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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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".