign certificates; and the subscriber's liability and obligations.

Colombian Decree 1747, through which Law 527 is partially regulated in relation to certification entities, certificates and digital signatures, regulates the use of time-stamps, the closed and open Certification Entities requirements, including its accreditation process, security procedures and systems requirements, outsourced services, audit requirements or the use of digital certificates among other aspects.

Decree 1747 also regulates aspects related to the electronic data exchange, data message and document preservation (whether performed by a third party or not).

Colombian Decree 2364/2012 regulates the use of the electronic signature, including a technological neutrality statement, electronic signature trustworthiness, signer's obligations, and criteria to establish the electronic signature security level.

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 certificate subscribers and third parties are 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: electronic signature certificate generation for natural or legal person service; certificate generation on the verification regarding the alteration between sending and receiving the data message and electronic transferable documents service, certified digital signature data creation service, electronic signature data creation service; data messages generation, transmission and reception registration and time-stamping services, electronic transferable documents registration, preservation and recording services, data messages and electronic transferable documents archive and preservation services, any other activity related to the digital and electronic signatures creation or usage and electronic data exchange services.

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

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 are required to specifically indicate the activities in which they intend to be accredited and demonstrate to the Colombian National Accreditation Body some specific requirements such as 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 have to comply the same requirements as the closes certification entities plus some other specific requirements such as have 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 in the related legislation.

5.4.5.3 Best practice

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:

- ETSI TS 102 042 [i.40] (certificate life-cycle) with regard to digital certificates issuance activities (digital signature);
- ETSI TS 102 023 [i.41] Policy requirements for time-stamping authorities, with regard to time-stamping services activities.

5.4.5.4 Trust representation

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

5.4.5.5 Reference material

Title	URL
Chilean Law 19799/2002 on electronic documents, electronic signature and signature certification services	http://www.oas.org/juridico/pdfs/mesicic4_chl_ley19799.pdf
Chilean Decree 181/2002 approves the Regulation on Chilean Law 19799 on electronic documents, electronic signature and signature certification services	https://www.leychile.cl/Navegar?idNorma=201668
Chilean Decree 24/2019 (from here on: Decree 24) approves an additional regulation for the provision of an advanced electronic signature certification service	https://www.leychile.cl/Navegar?idNorma=1130382
Section 2.4 of annual inspection guidelines for Certificate Service Providers v2.1	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2010/11/IAO.pdf https://www.entidadacreditadora.gob.cl/wp-content/uploads/2016/07/Gu%C3%ADa-para-Inspecci%C3%B3n-Anual-de-Servicios-de-Certificaci%C3%B3n-Fe-de-Erratas.pdf
Section 2.7.2 of the Accreditation Assessment Procedure Guidelines Advanced Electronic Signature Certification Service Provider version 2.0	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2010/11/FEA.pdf
Related biometric services	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2010/11/BIO.pdf
Related time-stamp service	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2010/11/TSA.pdf
Related mobile signature service	https://www.entidadacreditadora.gob.cl/wp-content/uploads/2019/01/Gu%C3%ADa-de-Evaluaci%C3%B3n-Procedimiento-de-Acreditaci%C3%B3n-PSC-FMO-v1.11-1p.pdf

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, (from now on: Law 4017 on electronic signatures), distinguishes between electronic signatures and digital signatures. In the Spanish terminology, the electronic signature will be equivalent to an ordinary electronic signature, and the digital signature, to an advanced electronic signature.

Law 4017 on electronic signatures 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.

The Industry and Commerce Ministry, through the Vice Ministry of Commerce, is required to act as the Application Authority, and one of its functions is to authorize the operation of certification entities in Paraguay and to supervise and audit these entities.

According to article 21 of the Decree 7369, 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.

Article 8 of Decree 7369 also establishes that, in cases of foreign entities, compliance with the requirements contemplated in Law 4017 on electronic signatures, in the Decree and all the other requirements established by the Application Authority is required to be accredited.

Paraguayan legislation considers the provision of the following services: electronic signature certificates generation service; digital signature certificates generation service; time-stamping services; digital certificates in software module issuance service for individuals, legal entities, machines and applications data messages preservation service; data messages and digital document preservation services; public files digitalization service, and its preservation; original document reproduction through electronic means; and data messages delivery.

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 September 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 4017 on electronic signatures, the Certification Services Provider is required to meet some specific requirements in order to obtain an accreditation to operate as a provider.

Article 7 of Decree 7369, by which the general regulation of the law 4017 on electronic signatures is approved (from here on: Decree 7369), establishes the accreditation process for Certificate Service Providers.

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. among others:

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

b) proof that the provider has a team of people, a physical and technological infrastructure and security procedures and systems, to comply with the obligations related to all the digital services for which the provider requests authorization.

Article 42 of Law 4017 on electronic signatures states that the Application Authority is required to design an audit system to periodically audit Paraguayan Certification Service Providers. That audit system may be implemented by the Application Authority or by a third party authorized 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.

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

Articles 38 and 39 of Law nº 4610, which modifies and expands the Law 4017 on electronic signatures, establish that another function of the Industry and Commerce Ministry, through the Vice Ministry of Commerce, as the Application Authority, is to determinate 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.40] as an assessment standard applicable to: Certification Practice Statement, Certification Policy, 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 Law 4017 on electronic signatures, once a certification service provider has been enabled, it 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 Decree 7369, that register is called the Public Register of Certification Service Providers.

5.4.6.5 Reference material

Title	URL
Digital Certification Entities specific accreditation criteria	https://onac.org.co/images/2018/ECD/CEA-4_1-10_2015-08-13.pdf

5.4.7 Peru

5.4.7.1 Legal context

Peruvian Law N° 27269 of 8 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 1999/93/EC [i.64]).

The Law, however, does not define other trust services, but the Supreme Decree N° 52/2008 of 18 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 n° 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 26 June 2001 and article 72 of Supreme Decree 52/2008, digital certificates issued by foreign entities will have the same validity and legal effect recognized by Peruvian law if these certificates are recognized 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 n° 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 recognized 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 recognized 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 recognized 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 be 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 recognized, 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 28 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 n° 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 recognized, it is included in an official registry, known as the "Registro Oficial de Prestadores de Servicio de Certificación Digital", operated by INDECOPI, according to article 3 of Supreme Decree n° 26/2016 of 28 April 2016. This official registry is available below in the reference table and is implemented as a Trusted List, using ETSI TS 102 231 [i.44], offering XML and PDF versions.

5.4.7.5 Identified enablers

Time Stamp Authority services are provided by "Registro Nacional de Identificación y Estado Civil" through Added Value Service Providers, named "PSVA-TSA-RENIC", accredited within the IOFE. These services also fulfil the requirements contained in the following standards: IETF RFC 3161 [i.12], IETF RFC 3628 [i.13], ETSI EN 319 421 [i.61], ETSI EN 319 422 [i.62] and ETSI EN 319 401 [i.57] TSA.

5.4.7.6 Reference material

Title	URL
Trusted List	https://www.indecopi.gob.pe/web/firmas-digitales/lista-de-servicios-de-confianza-trusted-services-list-tsl-

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 and of advanced electronic signature as well as national accreditation bodies (also called Electronic Certification Unit, from here on: ECU) obligations and requirements.

Law 18.600 also defines 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) regulate the use of centralized custody advanced electronic signature services and the accreditation procedure of the Trust Service Providers and the Certification Service Providers, including monitoring over the accredited ones.

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

Article 12 of Decree 436/2011 defines the provision of the following certification services: Certification Authority services, Registration Authority services and Electronic Time-Stamping services.

Section 1.8 of the natural person advanced electronic signature policy with centralized custody defines the provision of the following trust services: advanced electronic signature policy with centralized custody services, digital identification services, time-stamping services and other services established by the ECU.

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

5.4.8.2 Supervision and auditing

Accrediting

According to article 13 of Decree 436/2011, the Certification Service Provider accreditation process begins by submitting to the ECU an application containing the required information which varies if the applicant is a natural person or a legal person. Among others, the applicant has to attach a legal audit report prepared by independent auditors chosen from those who were authorized by the ECU and also following the protocol defined by the ECU, a description of the technological platform, or has to inform the security plans and procedures that guarantee the provision of certification services.

Once the accreditation application has been technically approved, it is required to be communicated to the applicant.

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 required by the ECU. Certification Service Providers may request the accreditation renewal to the ECU.

Auditing

Numeral 1 of the Resolution 2/2019 (23/01/2019) establishes that electronic signatures accredited Certification and Trust Service Providers are 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.

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.

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 accreditation of a Certification Service Provider produces the incorporation to the Accredited Certification Services Providers Registry. In the same way, article 18 of Law 18.600 determines the creation of an Accredited Certification Services Providers Registry in charge of the ECU.

5.4.8.5 Reference material

At present, no references are available.

5.5 The Middle East & Africa

5.5.1 Arab-African e-Certification Authorities Network (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 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

At present, no references are available.

5.5.2 Israel

5.5.2.1 Legal context

Israel established its Electronic Signature Law 5761-2001, originally in 2001. This was last amended in 2010. This law is similar to the EU Electronic Signatures Directive 1999/93/EC [i.64] 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 are audited against CEN Workshop Agreement - CWA 14167-1, a risk analysis and a review of certification practice statement based on IETF RFC 3647 [i.14].

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 [i.33] 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 two CAs are registered under the Electronic Signature Law in Israel. Approved CAs are listed on the Ministry of Justice website with information on their root certificates published in a national newspaper.

5.5.2.5 Reference material

Title	URL
eSignatures law	https://www.justice.gov.il/Units/ilita/subjects/HatimaElectronic/Pages/electronicsignlaw.aspx
Ministerial orders	https://www.justice.gov.il/Units/ilita/subjects/HatimaElectronic/Pages/HanhayotCA.aspx
Ministry web site giving list of approved CAs	https://www.justice.gov.il/Units/ilita/subjects/HatimaElectronic/MeidaMeRashamCA/Pages/Gormim.aspx

5.5.3 Sultanate of Oman

5.5.3.1 Legal context

Oman Public Key Infrastructure (PKI) is a national initiative that sets the infrastructure needed for all government entities to provide eServices in Oman. The Oman National PKI is owned and operated by Information Technology Authority (ITA) as the legally Competent Authority.

The Electronic Transactions Law of the Sultanate of Oman has been issued by His Majesty's Royal Decree 69/2008.

In sum, two of the Law's primary objectives were:

i) to help streamline efficiency as regards the process by which e-transactions are conducted, and

ii) to create a safe "environment" for e-transactions to take place, such as protecting e-signature confidentiality and data integrity. The Law provides a list of procedural requirements and safety nets to be implemented by "Authentication Service Providers" who manage and provide electronic transaction services.

As per article 22, an electronic transaction will be regarded as a bona fide transaction provided that the following conditions are met:

- if it is determined that the device used for creating the signature is within the scope of its use and confined to the signatory exclusively;
- if the device used for creation of the signature is exclusively under the control of the signer at the time of signing;
- if no changes are detected as having taken place to the e-signature after the signature's time stamp was created; and
- if no changes are detected as having taken place with respect to the transaction itself after the signature's time stamp was created.

The above provisions are similar in substance to the requirements of "advanced electronic signatures" as specified in the eIDAS Regulation, while additionally requiring a "signature time stamp".

Article 11.(2) states that unless proved otherwise, an electronic signature is considered protected if the conditions stipulated in article 22 are fulfilled and it intends to sign or authenticate an electronic message on which it was put and it has not being changed since being originated. It also states that this electronic signature is required to be a reliable signature.

In terms of trust service types, the Law is limited to the issuance of digital certificates and the provisions on CSPs (also called Authentication Service Providers, equivalent to trust service provider) are similar in substance to the provision of articles 24(2), (3) and (4) of the eIDAS Regulation. The Law also includes provision of protection of private data to be observed by CSPs.

The Law does not define specific levels of reliability for digital certificates or for CSPs, i.e. there is no such concept of "qualified" CSP, "qualified" certificates, or "qualified" electronic signature.

Article 42 of the Law allows for recognition of digital certificates issued by foreign CSPs, provided their level of reliability (credibility) is not less than the one imposed by the Law on Oman CSPs. The recognition is required to be established by a ministerial decision.

5.5.3.2 Supervision and auditing

Oman has taken substantial and proactive measures to ensure that all companies falling under the purview of the Law comply with its requirements.

The competent Authority licenses, for five renewable years, authentication services according to the provisions and conditions provided for in the Law and its executive regulations and decisions. Article 25(d) and article 26 of the Law provide that the Competent Authority has jurisdiction to "monitor, supervise and inspect" Authentication Service Providers to ensure that they have complied with the requirements of the Law. Further, article 27 provides that the Minister of the Competent Authority may execute "judicial seizure." Based on its inspections, if the Competent Authority determines that an Authentication Service Provider has failed to comply with any technical and/or procedural protocols as required by the Law, it may cancel (revoke) the Provider's licence, thereby prohibiting the Provider from further engaging in electronic transactions.

An entity should meet all the policies and the accreditation agreements approved by ITA, which will conduct auditing activities periodically and according to the auditing report.

An external Registration Authority (RA) may be accredited as an external RA to manage its own subscriber. This is believed more convenient for conducting subscribers' identifications. Registration and Validation Teams will be trained by ITA. RAs are required to be aligned with National PKI policies and accreditation agreement and are subject to similar periodic supervisory and auditing activities than CSPs. Four such RAs have been accredited so far: The Royal Oman Police, Omantel, Ooredoo and the Central Bank.

The Oman PKI is targeting a WebTrust accreditation for its new national PKI to be hosted in a cloud environment, further enabling Digital Signing Solution and Remote Signing.

5.5.3.3 Best practice

The Oman National PKI is owned and operated by ITA. Other entities from the Sultanate of Oman have the possibility to set up their own PKI according to local governing laws and after getting the approval from ITA, using PKI services provided by ITA. In this way, ITA has the ability to host a CA that is providing PKI Services, on behalf of other entities which request ITA to do so. The Oman National PKI Center acts as an Operational Authority, delivers certification services on behalf of ITA in accordance with ITA approved policies, requirements and agreements. The Oman National PKI Center acts as a Certification Service Provider and supports all IT services related to the operation of the Oman National PKI.

It is also possible to join the Oman National PKI as a Time Stamping Authority (TSA).

Signature validation service is also mentioned as a trust service.

ITA Mobile PKI is a solution for mobile authentication and signing by a PIN code using a mobile phone. It combines superior security and end user convenience. It enables strong authentication and legally binding signatures. It is based on a SIM card storage of the user's private key, with on-board key generator.

In Oman 15,7 million digital certificates (authentication and signature) were issued on national ID cards and nearly 111 000 on mobile devices. In terms of transactions, over the period July 2017 to February 2019, 14,2 million were realized via national ID cards (less than one per certificate on average over whole period) while 1,7 million were conducted on mobile devices (somewhat more than 15 transactions per person). Thus, whilst the usage of ID card-based certificates is low, those with mobile based certificates are much more likely to use them.

In terms of compliance with ETSI standards, the Oman National PKI is aligned with:

- ETSI TS 102 042 [i.40] Policy requirements for certification authorities issuing public key certificates;
- ETSI TS 101 456 [i.38] Policy requirements for certification authorities issuing qualified certificates.

Digital signature formats used in Oman are mainly oriented around PAdES, with compliance with ETSI EN 319 142-1 [i.56], ETSI TS 103 172 [i.47] PAdES Baseline Profile, ETSI TS 102 778-1 [i.45] and ETSI TS 102 778-4 [i.46] (PAdES LTV Profile).

Time Stamp Authority follows policy requirements on the operations and management practices from ETSI TS 102 023 [i.41] V1.2.2.

ITA operates a signature validation service both for its own purposes and as a Trusted Third Party for its customers, complying with ETSI TS 119 441 [i.52].

5.5.3.4 Trust representation

The Oman National PKI is based on a root-signing model, where sub-CAs are root-signed by the national Root-CA.

5.5.3.5 Reference material

Title	URL
Oman Royal Decree 69/2008	https://www.ita.gov.om/ITAPortal/MediaCenter/Document_Library.aspx
Oman national PKI	Presentations at the ETSI/TRA workshop (02.05.2019 - Dubai) https://docbox.etsi.org/Workshop/2019/201905_MiddleEast_AfricaWS_GlobalisationofTrustServices/Oman%20National%20PKI_2019.pdf https://docbox.etsi.org/Workshop/2019/201905_MiddleEast_AfricaWS_GlobalisationofTrustServices/Oman%20National%20PKI_ETSI%20workshop_Dubai.pdf

5.5.4 United Arab Emirates

5.5.4.1 Legal context

The current trust service-related legal context in the United Arab Emirates (UAE) is driven by the Federal Law No. (1) of 2006 on Electronic Commerce and Transactions and the Ministerial Resolution No. (1) of 2008 regarding the issuance of Certification Service Provider Regulations.

The current UAE TSP regulatory framework does not cover all types of trust services that can be offered. It is limited mainly to provisions on electronic signatures and on certification service providers (CSPs) issuing related digital certificates.

As announced at the ETSI/TRA workshop held in Dubai in May 2019, the UAE is currently undergoing a revision of its national laws on electronic trust services aiming to cover various types of qualified trust services covering the emerging market demands. The new regulatory framework is aimed to be fully aligned with the European eIDAS Regulation and includes comprehensive requirements, including technical standards for TSPs and qualified TSPs, supervision and auditing requirements.

The UAE is targeting international recognition, firstly addressing the EU, but extensible to other regions, in particular to the Gulf Cooperation Council, the political and economic alliance of six Middle Eastern countries, namely Saudi Arabia, Kuwait, the UAE, Qatar, Bahrain and Oman.

The envisaged nine types of qualified trust services are:

- The provision of qualified certificates for electronic signatures.
- The provision of qualified certificates for electronic seals.
- The qualified preservation of qualified electronic signatures.
- The qualified preservation of qualified electronic seals.
- The qualified validation of qualified electronic signatures.
- The qualified validation of qualified electronic seals.
- The provision of qualified time stamps.
- The provision of qualified electronic delivery services.
- The provision of remote-QSCD as a service.

It is interesting to note that the provision of digital certificates for website authentication is not envisaged as a qualified trust service while a limited licensing (approval) scheme is foreseen for foreign CSPs issuing TLS, website authentication and/or code-signing certificates to be allowed to operate in the UAE.

The last QTS is also interesting as the equivalent of the managing and operation of a QSCD by a third party on behalf of the signatory/creator of the seal is regulated as a QTS for which prior authorization, audit and supervision would be required under the new UAE laws.

The future secondary legislation, associated to the draft new Law on electronic trust services, are expected to be more prescriptive in terms of technical standards the (Q)TSPs will have to conform with. The framework would allow new types of technology to emerge but, as a general principle, for a specific type of technology, a determined set of relevant (international) technical standards will be enforced, aiming to ensure implementation of excellence and best practices as well as maximizing interoperability.

5.5.4.2 Supervision and auditing

Prior to its entrance in the market for issuing digital certificate, a CSP is required to be licensed by the Telecommunications Regulatory Authority acting as licensing and supervisory body. The process for obtaining and maintaining a license, issued for five renewable years, requires the CSP to undergo an audit upon application for a license for the first time, every two years from the term of the license and upon application for renewal of the license.

Subject to the audit results, to the supervisory activities and failure of the CSP to conform to the UAE Laws, the TRA may suspend or revoke the license of a CSP.

The current requirements on the auditor are currently rather limited requiring the auditor to be accredited by a recognized professional organization or association acceptable to the TRA, to be qualified as a Certified Information Systems Auditor, an AICPA Certified Information Technology Professional, a Certified Internal Auditor or to have another information security auditing credential recognized by the TRA, to be entitled to conduct ISO/IEC 27001 [i.24] audits and to possess sufficient knowledge of and experience in eSignature, PKI, electronic programmes and information security tools and systems, financial and security reviews and professional audit techniques.

The audit required to be conducted on a CSP is based on ISO/IEC 27001 [i.24], scoped to the provision of digital certificates by a CSP conformant to the provisions of the UAE Laws.

The new UAE licensing model has foreseen that the new UAE regulatory framework on (Q)TSP/(Q)TS is expected to be closely aligned with the model currently in force in Europe for the accreditation of auditors (conformity assessment bodies or CABs), i.e. ISO/IEC 17065 [i.23] supplemented by ETSI EN 319 403 [i.54], but with TRA technical resolutions (secondary legislation) and referenced standards as normative documents.

5.5.4.3 Best practice

The future UAE regulatory framework is expected to align the requirements from the future TRA technical resolutions (secondary legislation) with the latest versions of the trust services related ETSI standards. As a result, profiled versions of those standards would be the normative documents against which ISO/IEC 17065 [i.23] / ETSI EN 319 403 [i.54] accredited CABs would certify (Q)TSP/(Q)TS operating in the UAE.

5.5.4.4 Trust representation

The current trust representation of the licensed CSPs in the UAE is a simple list maintained by the TRA.

It is expected that the new UAE regulatory framework on electronic trust services will be based on a trusted list model compliant and interoperable with the EU trusted lists, leveraging on the ETSI TS 119 612 [i.53] specifications.

It is also expected that this trusted list-based trust representation will be the first step towards an extension to a Gulf Cooperation Council trusted list federating the trust representation of the (Q)TSP/(Q)TS of the Gulf Cooperation Council countries.

5.5.4.5 Reference material

Title	URL
Federal Law No. (1) of 2006 on Electronic Commerce and Transactions	Direct: https://www.tra.gov.ae/assets/B7jM7GgG.pdf.aspx Repository: https://government.ae/en/resources/laws
Ministerial Resolution No. (1) of 2008 regarding the issuance of Certification Service Provider Regulations	Direct: https://www.tra.gov.ae/assets/zfQj6vp3.pdf.aspx Repository: https://government.ae/en/resources/laws
The UAE current state and views on globalization of trust services	Presentation at the ETSI/TRA Middle East and Africa Workshop on Globalization of Trust Services - May 2, 2019.

5.5.5 Botswana

5.5.5.1 Legal context

The Electronic Communications and Transactions Act ("the Act"), enacted by Botswana in 2014, drives the legal provisions on electronic signatures as a fundamental element supporting electronic commerce. The Act is supplemented by subsidiary legislation in order to properly give effect to certain elements of the principal legislation, including the Electronic Communications and Transactions Regulations ("the Regulations") Statutory Instrument No. 42 of 2016, which was published on 8 April 2016.

The Act makes the Botswana Communications Regulatory Authority (BOCRA) responsible for accrediting and managing CAs, developing technical standards, handling legal and policy issues and appointing a pool of auditors from which interested CAs can choose during the auditing process.

For an electronic signature to be considered as equivalent to a handwritten signature, it needs to be secure in terms of article 25 of the Act, comparable in substance to the provisions of advanced electronic signature in Europe. The accreditation of an electronic signature product/service is necessary if one is claiming outright that his or her electronic signature product/service can provide the same evidentiary weight as a handwritten signature. The Regulation states that the Authority is required to only award accreditation of an electronic signature where it is satisfied that:

a) the secure electronic signature:

   i) conforms with the requirements of article 25 of the Act and is capable of identifying the signatory;

   ii) is created by a qualifying signature creation device and verified by a secure signature-verification device;

   iii) is based on a qualifying certificate; and

   iv) complies with the international standards with which the CSP claims in its application for accreditation;

b) the certification service provider meets the requirements of the Regulations including those set out in Schedule 2, which are comparable to requirements set out in articles 24.2, 24.3 and 24.4, and Annexes I and II from the eIDAS Regulation.

The Accreditation Certification Service Standards ("ACS Standards, 2017"), issued in accordance with the Regulations, Schedule 1, aim to further supplement the provision of the Act and the Regulations by providing details as to the standards that are to be achieved for a certification service provider to qualify for accreditation by BOCRA.

The accreditation certificate issued by BOCRA at the end of a successful CSP (CA) accreditation process is valid for two years.

The Electronic Records (Evidence) Act No. 13 of 2014 allows for the admissibility and authentication of electronic records as evidence in legal proceedings and admissibility, in evidence, of electronic records as original records. Section 5 of the Act provides that nothing in the rules of evidence is required to apply to deny admissibility of an electronic record as evidence because it is an electronic record. Section 6(2) of the Act designates BOCRA as the Certifying Authority and requires BOCRA to establish an approved process for the production of electronic documents and also certify electronic records systems for purpose of integrity. The Electronic Records (Evidence) Regulations of 2016 establish an approved process for the certification of electronic systems. Unless otherwise provided in any other written law, where an electronic record is tendered as evidence, such an electronic record is required to be admissible if it is relevant and if it is produced in accordance with this approved process.

5.5.5.2 Supervision and auditing

Auditors are independent audit firms appointed by the BOCRA in accordance with the Act and the Regulations. BOCRA publishes an Accredited Certification Standards Compliance Checklist for compliance audit purposes.

CAs applying for an accreditation may choose an auditor from the pool of auditors appointed by BOCRA. A conformity audit is required at accreditation initiation and renewal.

BOCRA monitors the conduct, systems and operations of accredited CSPs to ensure they comply with the laws and where necessary may require accredited CSPs to undergo an audit so to verify. BOCRA may temporarily suspend or cancel an accreditation.

5.5.5.3 Best practice

As mentioned above, the ACS Standards supplement the provision of the Act and the Regulations by providing details as to the standards that are to be achieved for a CSP to qualify for accreditation by BOCRA.

The ACS Standards require a qualifying CA to be compliant with ISO 21188:2006 [i.28]. Thus, in order to be accredited, a CSP is required to show that it abides by ISO 21188:2006 [i.28] in its entirety as well as the provisions in the ACS Standards.

In addition, the Authority will recognize for accreditation CAs which complies with WebTrust, CA/Browser Forum Baseline Requirements [i.22] and ETSI TS 101 456 [i.38].

5.5.5.4 Trust representation

The Regulations requires BOCRA to keep, maintain and publish a register, on its website or by any other means, of all accredited CSPs, together with their names and address.

The recognition of foreign digital certificates and foreign electronic signatures is automatically established by the Electronic Communications and Transactions Act of 2014 (Part V, 31). The determination of the legal effectiveness of a certificate or of an electronic signature is regardless of the location where they have been issued or created/used and of the location of the issuer or signatory. Foreign certificates and electronic signatures are required to have the same legal effect in Botswana as their local counterparts as they offer a substantially equivalent level of reliability.

5.5.5.5 Reference material

Title	URL
Electronic Communications and Transactions Act 2014	https://www.bocra.org.bw/sites/default/files/documents/Electronic-Communications-and-Transactions-Act-2014.pdf
Electronic Communications and Transactions (Amendment) Act 2018	https://www.bocra.org.bw/sites/default/files/documents/31%20Act%2010-08-2017-electro%20comm%20and%20trans%20.pdf
Electronic Communications and Transactions Regulations, 2016	https://www.bocra.org.bw/sites/default/files/Electronic%20Communications%20and%20Transactions%20Act%20Regulations%202016.pdf
Electronic Records (Evidence) Act 2014	https://www.bocra.org.bw/sites/default/files/documents/Electronic%20Records%20Act.pdf
Electronic Records (Evidence) Regulations - SI 55 of 2016	https://www.bocra.org.bw/sites/default/files/documents/Electronic%20Records%20%28Evidence%29%20Regulations%20-%20SI%2055%20of%202016.pdf
Application procedure for secure electronic signature provider (Certification Authority) - Accreditation - August 2017	https://www.bocra.org.bw/sites/default/files/Accreditation%20Procedure%20-%20rev%201%20%28002%29%20%281%29.pdf
Accreditation Certification Service Standard, 2017 (ACS Standards, 2017)	https://www.bocra.org.bw/sites/default/files/ACS%20Standards%20-%20August%202017.pdf
Accredited Certification Standards Compliance Checklist	https://www.bocra.org.bw/sites/default/files/ACS-checklist%20%281%29.pdf

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 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

Presently no references materials available.

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 Hongkong 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).

Hong Kong is committed to establishing the infrastructure to facilitate a digital economy. One of such infrastructures is the legal framework to support secure electronic transactions. The Electronic Transactions Ordinance (Cap. 553) ("ETO"), which was enacted in January 2000 and updated in June 2004, provides the legal framework for the recognition of electronic records and signatures, giving them the same legal status as their paper counterparts.

Hongkong Post is a Recognized Certification Authority ("CA") by virtue of the ETO who perform the functions and provide the services of a CA. Since 1 April 2007, the Hongkong Post CA operations have been outsourced with private sector participation. At the time of writing the present document, Hongkong Post CA has awarded a contract ("Contract") to Certizen Limited for operating and maintaining the systems and services of Hongkong Post CA.

Commercial CA may voluntarily apply to the Government of Hong Kong Special Administrative Region for recognition and once recognized the CA is required to comply with the requirements of the ETO and the Code of Practice for Recognized Certification Authorities ("Code of Practice") published by the Government Chief Information Officer ("GCIO") with a view to enhancing public confidence in electronic transaction with the use of recognized digital certificates issued by recognized CAs. Recognition will only be granted to those CAs that have reached a standard acceptable to the GCIO and hence the trustworthiness of their systems and services is better ensured.

The key provisions of the ETO aim to provide that:

a) if a rule of law requires or permits information to be or given in writing, the use of electronic records satisfies the rule of law;

b) if a rule of law under a statutory provision specified in Schedule 3 to the ETO requires or permits a document to be served on a person by personal service or by post, the service of the document in the form of an electronic record satisfies the rule of law;

c) if a rule of law requires a signature of a person on a document and neither the person whose signature is required nor the person to whom the signature is to be given is or is acting on behalf of a government entity, an electronic signature satisfies the requirement;

d) if a rule of law requires a signature of a person on a document and the person whose signature is required and/or the person to whom the signature is to be given is/are acting on behalf of a government entity/entities, a digital signature satisfies the requirement;

e) if a rule of law requires certain information to be presented or retained in its original form, that requirement is satisfied by presenting or retaining the information in the form of electronic records; and

f) if a rule of law requires certain information to be retained, that requirement is satisfied by retaining electronic records.

For transactions not involving Government entities, a signature requirement under the law can be met by any form of electronic signature so long as it is reliable, appropriate and agreed by the recipient of the signature. For transactions involving Government entities, a signature requirement under the law will be satisfied by digital signature.

Hongkong Post CA issues the following types of digital certificates to individuals and organizations in Hong Kong:

- Hongkong Post e-Cert for authentication, signing electronic transactions, encrypted emails or TLS/SSL communications.
- Hongkong Post Bank-Cert for signing electronic documents in banking industry.
- Hongkong Post g-Cert for signing electronic transactions, encrypted emails or instant messages of the Government bureaux and departments.

Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong

The Mainland of China and Hong Kong have concluded a number of free trade agreements under the main document of "Mainland/Hong Kong Closer Economic Partnership Arrangement" since 2003. On 29 July 2008, the Mainland of China and Hong Kong signed the Supplement V to this partnership agreement, which laid out the "Framework for the Mutual Recognition of Electronic Signature Certificates", and hence developed the "Arrangement for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong" ("Arrangement") and "Certificate Policy for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong" ("Mutual Recognition Certificate Policy") in August 2012.

Under the Arrangement, CA recognized under the ETO may submit their applications to GCIO for participation in the mutual recognition scheme. On 30 September 2018, an updated version of the Mutual Recognition Certificate Policy in Guangdong and Hong Kong was published to support remote non-face-to-face identity verification and enhance the technical standards of the mutual recognition certificates to meet the development of cross-boundary business in the industry.

Hongkong Post CA issues the following types of digital certificates with mutual recognition status to individuals and organizations in Hong Kong:

- Hongkong Post e-Cert for authentication or signing electronic transactions.

5.6.2.2 Supervision and auditing

Recognition as a Recognized CA

Under the ETO, the Government Chief Information Officer ("GCIO") is the authority for granting recognition to certification authorities ("CAs") and to the certificates that recognized CAs issue. Recognition will only be granted to those CAs and digital certificates that meet the trustworthiness standard and other requirements of the Government. Recognition of CAs and certificates is governed under relevant provisions of the ETO.

In determining whether the CA is suitable for recognition, the GCIO is required to, in addition to any other matter the GCIO considers relevant, take into account the following:

- whether the applicant has the appropriate financial status for operating as a recognized CA in accordance with the ETO and the Code of Practice for Recognized Certification Authorities ("Code of Practice");
- the arrangements put in place or proposed to be put in place by the applicant to cover any liability that may arise from its activities relevant for the purposes of the ETO;
- the system, procedure, security arrangements and standards used or proposed to be used by the applicant to issue certificates to subscribers;
- a report which contains an assessment as to whether the CA is capable of complying with the provisions of the ETO and of the Code of Practice as are specified in the Code of Practice;
- whether the CA and its responsible officers are fit and proper persons; and
- the reliance limits set or proposed to be set by the CA for its certificates.

Regarding the above-mentioned report, it is required to be prepared by a person approved by the GCIO as being qualified to make such a report. Qualifications of the person are set out in the Code of Practice.

For recognized commercial CA, the validity period for recognition will normally be three years. The recognized commercial CA may apply to the GCIO for renewal of the recognition.

For Hongkong Post CA, the recognition is perpetual by virtue under the ETO. Furthermore, with respect to the publication of information responsibilities for CA that adhere to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [i.31] published by CA/Browser Forum, Hongkong Post has disclosed its Certification Practice Statements and its commitment to provide Publicly-Trusted Certificates including SSL certificates in conformity with CA/Browser Forum Baseline Rreuqirement. The WebTrust for CA audit, the WebTrust for SSL Baseline Requirements, and the WebTrust for Extended Validation SSL certificate operation for Hongkong Post CA are performed annually and the audit reports are disclosed on its website.

Common web browsers such as Microsoft® Internet Explorer, Apple® Safari, Mozilla® Firefox™ and Google Chrome® come with the Hongkong Post CA root certificate included, in other words trusted by default. Users of these web browsers visiting websites that are installed with the Hongkong Post e-Cert (Server) certificate will be free from certain alert messages or manual intervention when their browsers establish a secure connection to these websites.

Hongkong Post CA is also a member of the Adobe® Approved Trust List ("AATL"). AATL was introduced in Adobe® Acrobat Reader® v9.0. Therefore, Hongkong Post CA's signing certificates are compatible with Adobe® Version 9+.

Recognition of Certificates

A recognized CA may apply to the GCIO for recognition of some or all of its certificates.

In general, as long as a recognized CA maintains its recognition status, the recognition status of a recognized certificate issued by the recognized CA will not change provided that the relevant certification practice statement ("CPS"), including the relevant certificate policy that governs the recognized certificate, has not materially changed.

For the recognition of a particular certificate or a type, class or description of certificates, the GCIO is required to, in addition to any other matter the GCIO considers relevant, take into account the following:

- whether the certificate(s) are issued in accordance with the recognized CA's CPS;
- whether the certificate(s) are issued in accordance with the Code of Practice;
- the reliance limit set or proposed to be set for that particular certificate, or that type, class or description of certificates, as the case may require; and
- the insurance policy put in place or proposed to be put in place by the recognized CA to cover any liability that may arise from the issue of that particular certificate, or that type, class or description of certificates, as the case may be.

5.6.2.3 Best practice

According to the Code of Practice published by the GCIO, the Mutual Recognition Certificate Policy, the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [i.31] published by CA/Browser Forum and the Principles and Criteria of WebTrust for CA, Hongkong Post CA publishes its certification practice statement ("CPS") for the types, classes or descriptions of recognized certificates that it issues in its website.

The structure of certification practice statement ("CPS") follows either IETF RFC 3647 [i.14] or IETF RFC 2527 [i.10] standard depending on the types of recognized certificates.

Hongkong Post CA digital certificate services are based on the Recommendation ITU-T X.509 [i.65] and the IETF equivalent IETF RFC 5280 [i.17] standard. In respect to TLS/SSL certificates, Hongkong Post CA supports Certificate Transparency in accordance with IETF RFC 6962 [i.20] standard and Online Certificate Status Protocol response conforms to IETF RFC 6960 [i.19] and IETF RFC 5019 [i.15] standards.

5.6.2.4 Trust representation

Trust representation of recognized CA in Hong Kong can be realized by either trust service store mechanism or trust list/record mechanism.

For example, recognized certificate issued by Hongkong Post CA is published in a disclosure record of GCIO website for public access. The disclosure record contains a statement of establishment of CA, contact details, CA certificates, repository information, CPS and assessment reports.

For recognized certificate with mutual recognition status and the verification method of such certificate type, an official trust list is published by the Government of the two places for public access.

Common browsers such as Microsoft® Internet Explorer, Apple® Safari, Mozilla® Firefox™ and Google Chrome®, and Adobe® Acrobat Reader® have trusted Hongkong Post CA root certificate in their root certificate store.

5.6.2.5 Reference material

Title	URL
Certizen homepage	https://www.certizen.com
Introduction to the Electronic Transactions Ordinance (Chapter 553)	https://www.ogcio.gov.hk/en/our_work/regulation/eto/ordinance/introduction/
Subsidiary Legislation Under the ETO	https://www.ogcio.gov.hk/en/our_work/regulation/eto/ordinance/subsidiary/
Disclosure Records of Recognized Certification Authorities	https://www.ogcio.gov.hk/en/our_work/regulation/eto/ca/disclosure_records/index.html
List of recognized certificates available for subscriptions	https://www.ogcio.gov.hk/en/our_work/regulation/eto/ca/rec_certs/
Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong	https://www.ogcio.gov.hk/en/our_work/business/mainland/cepa/mr_ecert/
Trust List of Certificate Types with Mutual Recognition Status	https://www.ogcio.gov.hk/en/our_work/business/mainland/cepa/mr_ecert/trust_list/hk_guangdong_ecert_trust.html

5.6.3 India

5.6.3.1 Legal context

For the PKI scheme managing Digital Signature Certificates 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 established the Root CA of India under section 18(b) of the Adherence to Information Technology Act, 2000 (IT Act) to digitally sign the public keys of CAs in the country. The Root CA of India 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.53] 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. Popularly known as eSign, this remote signing is made through a regulated but openly published APIs making it easier for any application to develop and integrate it. The live integration licensing of these APIs go through on-boarding procedure of application (like banks, enterprise resource planning, private sector, government applications, etc.) by CA through which they facilitate to end users. The security architecture of this remote signing system contains tamper-protected environment for signer activation as well as private key activities. The private keys are generated in a minimum of FIPS 140-2 [i.29] Level 3+ Hardware Security Modules in a trusted & tamper protected environment. While the architecture supports both RSA and ECC algorithms, CAs in India use ECC keys for its smaller size and faster functionality. Some of the CAs also use LTV and Timestamp enabled signatures in line with IETF RFC 3126 [i.11] to support signatures with complete validation. This achieves Long Term Archival requirements. As the signature responses support "RAW-ECDSA" as well as "PKCS#7" and IETF RFC 5652 [i.18] Cryptographic Message Syntax detached signatures, the use case implementations cover PDF documents, text signing, JSON signing, XML signing among various document types. The overall scheme and architecture is analysed and compared against ETSI requirements, and broadly meets with CEN Standards for remote signing systems (CEN EN 419 241-1 [i.35] and CEN EN 419 241-2 [i.36], CEN EN 419 221-5 [i.37]) and ETSI Signature Creation Protocols and Policy Requirements (ETSI TS 119 431-1 [i.49] and ETSI TS 119 431-2 [i.50], ETSI TS 119 432 [i.51]). As of 2019, this remote signing model has more than 50 million unique users covering nearly 4 % of its population.

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, TLS/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 [i.54].

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 empanelled 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 CCA by trained, empanelled auditors. The criteria are described as a checklist and is more or less equivalent to other global audit schemes.

5.6.3.3 Best practice

CCA tightly governs this ecosystem with their approved India PKI Certificate Policy (CP). CAs are not allowed to have their own CP and should necessarily comply with India PKI CP which defines different classes/assurance levels, the key protection/storage requirements, certificate profiles, liability, etc.

While CAs are required to publish their own Certificate Practice Statement (CPS), this is imposed through a standard CPS template provided by CPS with nearly-zero deviation permitted. The final CPS is submitted by CA to CCA and goes through approval process, and later published in websites of CCA as well as the CA. CAs are required to run their own repository and publish this CPS, along with other prescribed information. CPS contains controls on the CAs that are similar or equivalent to ETSI EN 319 411-1 [i.58]: 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.

Apart from publishing CP and governing CPS, CCA also provides detailed guidelines on CA physical infrastructure (Site) Guidelines, remote signing guidelines, TLS/SSL guidelines, timestamping guidelines, etc.

5.6.3.4 Trust representation

As of 2019, there about 10 CAs licensed and operations in India. It is mandatory for a CA to be licensed under CCA as per Indian IT Act. The licensed CAs are issued with technical certification through public key which is under root CA and forms the trust chain. This is in addition to a paper license certificate approved by CCA. Additionally, the licensed CAs are publicly published in CCA website, which forms as authentic source of published trust list for India. Under India PKI CP, all relying parties are required to trust and accept the certificate issued under this trust list.

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

Title	URL
India Controller of Certification Authorities (CCA)	http://www.cca.gov.in/
CA infrastructure and CCA hierarchy	http://www.cca.gov.in/IndiaPKIPolicyFramework.html
Complete list of accredited CAs	http://www.cca.gov.in/licensed_ca.html
Complete list of all CA certificates	http://www.cca.gov.in/ca_certificates.html
List of empanelled auditors	http://www.cca.gov.in/list_emplaned_auditors.html
Adequacy of security policies and implementation	http://www.cca.gov.in/adequacy_of_security.html
Existence of adequate physical security	http://www.cca.gov.in/existence_of_adequate.html
Evaluation of functionalities in technology as it supports CA operations	http://www.cca.gov.in/evaluation_of_functionalities.html
CA's services administration processes and procedures	http://www.cca.gov.in/ca_services.html
Compliance to relevant CPS as approved and provided by the Controller	http://www.cca.gov.in/compliance_to_relevant.html
Adequacy of contracts/agreements for all outsourced CA operations	http://www.cca.gov.in/adequacy_of_contracts.html
Adherence to Information Technology Act, 2000, the rules and regulations thereunder, and guidelines issued by the Controller from time-to-time	http://www.cca.gov.in/adherence_to_information.html
CCA Certificate Practice Statement (CPS)	http://cca.gov.in/cps.html

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, Japanese Institute for the Promotion of Digital Economy and Community (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.58] and ETSI EN 319 411-2 [i.59] 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 certificate policy and certification practices statement of each Accredited Certification Business is created in compliance with IETF RFC 2527 [i.10].

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 audited 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, the accreditation entity of e-Signature Act is Ministry of Internal Affairs and Communication, Ministry of Justice and Ministry of Economy, Trade and Industry. 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 receives and makes a decision to or not to accredit the SCB. It should be noted that the DIO will be established in Japan.

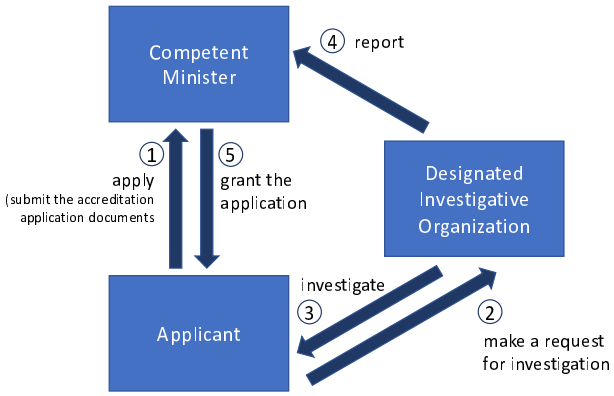

Figure 4: Accreditation scheme (derived from competent ministry)

JIPDEC has been also running the "JCAN Trusted Service Registration", which examines the reliability of certificate issuing authorities, Local Registration Authorities and electronic contracts (remote e-signature models). As many private Certification Authorities have not received external review, this service assesses the credibility from the perspective of a third party and publishes the results in an easy-to-understand format.

Japan Data Communications Association (JADAC) runs the accreditation program for Time Authorities and Time-Stamping Authorities, which is a voluntary program for time-stamping services. The program can approve the accreditation of the services of both types of authorities 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.40];
- ETSI EN 319 411-1 [i.58]; and
- ETSI EN 319 411-2 [i.59].

Furthermore, and although not able to compare perfectly, JCAN Trusted Service Registration and ETSI EN 319 403 [i.54] 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 Time Authorities and Time Stamping Authority services references ISO/IEC standards, including:

- ISO/IEC 18014 parts 1 to 3 on time-stamping services [i.21];
- IETF RFC 3161 [i.12] - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP);
- ETSI TS 102 023 [i.41] Policy requirements for time-stamping authorities.

With a view towards equivalence with ETSI EN 319 403 [i.54], 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.53] 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 JCAN trusted services examined by JIPDEC is published to the JCAN Trusted Service Registration List.

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.53] 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.53].

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.58] and ETSI EN 319 411-2 [i.59], according to some interviewed experts, should be established in Japan.

5.6.4.6 Reference material

Title	URL
JIPDEC trusted service registration	https://itc.jipdec.or.jp/jcan-trusted-service
JIPDEC accredited certification services list	https://esac.jipdec.or.jp/srvList.html
Ministry of Internal Affairs and Communication	http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/d-nintei.html
Ministry of Justice	http://www.moj.go.jp/MINJI/minji32.html
Ministry of Economy, Trade and Industry	http://www.meti.go.jp/policy/netsecurity/esig-srvlist.html
Time Stamping Service Accreditation Center	https://www.dekyo.or.jp/tb/contents/english/index.html
e-Government recommended cipher list	https://www.cryptrec.go.jp/en/list.html

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 website, 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 in clause 5.2.1.

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, non profit organisation 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

Title	URL
Asia PKI homepage	https://www.asiapki.org

NOTE: A report by the Asia PKI consortium is in progress describing the approach taken by members of the Consortium which may be taken into account in later versions of the present document. 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

5.7.1.1 Legal context

The Secure Electronic Signatures Regulation (SOR/2005-30) was adopted pursuant to the Personal Information Protection and Electronic Documents Act and the Canada Evidence Act. This regulation is based on the use of digital signatures supported by public key certificates giving legal presumption. The regulation has minimal further technical requirements on the certificate or the certificate authority. It states that CAs recognized as such are listed on the website of the Treasury Board Secretariat.

However, there is little sign of general adoption of electronic signatures under this regulation.

The official Government of Canada PKI is governed by the Treasury Board. One branch of the Department of National Defense PKI which is Cross-Certified with US Department of Defense as part of the Five-Eyes intelligence programme. The only trust for PKI within the Federal Government is to the Government of Canada Root. In 2009, the specific policy on PKI was rescinded to align responsibilities and accountabilities for secure electronic transactions under the general Canadian policy on government security and its supporting instruments.

A pan-Canadian trust framework has been established, but this is generally concerned with identity management and does not have much specific focus on PKI.

5.7.1.2 Supervision and auditing

There is a process defined on the Canadian Treasure Board website on the recognition process for certificate authorities under the secure electronic signatures regulation, but it could not be ascertained whether this has been applied to any CAs.

5.7.1.3 Best practice

Examples of best practice are presently unknown.

5.7.1.4 Trust representation

Officially, certificate authorities are listed on the Treasury Board's website, though it is not clear whether such a list exists.

5.7.1.5 Reference material

Title	URL
Secure Electronic Signatures Regulation	https://laws-lois.justice.gc.ca/eng/regulations/sor-2005-30/index.html
Secure Electronic Signature Regulations Recognition Process	https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/secure-electronic-signature-regulations-recognition-process.html
Government of Canada PKI	https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=20008

5.7.2 México

5.7.2.1 Legal context

Mexican Advanced Electronic Signature Law of 11 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 Service Providers are 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 CAs, RAs, 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 Service Providers is required to be subject, and the Mexican Commerce Code also define other trust services such 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 Legally Authorized Third Party, 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 1999/93/EC [i.64]).

According to the General Rules, the Mexican Federal Government seeks to strengthen policies, strategies and guidelines on the use of advanced electronic signatures as a factor in electronic government and the simplification of the interaction between traders and government. 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 Service Providers for the issuance of digital certificates and other additional services of advanced electronic signatures.

According to article 114 of the Mexican Commercial Code, 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.

Additionally, 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, article 114 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 for Certification Service Providers; and
- The Mexican Commercial Code Regulation regarding Certification Service 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).

The accreditation process may be seen analogous to the eIDAS qualification process. According to articles 5 and 102 of the Mexican Commercial Code Regulation regarding Certification Service Providers, 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, economic 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 Service 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 Service 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 Service Provider, requirements determined by Mexican Commercial Code and its Regulation regarding Certification Service Providers;

4) resolve within forty-five working days following the submission of the application whether or not to grant accreditation as Certification Service 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 Service Providers, the audits performed by the Economy Department to the Certification Service Providers are 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 the other is that, while the ordinary will be carried out in working days and working hours, the extraordinary may be performed any time.

In order to be able to practice visits, the verifier 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 parties 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 a photograph issued by a competent authority accrediting the verifier to perform that function, and he or she will provide a copy to the owner, responsible party or 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 or 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 his or her own minutes.

The Mexican Acts and Regulations do not determine the validity of the Certificate Service Provider accreditation, as the basis of the audit repetition is not known.

5.7.2.3 Best practice

According to the General Rules, the Mexican Federal Government, through the Economy Department, is required to establish the standards in computer security related to electronic commerce and advanced electronic signatures, applying the principle of technological neutrality.

In order to be accredited, and to maintain that accreditation, according to several numerals contained in the General Rules, 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.40] applicable to:

- Physical security (ETSI TS 102 042 [i.40], clause 7.4.4);
- Business Continuity Plan (ETSI TS 102 042 [i.40], clause 7.4.8);
- Certificate Policy;
- Key Administration Plan (ETSI TS 102 042 [i.40], clause 7.2).

5.7.2.4 Trust representation

According to article 3 of the Mexican Commercial Code Regulation regarding Certification Service 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

Title	URL
Mexican Advanced Electronic Signature Law of 11 January 2012	https://eservicios.impi.gob.mx/seimpi/ayudaSEIMPI/LFEA.pdf
General Rules for Certification Services Providers	https://www.economia.gob.mx/files/transparencia/REGLA03.pdf
Mexican Commerce Code	http://www.diputados.gob.mx/LeyesBiblio/pdf/3_311218.pdf
Mexican Commercial Code Regulation regarding Certification Services Providers	http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_CComer_MPSC.pdf
Third Title of the Federal Administrative Procedure Law	http://www.diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf

5.7.3 US Federal PKI

5.7.3.1 Legal context

The US Federal PKI (FPKI) covers US Federal, State, Local, Tribal, Territorial, international governments and commercial organizations that work together to provide services for the benefit of the Federal Government.

In contrast to the Trusted List framework of eIDAS, the US FPKI 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 FPKI 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 FPKI Architecture. 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

The operation of CAs within the FPKI are overseen by a Policy Management Authority (PMA). The PMA oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain and generally oversees and manages the PKI Certificate Policies. For the FBCA, the PMA is the FPKIPA.

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-BioPharma, as previously mentioned).

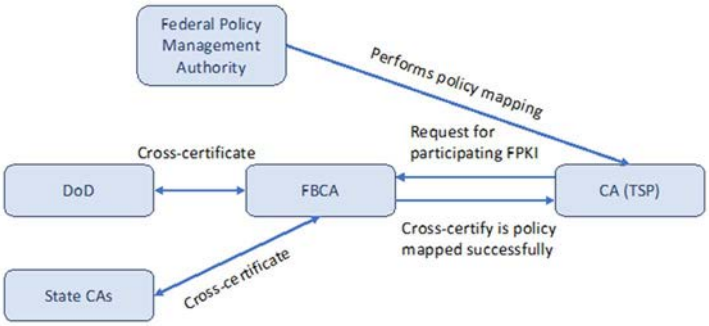

Figure 5: The trust framework of US Federal PKI

Cross-certification with FBCA can demonstrate that the TSP operation and its security level is equivalent to what the US Federal Government requires for their PKI system, which hence guarantees harmonization. However, one notable shortcoming of the system, as it currently stands, is that it is the need for of a bridge certificates are not regularly reviewed and sometimes includes TSPs that are still trusted, though without reason.

Requirements for audit are defined in the FPKI audit requirements. This requires CA to have a Certification Practice Statement, which conforms to the Certificate Policy that it claims to support.

5.7.3.3 Best practice

The FPKI defines Certificate Policies to which CAs conform.

5.7.3.4 Trust representation

Trust between different CAs is represented by a Bridge Certificate issued by the Federal Bridge CA under authorization of the FPKI PMA.

5.7.3.5 Identified enablers

Based on a comparison between the forerunning of the current ETSI standards for qualified certificates ETSI TS 101 456 [i.38] in ETSI TR 102 458 [i.66], most of the policy requirements are comparable with those of the ETSI.

The Federal Bridge Policy Management Authority has a similar role as supervisory bodies under the EU.

5.7.3.6 Identified barriers

The FPKI operates through agreements rather than regulatory controls.

It is unclear whether the Federal Bridge policies are directly comparable with the current requirements for qualified certificates.

5.7.3.7 Reference material

Title	URL
US FPKI: – Trust framework – Certificate Policies – FPKI Key recovery policy – Certification Authorities – PIV Interoperable information – Organization Information	https://www.idmanagement.gov/topics/fpki/
Federal PKI Audit requirements	https://www.idmanagement.gov/community/twg/fpki-cas-audit-info/

5.8 Other

5.8.1 Russia

5.8.1.1 Legal context

The Russian Government PKI is regulated by the Ministry of Digital Development, Communications and Mass Media. It is a hierarchical PKI architecture with a state root CA; accredited CAs are subordinate to the state root CA.

Accredited CAs are required to use certified means of cryptographic protection of information implementing Russian cryptographic algorithms (software or hardware used to create and verify digital signatures). There are restrictions on the export of Russian means of cryptographic protection of information, significantly complicating the reliable verification of Russian digital signatures outside of Russia.

5.8.1.2 Supervision and auditing

There is no regular audit of accredited CAs. The Ministry of Digital Development, in the accreditation of a new CA or when renewing the accreditation of existing CA, conducts a documentary check of conformity of the CA to requirements of the legislation. In the case of a complaint being raised by users about the work of an accredited CA, the Ministry of Digital Development, together with the Federal Security Service, may conduct an on-site inspection of the CA.

5.8.1.3 Best practice

It is required by law that the provisions of the Certificate Policy do not contradict operational documentation on means of CAs approved by the Federal Security Service. It is recommended to draw up a Certificate Policy in accordance with IETF RFC 3647 [i.14] (but it is not obligatory).

There is an urgent problem of verification of the powers of the signatories. Variants for organizing such checks are currently being discussed. At the same time, the infrastructure of trust services for verification and validation of digital signatures is being developed. This infrastructure will be primarily used to verify the digital signatures created in the Member States of the Eurasian Economic Union.

5.8.1.4 Trust representation

A hierarchical PKI architecture with a state root CA. Accredited CAs are subordinate to the state root CA. There is also a trust status list. The suspension of CA accreditation is reflected only in the TSL. CRL of the root CA does not contain information about the suspension of the sub-CA accreditation status.

5.8.1.5 Identified enablers

Cross-recognition improvement can be achieved through the formation of trusted infrastructures (including PKI) based on common principles, e.g. on the principles proposed by UN/CEFACT (https://www.unece.org/fileadmin/DAM/cefact/cf_plenary/2018_plenary/ECE_TRADE_C_CEFACT_2018_7E.pdf).

5.8.1.6 Reference material

Title	URL
Federal Law of the Russian Federation No. 63-FZ "On Electronic Signatures"	http://www.consultant.ru/document/cons_doc_LAW_112701/
Code of Administrative Offenses of the Russian Federation 30.12.2001 No. 195-FZ	http://www.consultant.ru/document/cons_doc_LAW_34661/
Order of the Government of the Russian Federation of April 16, 2012 No. 313 "About approval of the Regulations on licensing of activities for development, production, distribution of the cryptography (cryptographic) tools, information systems and telecommunication systems protected with use of the cryptography (cryptographic) tools, to performance of works, rendering services in the field of enciphering of information, to maintenance of the cryptography (cryptographic) tools, information systems and telecommunication systems protected with use of the cryptography (cryptographic) tools (except for case if maintenance of the cryptography (cryptographic) tools, the information systems and telecommunication systems protected with use of the cryptography (cryptographic) tools is performed for ensuring own needs of the legal entity or the individual entrepreneur" (Current state on 18.05.2017)	https://cis-legislation.com/document.fwx?rgn=51365 (http://www.consultant.ru/document/cons_doc_LAW_128739/ https://rg.ru/2012/04/24/shifry-site-dok.html
Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation 14.08.2017 No. 416: "On approval of the procedure for transferring registers of qualified certificates of electronic signature keys and other information issued by accredited certification centres to the federal executive body authorized in the field of using electronic signatures in case of termination of activity of the accredited certification centre"	https://digital.gov.ru/ru/documents/5743/
Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation 22.08.2017 No. 436: "On approval of the procedure for the formation and maintenance of registers of qualified certificates of electronic signature verification keys issued by accredited certification centres, as well as the provision of information from such registries"	https://digital.gov.ru/ru/documents/5755/
Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation 30.11.2015 No. 48: "On approval of administrative regulations for the provision by the Ministry of Telecom and Mass Media of the Russian Federation of the state service for the accreditation of certification centres and the fulfilment by the Ministry of Telecom and Mass Communications of the Russian Federation of the state function of state control and supervision of compliance by accredited certifying centres with the requirements established by the Federal Law "On electronic signature" "and to which these certifying centres would comply whether accredited"	https://rg.ru/2012/11/02/svyaz-dok.html

5.8.2 Switzerland

5.8.2.1 Legal context

The Swiss 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 ISO/IEC 17021-1 [i.22]) is presently accredited by the Swiss Accreditation Service (article 1). Recognition bodies according to article 16 of the Law on the Electronic Signature are responsible for the audit. The recognition body is accredited by the Swiss Accreditation Service (article 1). The recognition body is comparable to the CAB according eIDAS. There is currently only one recognition body.

The recognition body notifies the accreditation body of the providers they recognize. 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 (SB) like in other EU countries.

The Federal Office of Justice and the Federal Office of Communications are responsible for the regulation. They are not involved in the audit scheme. The Federal Office of Communications 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 [i.22] and on the technical requirements defined in the technical and administrative regulations. This process is more or less equivalent to the process described in ETSI EN 319 403 [i.54] under clause 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 ETSI EN 319 403 [i.54] 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 recognized certification provider.

5.8.2.3 Best practice

The recognized 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 ETSI EN 319 411-2 [i.59] and indirectly to ETSI EN 319 411-1 [i.58].

The regulations also refer to other ETSI and CEN standards such as ETSI EN 319 412-parts 1 to 5 [i.60] (certificate profiles), ETSI EN 319 421 [i.61] and ETSI EN 319 422 [i.62] (time-stamping) and CEN EN 419211 parts 1 to 6 [i.34] (secure signature creation device protection profiles).

Additionally, Switzerland plans to implement a machine-readable Trusted List according to ETSI TS 119 612 [i.53] 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 article 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 is the centre of expertise for Switzerland's European policy.

5.8.2.6 Reference material

Title	URL
Law on the Electronic Signature	https://www.admin.ch/opc/fr/classified-compilation/20131913/index.html
Current Swiss Accreditation Service	https://home.kpmg.com/ch/de/home/dienstleistungen/advisory/consulting/information-protection-and-business-resilience.html
List of recognized Certification Service Providers	https://www.sas.admin.ch/sas/fr/home/akkreditiertestellen/akkrstellensuchesas/pki.html
Directorate for European Affairs, the center of expertise for Switzerland's European policy	https://www.eda.admin.ch/dea/en/home.html
SR 943.03 Law on certification services in the area of electronic signature and other applications of digital certificates (Law on the electronic signature)	https://www.admin.ch/opc/fr/classified-compilation/20131913/index.html
SR 943.032 Decree on certification services in the area of electronic signature and other applications of digital certificates (Decree on the electronic signature)	https://www.admin.ch/opc/fr/classified-compilation/20162168/index.html
SR 943.032.1 OFCOMs decree on certification services in the area of electronic signature and other applications of digital certificates	https://www.admin.ch/opc/fr/classified-compilation/20162169/index.html
SR 943.032.1 Technical and administrative regulations concerning certification services in the area of electronic signature and other applications of digital certificates	https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/communication-numerique/signature-electronique.html

6 Analysis of Enablers and Barriers to Mutual Recognition

6.1 Introduction

The following text summarizes the main approaches taken by existing national and international PKI-based trust services as described in clause 5, and then the responses to the questionnaire as well as information gathered through desktop research. This is followed by a consideration of the enablers and barriers that have been identified for each pillar. Annex C provides a description of the EU eIDAS Regulation against which the comparison is made.

6.2 Legal context

6.2.1 General Approaches

From a legal perspective, there exist different approaches to regulating trust services. These can be grouped 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 an "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 recognized 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 1999/93/EC [i.64]) and, nowadays, also legal person electronic seals, time stamps, certified electronic delivery evidences and web authentication certificates (eIDAS Regulation). 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 effect 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 Directive 1999/93/EC [i.64] and the eIDAS Regulation 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 accepting foreign qualified trust services in their territory, even when used in electronic government processes.

The eIDAS Regulation 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 non-EU national laws have formally adopted UNCITRAL's approach on electronic signatures, 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. In many cases, this requires compliance with very specific technical standards imposed by a supervisory body. Also, some national laws have been extended to cover other trust services such as time-stamping and, in some cases, electronic identities, applying the same regulatory approach and are, thus, similar to the eIDAS Regulation.

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 certificates for electronic signatures or electronic seals 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 the regulation approach, 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 on the autonomy of the will of parties, normally organized through associations with different governance models.

In the first case, there is a party with a very strong power of negotiation that allows this party to impose its requirements (e.g. Adobe®, Google®, etc.), based on non-negotiable agreements, to the rest of the parties. This is primarily aimed at website authentication.

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, for users in a business domain (e.g. SAFE-BioPharma®) or for a specific usage, such as Internet trust embedded in applications (e.g. 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 on the corresponding agreements, but always considering any legal limitations on the autonomy of the will of the parties.

6.2.2 Enablers

A first enabler is the existence of legal concepts for non-qualified trust services, as it eases their reuse as foundational bases for comparing different regulations or defining multilateral agreement-based frameworks.

For 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 frameworks or in a particular application of domain supported by agreements.

The eIDAS-aligned ETSI trust services standards provide a framework supporting both qualified and non-qualified approaches around requirements which mostly apply to both. This enables implementations aimed at the EU qualified status to also interoperate at the non-qualified level, facilitating global transactions supported by EU trust services providing website authentication and supporting advanced electronic signatures for businesses e.g. for global transactions.

A second enabler is precisely the concept of qualification, because it is constructed around a set of specific requirements, thus allowing the comparison between institutions in different regulatory and agreement-based approaches and easing recognition. Thus, for example, 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.

Furthermore, in the absence of agreement on the recognition of trust services as qualified under article 14 of the eIDAS Regulation, it can be shown that a non-EU trust service meets the technical requirements of the Regulation for qualified trust services, and has been authorized by an independent body which has technical oversight of the operation of trust service and can react to incidents that occur within the trust service.

If mutual recognition of EU qualified trust services can be achieved with other nations, this will have the advantage to remove a barrier to entering the EU market, and also that parties requiring to trust TSPs in an open market know they can rely on a TSP authorized under a qualified scheme. Currently, with the number of different schemes applied in the open market, a TSP needs to get authorization from every application provider which its customers may be using, and relying parties generally depend on the application provider to make the trust decision on its behalf.

6.2.3 Barriers

Currently, the main barrier to the mutual recognition of qualified trust services is the lack of agreement under article 14 with other non-EU nation or international organizations. Any such agreement, under international law, is likely to require reciprocity. Thus, the lack of legal recognition of non-EU trust service providers as qualified in the EU, impacts the recognition of EU qualified trust service providers as meeting the requirements of non-EU nations. However, given that in many countries the requirements are below those for EU qualified TSPs, EU qualified trust services are being accepted as meeting other national or sector requirements.

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 are considered in all legal systems (e.g. legal persons seals).

6.3 Supervision and auditing

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-authorization) and regular audits throughout the lifecycle of the provided trust services.

In schemes based around agreements, particularly in North America and international groups such as the US FPKI and SAFE-BioPharma®, a similar role to the supervisory authority is taken on by a body called the Policy Management Authority (PMA). This authority sets the certificate policy requirements required to be accepted by the scheme and ensures through audit that the CAs (i.e. TSPs issuing certificates) Certificate Practice Statement meets the requirements of the Certificate Policy.

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, the accreditation requirements may come from three different sources:

- a nationally defined scheme, as for the majority of third countries (e.g. Brazil, India, Japan, Australia, South Korea, etc.);
- an accreditation scheme where national accreditation bodies, signatories of the International Accreditation Forum & ILAC multilateral agreement, are accrediting CABs under a standardized framework. This framework is either ISO/IEC 17065 [i.23] supplemented by ETSI EN 319 403 [i.54], like in Europe as the EA promoted accreditation scheme for eIDAS accredited CABs, or ISO/IEC 17021-1 [i.22] (e.g. Switzerland); or
- an ad hoc commercial scheme, namely the WebTrust certification scheme, requiring the auditors to be WebTrust practitioners licensed by CPA Canada.

ISO/IEC 17065 [i.23] supplemented by the ETSI EN 319 403 [i.54] 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 auditing and assessing TSP. The European cooperation for Accreditation (EA) has promoted the ISO/IEC 17065 [i.23] framework supplemented by ETSI EN 319 403 [i.54] 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 [i.23] framework supplemented by ETSI EN 319 403 [i.54] is widely used for assessing conformance of TSP 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 accreditation and certification framework

WebTrust is an internationally well-known 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 organizational 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 CABs in article 3 (18) as falling out of the scope of Regulation (EU) 765/2008 [i.8] where accreditation of CABs is performed by national accreditation bodies (NABs). However, the confidence in the WebTrust licensed practitioner to conduct audits with the same rigour and qualifications as Regulation (EU) 765/2008 [i.8] accredited CABs, under ISO/IEC 17065 [i.23] supplemented by ETSI EN 319 403 [i.54] 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 centralized 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 Forum 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

Policy management authorities as adopted in US FPKI and many commercial PKI schemes such as CertiPath® and SAFE-BioPharma® have a similar oversight as EU supervisory authorities carrying out a similar role in ensuring a TSP meets the certificate policy requirements through its certificate practices.

The accreditation framework based on ISO/IEC 17065 [i.23] supplemented by ETSI EN 319 403 [i.54] is a framework dedicated to the assessment of TSP 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 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 recognized framework (like ISO/IEC 17065 [i.23] is) will benefit from international recognition under the principle "certified once recognized everywhere".

It is believed that the IAF MLA driven accreditation scheme based on ISO/IEC 17065 **[**i.23**]** (potentially supplemented by ETSI EN 319 403 [i.54]) is a very natural and interesting candidate for any country to base their national TSP certification scheme on. By nature, this framework allows assessing conformance to any set of criteria, be it standards (e.g. ETSI standards on TSPs and the trust services it provides), be it legal provision (e.g. eIDAS requirements on QTSP/QTS), be it industry specifications (e.g. CA/Browser Forum requirements [i.31]), etc.

The EA has promoted the ISO/IEC 17065 [i.23] framework supplemented by ETSI EN 319 403 [i.54] 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 CABs 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.

The WebTrust audit scheme provides a similar degree of assurance as a formally accredited CAB that a TSP is operating in line with best practices. However, this is not recognized as being based on officially accredited auditor as required for the audit of qualified TSPs.

The formal recognition of a certification scheme under the Cybersecurity Act (EU) 2019/881 [i.9] based around ETSI EN 319 403 [i.54] could help minimize variation of approaches to the audit of trust service providers (see below).

6.3.3 Barriers

Currently, there is no formally recognized accreditation scheme under the eIDAS regulation [i.4], as covered by article 20.4.

The lack of globally adopted accreditation scheme for auditors/CABs assessing PKI-based TSPs is still a barrier to the general global mutual recognition of trust services. ETSI have established with the EA a standard for conformity assessment and audit ETSI EN 319 403 [i.54] based on the International Standard for conformity assessment of products and services ISO/IEC 17065 [i.23]. This is the first and only standard which provides for formal accreditation of auditors/CABs as required by eIDAS. The global recognition of ETSI EN 319 403 [i.54] should be promoted particularly through the International Accreditation Forum (IAF).

In the absence of a global accreditation scheme for the audit of TSPs, some flexibility may be necessary in the area of audit schemes, and schemes such as WebTrust might need to be recognized as comparable to an audit scheme based on formally accredited auditors.

There is a particular problem in the EU which is often pointed out by non-EU countries as jeopardizing the mutual recognition of EU QTSP/QTS, in that the legal requirements for the audit is only that the legal requirements are met not that any specific best practices, such as the ETSI standards, are followed. This can lead to diversity in the quality of the results of the assessments. Outside the EU, it is common practice that the audits are based around best practice standards as well as high level, technology neutral, regulations. Greater confidence outside the EU would be achieved if similar requirements for adoption of recognized best practices is adopted.

There is a need for a harmonised set of certification schemes with more specific criteria for acceptability based on ISO/IEC 17065 [i.23], supplemented by ETSI EN 319 403 [i.54] against recognized best practice standards including, but not necessarily limited to, ETSI standards.

6.4 Best Practice

6.4.1 General approaches

All known general-purpose PKI-based trust services are based on the Recommendation ITU-T X.509 [i.65] or the IETF equivalent IETF RFC 5280 [i.17].

The structure (table of content) of most PKI-based trust services are based on trust service policies and practices statements which follow IETF RFC 3647 [i.14].

Some PKI services are based on the earlier ETSI specifications ETSI TS 101 456 [i.38] and ETSI TS 102 042 [i.40]. These are "historical" specifications and were used as the basis for the ETSI EN 319 411-1 [i.58] and ETSI EN 319 411-2 [i.59] Policy Requirements, the latter being aimed to support the eIDAS Regulation (EU) 910/2014 [i.4].

International standards in the area of PKI-based trust services are currently directed at financial services in ISO 21188 [i.28]. However, the emerging standard currently ISO/IEC CD 27099 [i.26], may provide a generic basis for trust services but probably still needs adaption for the particular needs of a community.

6.4.2 Enablers

The use of generally adopted standards, such as Recommendation ITU-T X.509 [i.65] and the definition of a certificate policy IETF RFC 3647 [i.14] 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 ETSI EN 319 411-1 [i.58] and ETSI EN 319 411-2 [i.59], then technical comparison between PKI systems under different regimes should be straight forward. If non-EU PKIs are based on the earlier standards (ETSI TS 101 456 [i.38] or ETSI TS 102 042 [i.40]) 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 Forum Baseline Requirements [i.31] or EV Guidelines [i.32] provides a common set of policy requirements, with EV guidelines being necessary for the qualified level. Where other standards provide generally acceptable practices, such as ISO 21188 [i.28] (or its potential derivative which takes into account general information security practices currently ISO/IEC CD 27099 [i.26]), this may assist in comparison.

The acceptance of ETSI standards by the CA/Browser Forum and many non-EU countries is leading the way towards harmonized best practices.

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 Regulation is still a barrier to the general global mutual recognition of trust services although ETSI standards are already serving this global need.

The current ETSI standard for qualified trust services ETSI EN 319 411-2 [i.59] is aimed specifically at the EU and the eIDAS Regulation. This means that a non-EU country cannot easily claim equivalence of its practices to EU-qualified. For full alignment, TSPs claiming conformance to such a policy will also need to be overseen by an authority equivalent to a supervisory authority, such as a policy management authority, that applies equivalent roles regarding audit and incident reporting, and requires use of secure signature creation device (local or remote) for holding the signing key.

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 ETSI TS 119 612 [i.53] or sometimes in the older version of the specification (ETSI TS 102 231 [i.44]).
- 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.

SAFE-BioPharma® and Adobe® have demonstrated that it is possible to map representations between an ETSI TS 119 612 [i.53] 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 also efficient.

A trusted list-based model may facilitate independence from 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 the technical mutual 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.

It has been shown that other forms of trust representation, such as bridge certificates, can be mapped to an equivalent of the EU trusted lists providing a basis representing trust based on equivalence in the other areas of comparison.

6.5.3 Barriers

Extended specifications for trust list to trust list 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 ETSI TS 119 612 [i.53].

Currently, ETSI EN 319 412-5 [i.60] QcCompliance statement specification is specific to the EU. This should be updated to extend its scope to non-EU countries.

7 Conclusions

7.1 Introduction

The following conclusions are reached through a consideration of the current PKI-based trust service schemes as described in clause 5, followed by the cross-scheme analysis given in clause 6.

7.2 General

a) In order to establish mutual recognition between EU and non-EU PKI based trust services, each of the 4 areas of comparison identified in clause 4.2 needs to be taken into account.

b) During the study, a number of transnational groups helped to provide input to this study: Asia PKI Consortium, Arab African e-Certification Authorities Network, International Mutual Recognition Technical Working Group (with members from EU, Japan and North America). It is recommended that ETSI maintain an ongoing liaison with these groups to exchange information relevant to mutual recognition.

7.3 Legal Context

c) Further harmonising at the international level, e.g. UNCITRAL work, with common principles addressing trust services in national laws and cross-border recognition will significantly assist in mutual recognition.

d) The EU should take the opportunity of 2020 revision of the eIDAS Regulation to further facilitate the international mutual recognition.

e) The EU approach to mutual recognition needs to recognize the significant role agreement-based trust service schemes play in the global market as well as the existence of schemes based on a national regulatory framework.

f) Non-qualified trust services supporting advanced electronic signatures may act as a basis for the recognition of cross-border transactions according to different regulatory framework schemes based on agreements.

g) The advantages of EU qualified trust services should be promoted. In particular that the use of qualified trust services provides a single legal framework which avoids the variety of application specific trust schemes that need to be provided by each platform provider.

h) The lack of agreement under eIDAS article 14 is a barrier to the mutual recognition of trust services outside the EU to be recognized as qualified trust services inside the EU.

7.4 Supervision and Auditing

i) The ETSI standard for conformity assessment and audit ETSI EN 319 403 [i.54] should be promoted globally, particularly through the International Accreditation Forum (IAF), as the only existing practical scheme for assessment of trust service providers based on international standards for conformity assessment.

j) In the absence of a global accreditation scheme for the audit of trust service providers, some flexibility may be necessary in the area of audit schemes, and schemes such as WebTrust might need to be recognized comparable to an audit scheme based on formally accredited auditors.

k) The lack of consistency of the best practices used in the audit schemes for qualified trust services in Europe is jeopardizing their mutual recognition.

l) The role of Policy Management Authorities (PMA) in agreement-based PKI schemes in overseeing the operation of trust services should be taken into account when considering mutual recognition, and PMAs should be encouraged to apply, within its domain, the same type of oversight functions as an EU supervisory body.

m) The formal recognition of ETSI EN 319 403 [i.54] through eIDAS article 20.4 [i.4] or a certification scheme under the cyber security regulation [i.9] would significantly assist in clarifying that use of ETSI EN 319 403 [i.54] should be the preferred basis for cross recognition.

7.5 Best Practice

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

o) Non-EU countries looking for mutual recognition should be encouraged to adopt the latest ETSI eIDAS-based standards particularly where they have already adopted earlier ETSI standards based on the Electronic Signatures Directive [i.64].

p) ETSI standards should be extended to provide an interoperable equivalent to the EU Qualified Certificate Policies which may be adopted by non-EU countries and or agreement-based scheme. This should achieve equivalent level of security and functionality as required by the eIDAS Regulation, including oversight by an authority and use of a secure signature creation device.

q) The upcoming international standards currently ISO/IEC CD 27099 [i.26] on PKI policy and practices framework should be influenced to ensure that it is aligned with ETSI standards for trust services.

r) ETSI standards should take into account ISO/IEC 27701 [i.27] on privacy to facilitate international alignment.

7.6 Trust Representation

s) PKI schemes aiming to achieve mutual recognition with the EU should be encouraged to map their trust representation (e.g. using bridge certificates) into an equivalent to EU trusted lists to facilitate mutual recognition with EU implementations based around trusted lists.

t) The ETSI EN 319 412-5 [i.60] QcCompliance statement should be updated to extend its scope to non-EU countries.

Annex A:
Study Questionnaire

ETSI Study on Globalization of European Trust Services

Questionnaire on Globally Relevant PKI and Trust Services

V2.1

Introduction

ETSI has tasked a group of experts 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 related to EU trust services for:
  - policy requirements, defined in ETSI EN 319 4DD series (e.g. ETSI EN 319 411-2 [i.59]) and ETSI EN 319 5DD series (e.g. ETSI EN 319 531 [i.63]);
  - assessment scheme, defined in ETSI EN 319 403 [i.54]; 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 the study team in carrying out this study, it is requested that some basic information is provided about your PKI-based trust schemes with links to any further details that may be available. The study team requests 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): Organization(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 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 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 areas of comparison identified in clause 4.2 and, the comparison process is executed in line with the four steps described in clause 4.3.

   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, finalized and signed.

   b. The corresponding MRA execution plan should be drafted, finalized 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 realization that can be addressed using the four steps method from clause 4.3 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

C.1 Introduction

C.1.1 Overview

The eIDAS Regulation [i.5] 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 frameworks, 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 introduced the notions of Qualified Trust Service (QTS) and Qualified Trust Service Provider (QTSP) with a view to indicate 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 that meet the eIDAS requirements applicable to EU QTSP/QTS, hence de facto limiting article 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 third country TSP with EU QTSP/QTS is required to be recognized in an agreement concluded between the European Union and the third country in question (or an international organization) in accordance with article 218 of the Treaty on the Functioning of the European Union.

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 recognized as legally equivalent to trust services provided by TSPs in the third country or international organization 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 third country TSP counterparts, the mutual international recognition between Qualified Electronic Signatures (QESig) and their third country electronic signatures is made possible by definition in eIDAS in combination with article 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 third 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 third country TSP recognized under an article 14 agreement concluded with the EU for being legally equivalent to a Qualified Certificate for electronic signatures issued by an EU QTSP/QTS, this third country electronic signature will be deemed legally equivalent to an EU Qualified Electronic Signature (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 a Qualified Certificate for electronic signature (or third country equivalent).

The mechanisms, or the absence of mechanisms, for (mutual) recognition of third country signature creation devices as (legally) equivalent to EU QSCD are presented in clauses C.1.5 below.

C.1.4 Mutual recognition of qualified electronic seals

The mutual recognition principle developed in the previous clause is mutatis mutandis applicable for the mutual recognition of the legal equivalence of third country electronic seals to EU Qualified Electronic Seals (QESeals).

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

The mechanisms for the (mutual) recognition of third 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 are required to notify to the European Commission of the names and addresses of those designated certification bodies. The European Commission 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 European Commission 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 third country signature creation device to be recognized as (legally) equivalent to an EU QSCD is to be certified as an EU QSCD, i.e. the third 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 third country certifying devices in accordance with CID (EU) 2016/650 [i.7].

C.2 Legal Context

C.2.1 Nine types of EU QTSP/QTS

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

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

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

3) 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 signatures 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:
  - (Article 5) relating to processing and protection of personal data;
  - (Articles13.2 & 13.3) relating to liability and burden of the proof;
  - (Article 15) relating to accessibility for person with disabilities;
  - (Article 19.1) relating to implementing appropriate technical and organizational measures to manage the risks;
  - (Article 19.2) relating to security and personal data breach notification;
  - (Article 20.1) relating to completion and internal procedures;
  - (Article 23) relating to use of the EU trust mark for QTS; and
  - (Article 24 (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 C.1 below, for the nine types of QTSP/QTS.

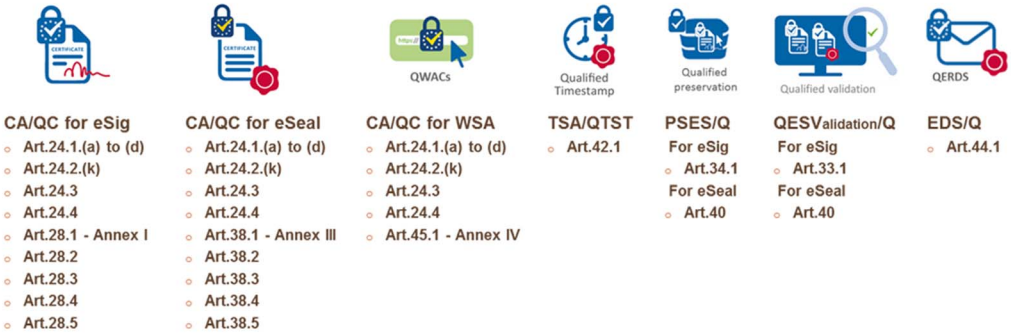

Figure C.1: EU QTSP/QTS specific requirements as laid down in eIDAS [i.4]

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 are 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 is granted a qualified status, it will be subject to a pre-authorization 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 CAB. Before notifying the competent SB of their intention to start providing qualified trust services, the future QTSP/QTS is required to successfully pass an external assessment (audit) to confirm that it fulfils the requirements from eIDAS. That audit is required to be conducted by a CAB specifically accredited to carry out assessments of QTSP/QTS against eIDAS requirements. 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 authorized to provide the corresponding QTS.

Once granted a qualified status, QTSPs and their QTSs have the obligation to pass, and submit to the competent SB 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 are 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

Article 3.18 of eIDAS [i.3] requires CABs to be accredited in accordance with Regulation (EC) No 765/2008 [i.8] 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 EA is the body recognized under Regulation (EC) No 765/2008 [i.8] 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 recognize 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 recognized body, under Regulation (EC) No 765/2008 [i.8], as competent to develop sectoral or specific accreditation schemes. This may be done on request by 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.54] 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 ETSI EN 319 403 [i.54] defined accreditation scheme is such that:

i) it requires the accreditation of the CAB to be based on ISO/IEC 17065 [i.23]; and

ii) it supplements the general requirements provided in ISO/IEC 17065 [i.23] to provide additional dedicated requirements for CABs performing certification of TSP 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 a "framework" for the conformity assessment of TSP against specific 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.

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

No standard may be imposed to a QTSP/QTS as a condition for them to be recognized 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 maximize interoperability. They also may significantly help CAB to design their certification scheme for conducting assessment of QTSP/QTS against the requirements of eIDAS.

However, ETSI have defined a set of standards which are recognized by many of the EU national supervisory authorities as best practices aimed at meeting the requirements of eIDAS and have been adopted as the basis for the national audit schemes.

C.5 Trust representation of EU QTSP/QTS

C.5.1 EU Trust Mark for QTS

A QTSP/QTS may use the EU Trust Mark to publicize that its trust service is 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 European Economic Area relevance)). It, however, provides no assurance that the TSP has been accepted by its national supervisory authority as "qualified". The qualified status of a TSP is required to be verified using the EU national trusted lists (see below).

The use of the Trust Mark is covered by the official journal of the European Union L 128, 23.5.2015, p. 13-15). The Trust Mark shown below in Figure C.2 can only be used by a QTSP to "label" its QTS.

Figure C.2: 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.53], 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 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 Member States have the obligation to include in their national trusted list the information related to the grant of a qualified status to a TSP 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.

On a voluntary basis, EU Member States 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 that provides them.

In order to validate that a trust service is a qualified one under the eIDAS Regulation [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.

The LOTL also plays an important role in authenticating EU Member States trusted lists. Each national trusted list is electronically signed or sealed by its EU Member States 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.53] provides specifications for trusted lists in two contexts, namely the European Union legislative context as set by the eIDAS Regulation [i.5] and the context of countries outside the European Union and the European Economic Area countries, or of international organizations willing to issue trusted lists in accordance with the present document.

The benefits from the adoption of ETSI TS 119 612 [i.53] 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; and
- 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 third country with regards to the mutual recognition of trust services, the specifications for the LOTL, based on ETSI TS 119 612 [i.53], allows for pointing to the trusted list of that third country or to a trusted list representation of the trust representation in use in that third country with respect the recognized equivalent TSP.

Annex D:
Reports of Workshops

D.1 Introduction

Four workshops were held in Dubai, Tokyo, Mexico City and New York aimed at getting an understanding of the approaches taken in different regions of the world.

The following provide key points of these four workshops.

D.2 Dubai

02 May 2019 | Dubai

Event web site

https://www.etsi.org/events/past-events/1560-2019-05-etsi-tra-middle-east-and-africa-workshop-on-globalisation-of-trust-services

Presentations

https://docbox.etsi.org/Workshop/2019/201905_MiddleEast_AfricaWS_GlobalisationofTrustServices

Background

The workshop was organized as part of the ETSI study investigating existing PKI-based trust services schemes that operate in different regions of the world, and their possible mutual recognition and/or global acceptance. In particular, the study aimed to identify further steps which could be taken to facilitate mutual recognition between EU trust services, based on ETSI standards supporting the eIDAS Regulation, and trust services from other schemes.

The first of a series of workshops in 2019, this event aimed to get in a dialogue with the relevant trust scheme operators from the Middle East and Africa.

Attendance

The workshop, hosted by the Telecommunications Regulatory Authority (TRA) of the United Arab Emirates (UAE), was attended by 30+ attendees representing Middle Eastern countries (UAE, Oman, Saudi Arabia, Bahrain, Turkey) and African countries (Algeria, Burkina Faso, Nigeria, Senegal, Tunisia).

Key Points

1) The UAE is very committed to work with the EU at preparing the path towards mutual recognition of corresponding qualified trust services. Close working relationship is to be maintained with UAE including ongoing activities and possible coordination;

2) The AICTO is also keen to work with the EU, with ETSI particularly, and contact should be maintained with their representative at the workshop. AAECA-Net representative to be invited at one of the ETSI ESI meeting (end 2019);

3) Collaboration, cooperation, exchanges of information and technical best practices were identified as key success factors for achieving mutual recognition;

4) There is a need for improving the dissemination and promotion of ETSI standards towards Middle Eastern and African countries; and

5) eIDAS is seen as a mature legal framework for specifying electronic trust services and used as a basis for setting-up or extending existing non-EU national legislative frameworks.

D.3 Tokyo

22-23 May 2019 | Tokyo

Event web site

https://www.etsi.org/events/1580-2019-05-tokyo-workshop-on-globalization-of-trust-services

Presentations

https://docbox.etsi.org/Workshop/2019/201905_Tokyo_GlobalizationofTrustServices

Background

This workshop aimed to get in a dialogue with the relevant trust scheme operators, following the Dubai workshop at the beginning of May 2019.

The workshop followed on from a series of online meetings held by a working group with Japanese experts and experts from North America, on International Mutual Recognition of Trust services (IMRT). At these meetings, a dialogue had already been established on issues relating to mutual recognition.

Attendance

The workshop, hosted by Keio University and JIPDEC, was attended by 120 primarily Japanese participants, although other Asian nations such as India were also represented.

Key Points

1) Japan is very keen to work to work with the EU at building bridges of trust and interoperability. Close working relationship is to be maintained with Japan including ongoing activities of the IMRT-WG and possible coordination of the US workshop.

2) The Asia Pacific Consortium is also keen to work with the EU and contact should be maintained with their representative at the workshop.

3) The presentation on the Asia Pacific Consortium included some very useful information on the activities of each of its members. Their representative requested that this remain confidential until the consortium had agreed to a report on which the presentation is based. As soon as the present document becomes available is planned to use the present document as input to the ETSI's report.

4) Japan is continuing to look at the EU approach to remote signatures based on ETSI and CEN standards. Some explanations of the approach taken were given at informal discussions following the workshop and assistance has been offered with any further questions that may arise with the adaption of these standards to Japanese requirements.

There is a current need to justify the use of other trust services than e-signatures for signing. This includes the need for legal recognition of time-stamping, support for other aspects of trust services including qualified seals, qualified website certificates and the Trust Service Status List:

1) the general Ministry of Economy, Trade & Industry model of cyber security may provide useful context for trust services, going forward and of interest to TC Cyber; and

2) after the 2017 workshop with ETSI members with Japan, which had a similar structure, there has been a persistent and strong motivation to continue on the path of collaboration with Japan. And also, there is significant benefit with ongoing dialogue with the Asia PKI Consortium.

D.4 Mexico City

27 June 2019 | Mexico City

Event web site

https://www.etsi.org/events/1591-2019-06-etsi-logalty-latam-workshop-on-globalisation-of-trust-services

Background

This Workshop was organized as part of the ETSI study that investigates the current trusted services systems operating in different regions of the world (in this case, Mexico and Latin America), and the possible mutual recognition and/or global acceptance.

The objective of the workshop was to present the European framework of standards in trusted services on eIDAS and to relate it to its application in Mexico and other Latin American countries; to share with the regulatory, supervisors, and official bodies of all current trusted services and discuss how to fit the trust models with ETSI experts.

Attendance

The workshop was attended by 122 people, mainly Mexicans, although there were also 14 attendees from other countries through video streaming, such as Guatemala, Colombia and Japan.

The presence of a significant number of personnel of the Supervisory Body of the Certification Services of Mexico was noteworthy. Most of attendees were senior managers of companies from different sectors, such as insurance, banking, consulting and industry.

There were personnel from the Mexican regulator, Economy Secretariat, and the Spanish National Statistics Institute very active in the debate, being 12 % of the attendees, and personnel from the Spanish Embassy.

Key points:

1) All ETSI reports are very valuable for the standardization and normalization in Mexico and the rest of Latin American countries.

2) Mexico uses ETSI standards for TSP accreditation. It is recommended that Mexico keep on following the lines that have already been given, with excellent practices in some cases at a global level.

3) The European framework with eIDAS Regulation together with the ETSI standards leads the future way in which medium and long-term objectives can be established at a national level.

4) It is recommended that the EU standards based ecosystem are taken into consideration in all projects, actions, and regulations related to electronic certification and digital identity services. This is very important since there are thirty million people without internet access.

5) The standards, together with compliance with applicable regulations, make the electronic evidence more robust. This is very relevant, but it is not enough for the evidence to be fully robust. The electronic evidence is very complex; the judges protect users and workers and the interposition is vital, even more with the notarial intervention.

6) In this context, the use of certification services and advanced electronic signature clearly reinforce electronic transactions, especially in a cross-border environment.

7) The standards to identify in the issuance of certificates can be used in sovereign identity models.

D.5 New York

3 September 2019 | New York

Event web site

https://www.etsi.org/events/1621-2019-09-etsi-north-america-workshop-on-globalisation-of-trust-services

Presentations

https://www.etsi.org/events/1621-2019-09-etsi-north-america-workshop-on-globalisation-of-trust-services#pane-2/

Background

This workshop aimed to get in a dialogue with the relevant trust scheme operators from the North America, and was the last of a series of workshops, also including Dubai, Tokyo and Mexico City.

Attendance

The workshop was hosted at the EU Delegation to the United Nations in New York. It was attended by 16 local attendees and eight remote attendees representing CAs, US Government agencies and software platform suppliers. In addition, there were Japanese representatives interested in mutual recognition with the EU and North America.

International Mutual Recognition Technical Working Group (IMRT-WG)

Immediately following the ETSI workshop was a meeting of IMRT-WG (see clause 5.2.6), an informal group of experts from EU, Japan and North America aimed at addressing the technical issues of mutual recognition of trust services. The group is working on a methodology based on the approach taken in this report and discussed setting up pilots for mutual recognition between the EU and SAFE-BioPharma® as well as between the EU and Japan. It was suggested that a version of the current ETSI Qualified Certificate Policy for electronic signatures be defined, which is comparable with all the requirements of eIDAS but not dependent on EU Regulations. This could be adopted by both commercially-based PKI, such as SAFE-BioPharma® and CertiPath® as well as countries looking to achieve cross-recognition with the EU.

Key Points

1) A global trust framework for mutual recognition of PKIs based in North America and Europe was considered important;

2) At discussions the following day at the International Mutual Recognition Technical Working Group meeting it was agreed to work on a trust framework for mutual recognition of PKIs with EU, Japan and interested North America PKI schemes such as SAFE-BioPharma;

3) If a global trust framework is to be achieved PKI schemes there is a need to avoid being "ego-centric" with each scheme requiring other schemes to adopts its approach. Rather, schemes should look towards achieving comparability with other schemes;

4) If global trust framework between EU and North America is to be achieved, this needs to take into account of the North American approach, based on bridge CAs with oversight by a Policy Management Authority, which may be compared with the use of EU Trusted Lists and supervisory authorities; and

5) A change to EU policy was considered necessary to allow trust frameworks located outside of the EU to participate in the EU Trust List infrastructure.

History

Document history		
V1.1.1	January 2020	Publication