ETSI TR 119 000 V1.3.1 (2023-05)

Electronic Signatures and Infrastructures (ESI);
The framework for standardization of digital signatures and trust services;
Overview

Reference
RTR/ESI-0019000v131

Keywords
digital signature, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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.

Introduction

The present document describes the general structure for ETSI/CEN digital signature and trust services standardization framework outlining standards applying to these areas and identifying a general structure for identifying these standards.

This framework has been established and will be maintained to address any elements identified as missing in the framework for standardization of signatures and trust services. Unless specifically addressing specific types of legally defined electronic signatures (e.g. as in Regulation 910/2014/EU [i.1]), all documents of the framework intend to cover digital signatures supported by PKI and public key certificates [i.2], and aim to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from EU legislation [i.1].

Digital signatures are described as data appended to, or being a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. Digital signatures are supported themselves by relevant trust services such as trust services issuing certificates. Digital signatures may be considered as a means of implementing electronic signatures and electronic seals as they are defined in the applicable European legislation [i.1]. An important element of the framework is the creation and validation of digital signatures. As business stakeholders even not familiar with signature underlying technology may already have deduced from Regulation 910/2014/EU [i.1], the creation and validation of signatures cannot be achieved in a fully opened environment without relying on one or several third-party trust services, tools or products. This namely covers digital certificate issuers to attest the identities of signers, time-stamping providers to attest trusted time association to a signature or an event, signature creation device issuers, and many other services related to the creation, validation and/or preservation of signatures. Such third parties moreover need to be trusted to some extent for providing their services in accordance with the expected legal or technical specifications. For this, one may rely on specific approval schemes operated by trustworthy organizations.

This framework includes standards for additional trust services identified in Regulation 910/2014/EU [i.1] which can be built on digital signatures and public key technology to provide authentication and integrity such as digitally signed time-stamps, website authentication and registered electronic delivery.

The objectives of this framework for standardization are:

a) To allow business stakeholders to implement and use products and services based on digital signatures more easily. A business-driven approach, with guidance on the use of standards in business terms, underlies the framework. Business driven guidance are provided for maximizing successful implementation of signatures-based products, services and applications by guiding the stakeholders through the definition and parameterization of the different elements or components of signatures and/or signature-based services/applications and guiding them consequently through the selection of the appropriate standards and their implementation.

b) To facilitate mutual recognition and cross-border interoperability of signatures and trust services.

c) To simplify standards, reduce unnecessary options and avoid diverging interpretations of the standards.

d) To target a clear status of European Standard (EN) for standardization deliverables whenever this is applicable.

e) To facilitate a global presentation of the signature and trust services standardization landscape, the availability and access to the standards.

In order to facilitate (cross-border) mutual recognition of solutions, services, and products based on digital signature and trust, this framework also aims to provide a common basis for approval schemes through the definition of standard requirements for the assessment of such solutions, services and products against the standards to ensure conformant solutions at common levels of security.

Regulation 910/2014/EU [i.1] is currently under review and may well result in requirements for further standardization relating to trust services which may be included in future versions of the present document.

1 Scope

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

NOTE: Each title providing the name of a listed standard in the framework for standardization of signatures includes a hyperlink that leads to download facilities for such a standard, including all its versions, both as TS/TR and/or as EN when applicable.

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] Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] Recommendation ITU-T X.509/ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.3] CCMB-2006-09-001: "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model"; Version 3.1, Revision 3, July 2009.

[i.4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.5] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.6] ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.7] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.8] IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".

[i.9] W3C® Recommendation 11 April 2013: "XML Signature Syntax and Processing Version 1.1".

[i.10] ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

[i.11] PKWARE: ".ZIP Application Note".

[i.12] ISO/IEC PRF 21320-1: "Information technology -- Document Container File -- Part 1: Core".

[i.13] IETF RFC 3161 (August 2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol".

[i.14] ETSI TS 101 733 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[i.15] ETSI TS 103 173 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[i.16] ETSI TS 102 778: "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1".

[i.17] ETSI TS 103 172 (V2.2.2): "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[i.18] ETSI TS 101 903 (V1.4.2): "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[i.19] ETSI TS 103 171 (V2.1.1): "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

[i.20] ETSI TS 102 918 (V1.3.1): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.21] ETSI TS 103 174 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

[i.22] SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms.

[i.23] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[i.24] CA/Browser Forum (V1.7): "Guidelines for The Issuance and Management of Extended Validation Certificates".

[i.25] CA/Browser Forum (V1.7): "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates".

[i.26] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance).

[i.27] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[i.28] UPU S52-2/CEN/TS 16326: "Functional specification for postal registered electronic mail".

NOTE: This is version 2 of the UPU S52 specification; date of adoption is 9 April 2013.

[i.29] W3C® Recommendation (2008): "XML-Signature Syntax and Processing (Second Edition)".

[i.30] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.31] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation".

[i.32] ETSI TR 119 300: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for cryptographic suites".

[i.33] ETSI TR 119 400: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for trust service providers supporting digital signatures and related services".

[i.34] ETSI TR 119 500: "Business Driven Guidance for Trust Application Service Providers".

[i.35] ETSI TR 119 600: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for trust service status lists providers".

[i.36] ETSI SR 019 020: "The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments".

[i.37] TR 419 030: "Rationalized structure for electronic signature standardization. Best practices for SMEs" (produced by CEN).

[i.38] TR 419 040: "Rationalized structure for electronic signature standardization - Guidelines for citizens" (produced by CEN).

[i.39] ETSI SR 019 050: "Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures".

[i.40] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.41] ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".

[i.42] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.43] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.44] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.45] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.46] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.47] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.48] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.49] ETSI TS 119 142-3: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)".

[i.50] ETSI TS 119 132-3: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES".

[i.51] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[i.52] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[i.53] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.54] ETSI TS 119 172-2: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies".

[i.55] ETSI TS 119 172-3: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 3: ASN.1 format for signature policies".

[i.56] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

[i.57] ETSI TS 119 182-1: "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

[i.58] ETSI TS 119 192: "Electronic Signatures and Infrastructures (ESI); AdES related Uniform Resource Identifier".

[i.59] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.60] ETSI TS 119 403-2: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates".

[i.61] ETSI TS 119 403-3: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers".

[i.62] ETSI TS 119 495: "Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking".

[i.63] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[i.64] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[i.65] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[i.66] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".

[i.67] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.68] 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.69] 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.70] ETSI SR 019 510: "Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures".

[i.71] ETSI TR 119 530: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Feasibility study: Interoperability profile between ETSI EN 319 532-based REM systems and PReM-based systems".

[i.72] ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".

[i.73] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.74] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.75] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.76] ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services".

[i.77] ETSI TS 119 524-1: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 1: Testing conformance".

[i.78] ETSI TS 119 524-2: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 2: Test suites for interoperability testing of Electronic Registered Delivery Service Providers".

[i.79] ETSI TS 119 534-1: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 1: Testing conformance".

[i.80] ETSI TS 119 534-2: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 2: Test suites for interoperability testing of providers using same format and transport protocols".

[i.81] ETSI TS 119 614-1: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Trusted Lists; Part 1: Specifications for testing conformance of XML representation of Trusted Lists".

[i.82] ETSI TS 119 615: "Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union Member States national trusted lists".

[i.83] TR 419 200: "Business driven guidance for signature creation and other related devices" (produced by CEN).

[i.84] TR 419 210: "Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N 910/2014 (eIDAS)" (produced by CEN).

[i.85] EN 419 211 (parts 1 to 6): "Protection profiles for secure signature creation device" (produced by CEN).

[i.86] TS/EN 419 221 (parts 1 to 6): "Protection profiles for TSP cryptographic modules (produced by CEN).

[i.87] EN 419 231: "Protection profile for trustworthy systems supporting time stamping" (produced by CEN).

[i.88] EN 419 241 (parts 1 and 2): "Security requirements for trustworthy systems supporting server signing" (produced by CEN).

[i.89] EN 419 251 (parts 1 to 3): "Security requirements for device for authentication" (produced by CEN).

[i.90] TS 419 261: "Security requirements for trustworthy systems managing certificated and time-stamps" (produced by CEN).

NOTE: Including managing certificates for electronic signatures.

[i.91] EN 419 212 (parts 1 to 5): "Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services" (produced by CEN).

[i.92] ETSI TR 119 124-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures - Testing Conformance and Interoperability; Part 1: Overview".

[i.93] ETSI TS 119 124-2: "Electronic Signatures and Infrastructures (ESI); CadES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of CadES baseline signatures".

[i.94] ETSI TS 119 124-3: "Electronic Signatures and Infrastructures (ESI); CadES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended CadES signatures".

[i.95] ETSI TS 119 124-4: "Electronic Signatures and Infrastructures (ESI); CadES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of CadES baseline signatures".

[i.96] ETSI TS 119 124-5: "Electronic Signatures and Infrastructures (ESI); CadES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended CadES signatures".

[i.97] ETSI TR 119 134-1: "Electronic Signatures and Infrastructures (ESI); XadES digital signatures - Testing Conformance and Interoperability; Part 1: Overview".

[i.98] ETSI TS 119 134-2: "Electronic Signatures and Infrastructures (ESI); XadES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of XadES baseline signatures".

[i.99] ETSI TS 119 134-3: "Electronic Signatures and Infrastructures (ESI); XadES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of extended XadES signatures".

[i.100] ETSI TS 119 134-4: "Electronic Signatures and Infrastructures (ESI); XadES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of XadES baseline signatures".

[i.101] ETSI TS 119 134-5: "Electronic Signatures and Infrastructures (ESI); XadES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of extended XadES signatures".

[i.102] ETSI TR 119 144-1: "Electronic Signatures and Infrastructures (ESI); PadES digital signatures - Testing Conformance and Interoperability; Part 1: Overview".

[i.103] ETSI TS 119 144-2: "Electronic Signatures and Infrastructures (ESI); PadES digital signatures - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of PadES baseline signatures".

[i.104] ETSI TS 119 144-3: "Electronic Signatures and Infrastructures (ESI); PadES digital signatures - Testing Conformance and Interoperability; Part 3: Test suites for testing interoperability of additional PadES signatures".

[i.105] ETSI TS 119 144-4: "Electronic Signatures and Infrastructures (ESI); PadES digital signatures - Testing Conformance and Interoperability; Part 4: Testing Conformance of PadES baseline signatures".

[i.106] ETSI TS 119 144-5: "Electronic Signatures and Infrastructures (ESI); PadES digital signatures - Testing Conformance and Interoperability; Part 5: Testing Conformance of additional PadES signatures".

[i.107] ETSI TR 119 164-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (AsiC) - Testing Conformance and Interoperability; Part 1: Overview".

[i.108] ETSI TS 119 164-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (AsiC) - Testing Conformance and Interoperability; Part 2: Test suites for testing interoperability of AsiC baseline containers".

[i.109] ETSI TS 119 164-3: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (AsiC) - Testing Compliance and Interoperability; Part 3: Test suites for testing interoperability of AsiC containers other than baseline".

[i.110] ETSI TS 119 164-4: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (AsiC) - Testing Compliance and Interoperability; Part 4: Testing Conformance of AsiC baseline containers".

[i.111] ETSI TS 119 164-5: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (AsiC) - Testing Compliance and Interoperability; Part 5: Testing Conformance of additional AsiC containers".

[i.112] ETSI TR 119 112: "Electronic Signatures and Infrastructures (ESI); Most significant differences between AdES/ASiC ENs and previous TSs".

[i.113] ETSI TS 119 122-3: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES".

[i.114] ETSI TS 119 152-1: "Electronic Signatures and Infrastructures (ESI); CBOR AdES (CB-AdES) digital signatures, Part 1: Building blocks and baseline signatures".

NOTE: This document is under development at the time of the publication of the present document.

[i.115] 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.116] 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.117] ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

[i.118] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

[i.119] ETSI TS 119 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.120] ETSI TS 119 461: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

[i.121] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.122] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

[i.123] ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services".

[i.124] ETSI TR 119 411-4: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2".

[i.125] ETSI TR 119 411-5: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 5: Guidelines for the coexistence of web browser and EU trust controls".

[i.126] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.127] ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".

[i.128] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents".

[i.129] ETSI EN 319 522-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats".

[i.130] ETSI EN 319 522-4 (all sub-parts): "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings".

[i.131] ETSI EN 319 532-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and architecture".

[i.132] ETSI EN 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic contents".

[i.133] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats".

[i.134] ETSI EN 319 532-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles".

[i.135] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.136] ETSI TS 119 322: "Electronic Signatures and Infrastructure (ESI); Schema for machine-readable cryptographic algorithms, and cipher suites catalogues".

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.5] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.5] apply.

4 General framework for standardization related to digital signatures and trust services

4.1 Classification scheme

4.1.1 Functional areas

The framework for standardization of signatures is organized around 6 (functional) areas and 5 types of documentation.

NOTE: Clause 4.1.5 addresses how this classification scheme can be expanded.

The 6 areas of the framework are the following:

1) **Signature creation and validation:** This area focuses on standards related to the creation and validation of digital signatures, covering:

   i) the policy and security requirements for signature creation applications and signature validation applications;

   ii) the expression of rules and procedures to be followed at creation, verification and for long term availability of signatures;

   iii) signature formats and packaging of signatures and signed documents; and

   iv) protection profiles, according to Common Criteria [i.3] for signature creation/verification applications.

2) **Signature creation and other related devices:** This area focuses on standards related to secure signature creation devices as they were defined in Directive 1999/93/EC [i.4], on qualified signature creation devices as defined in Regulation 910/2014/EU [i.1], on signature creation devices used by Trust Service Providers (TSPs) as well as other types of devices supporting signatures and related services such as authentication.

3) **Cryptographic suites:** This area covers standardization aspects related to the use of signature cryptographic suites, i.e. the suite of signature related algorithms including key generation algorithms, signing algorithms with parameters and padding method, verification algorithms, and hash functions.

4) **Trust service providers supporting digital signatures and related services:** This includes TSPs issuing public keys certificates (both EU-qualified and non-qualified) issued to natural and legal persons, including web server certificates, time-stamping services providers, TSPs offering signature validation services, and TSPs offering remote signature creation services (also called signing servers). The current list covers those services supporting digital signature that exist to date; other trust services may be identified at a future date.

5) **Trust application service providers:** This covers TSPs offering value added services applying digital signatures and that rely on the generation/validation of signatures in normal operation. This includes namely registered mail and other e-delivery services, as well as data preservation (long term archiving) services. This list may be extended as further services applying signatures are identified.

6) **Trust service status (list) providers:** This area covers the standardization related to the provision of trust service status lists and trusted lists as defined in the eIDAS Regulation [i.1].

An additional area, area 0 as depicted in figure 1, is gathering the present document as well as studies and other introductory deliverables related to the framework.

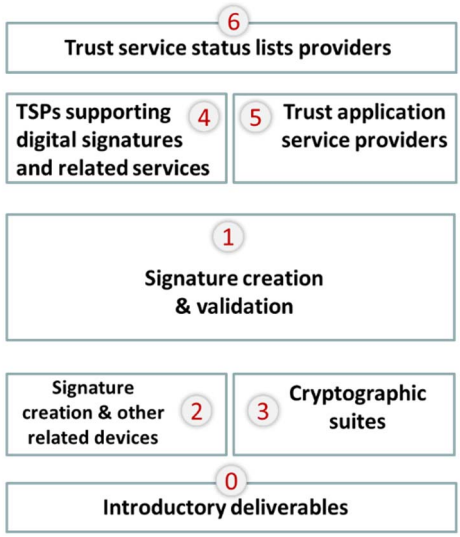

Figure 1: Overview of the structure of the framework for standardization of signatures

4.1.2 Document types

The documents required for standardization of each of the above functional areas have been organized around the following six types of documents:

1) **Guidance:** This type of documents does not include any normative requirements but provides business driven guidance on addressing the signature (functional) area, on the selection of applicable standards and their options for a particular business implementation context and associated business requirements, on the implementation of a standard (or a series of standards), on the assessment of a business implementation against a standard (or a series of standards), etc.

2) **Policy & security requirements:** This type of document specifies policy and security requirements for services and systems, including protection profiles. This brings together use of other technical standards and the security, physical, procedural and personnel requirements for systems implementing those technical standards.

3) **Technical specifications:** This type of document specifies technical requirements on systems. This includes but is not restricted to technical architectures (describing standardized elements for a system and their interrelationships), formats, protocols, algorithms, APIs, profiles of specific standards, etc.

4) **Conformity assessment:** This type of document addresses requirements for assessing the conformity of a system claiming conformity to a specific set of technical specifications, policy or security requirements (including protection profiles when applicable). This primarily includes conformity assessment rules (e.g. common criteria evaluation of products or assessment of systems and services).

5) **Testing conformance & interoperability:** This type of document addresses requirements and specifications for setting-up interoperability tests or testing systems or for setting-up tests or testing systems that will provide automated checks of compliance of products, services or systems with specific set(s) of technical specifications.

6) **Sector Specific Requirements:** This type of document profiles the use of other standards in this framework for a particular business sector (e.g. banking and financial services).

Figure 2: Illustration of document types in the framework for standardization of signatures

4.1.3 Structure with sub-areas

This general area-based structure of the framework can be broken down into further sub-areas. This identifies the primary sub-areas within the six functional areas as described in clause 4.2.1. For each area, a common set of 5 types of document addresses aspects applicable to all sub-areas, and per sub-area additional documents address aspects specific to each sub-area.

In the "signature creation and validation" area 1, sub-areas have been identified focusing on the specific standardized AdES formats, based on digital signatures, respectively CadES, XadES, JadES and PadES, as well as the AsiC format for signature containers that bind together a number of signed data objects with AdES applied to them or time-stamp tokens computed on them. AdES in mobile or distributed environments are also considered as part of this area.

In area 2, "signature creation and other related devices", documents are grouped in sub-areas with regards to the type of signature creation device, namely Secure/Qualified Signature Creation Devices (SSCDs/QSCDs), devices for TSPs, for TSAs, for signing servers and authentication devices.

Area 4, TSPs supporting digital signatures and related services, has been divided in sub-areas focusing on the different types of such TSPs, namely trust service providers issuing certificates, time-stamping service providers, signature generation service providers, signature validation or signature augmentation service providers, and identity proofing service providers.

Area 5, trust application service providers, contains three sub-areas, one dedicated to the provisioning of electronic registered delivery services, one to Registered Electronic Mail (REM) services, and another one dedicated to data preservation service providers.

4.1.4 Numbering scheme

A **consistent numbering** for such documentation was adopted to identify a single and consistent series of digital signatures standards and with the aim to keep the same number for each document whatever maturity level it reaches through its lifetime. The numbering scheme being used is defined as follows:

DD L19 xxx-z

Where:

DD indicates the deliverable type in the standardization process (SR, TS, TR and EN)

L when set to 4: identifies a CEN deliverable

when set to 0, 1, 2, or 3: identifies an ETSI deliverable and the type of deliverable in the standardization process

019 for ETSI published Special Report (SR)

119 for ETSI published Technical Specification (TS) and Technical Report (TR)

219 for ETSI published Standard (ES) and ETSI Guide (EG)

319 for ETSI published European Standard (EN)

419 for CEN published Technical Report (TR), Technical Specification (TS) or European Standard (EN)

19 indicates the series of standardization documents related to digital signatures and trust services

ETSI/CEN may further extend this numbering system in line with their own practices.

Xxx indicates the serial number (000 to 999):

where **X**xx identifies the area (0-generic to a number of areas; 1-Signature creation and validation; 2-Signature creation and other related devices; 3-Cryptographic suites; 4-Trust service providers supporting digital signatures; 5-Trust application service providers; 6-Trust service status lists providers);

where x**X**x identifies a sub-area within the identified area, or 0 for documents generic to a given area;

where xx**X** identifies the type of document (0-Guidance; 1-Policy and security requirements; 2-Technical specifications; 3-Conformity assessment; 4-Testing compliance and interoperability); 5-Sector specific requirements).

-z identifies multi-parts as some documents may be multi-part documents.

Additional numbering for identifying parts and versions will be in line with ETSI or CEN conventions depending on which organization publishes the document.

4.1.5 Guidance documents addressing the framework functional areas

As a pre-requisite to the use of the respective guidance document, each stakeholder needs to describe and model in as details as possible the business domain, business process or business application in which the implementation of digital signature standards is looked for. This aims to ensure that all the details relating to crucial aspects of the business environment are captured and that the implementation of digital signatures does not miss any of them. This pre-requisite step also includes a risk assessment, as a way of getting the needed information from where identifying policy and security requirements, so that once they are satisfied, stakeholders have a better assurance that the risks are identified and mitigated. The guidance documents, however do not aim at providing a complete guide on these topics but make readers aware of their relevance.

Elaborating the different sources of policy and security requirements, into resulting controls' objectives and controls to be implemented in the system and by addressing and analysing the essential business scoping parameters in the light of the context where the business process in which digital signature standards have to be implemented, the respective guidance documents will drive the stakeholders to the selection of standards and their options.

As illustrated in figure 3, a complete digital signatures solution may need to address requirements in several or most of the areas. However, depending on the expectations of the stakeholders, the following documents can be used as starting points:

a) when a stakeholder is facing the need or wish to implement digital signatures in a business process, it can start with ETSI TR 119 100 [i.31] on "Guidance on the use of standards for signature creation and validation";

b) when a stakeholder is facing the need or wish to use or design signature creation devices, it can consider the business scoping parameters and guided selection of standards as described in TR 419 200 [i.83] on "Guidance on the use of standards for signature creation and other related devices" taking into account business requirements that come from other areas as shown in figure 3 below;

c) when a stakeholder is facing the need or wish to be advised on cryptographic suites, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 300 [i.32] on "Guidance on the use of standards for cryptographic suites" taking into account business requirements that come from other areas as shown in figure 3 below;

d) when a stakeholder is facing the need or wish to provide TSP services either with the aim to issue certificates or to provide time-stamping services or to provide signature generation or validation services, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 400 [i.33] on "Guidance on the use of standards for trust service providers supporting digital signatures and related services" taking into account business requirements that come from other areas as shown in figure 3 below;

e) when a stakeholder is facing the need or wish to provide trust application service provider services either with the aim to provide electronic registered delivery services/registered electronic mail or to provide long term preservation services, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 500 [i.34] on "Business driven guidance for trust application service providers" taking into account business requirements that come from other areas as shown in figure 3 below;

f) when a stakeholder is facing the need or wish to publish approval status information on digital signature related trust services, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 600 [i.35] on "Guidance on the use of standards for trust service status lists providers" taking into account business requirements that come from other areas as shown in figure 3 below.

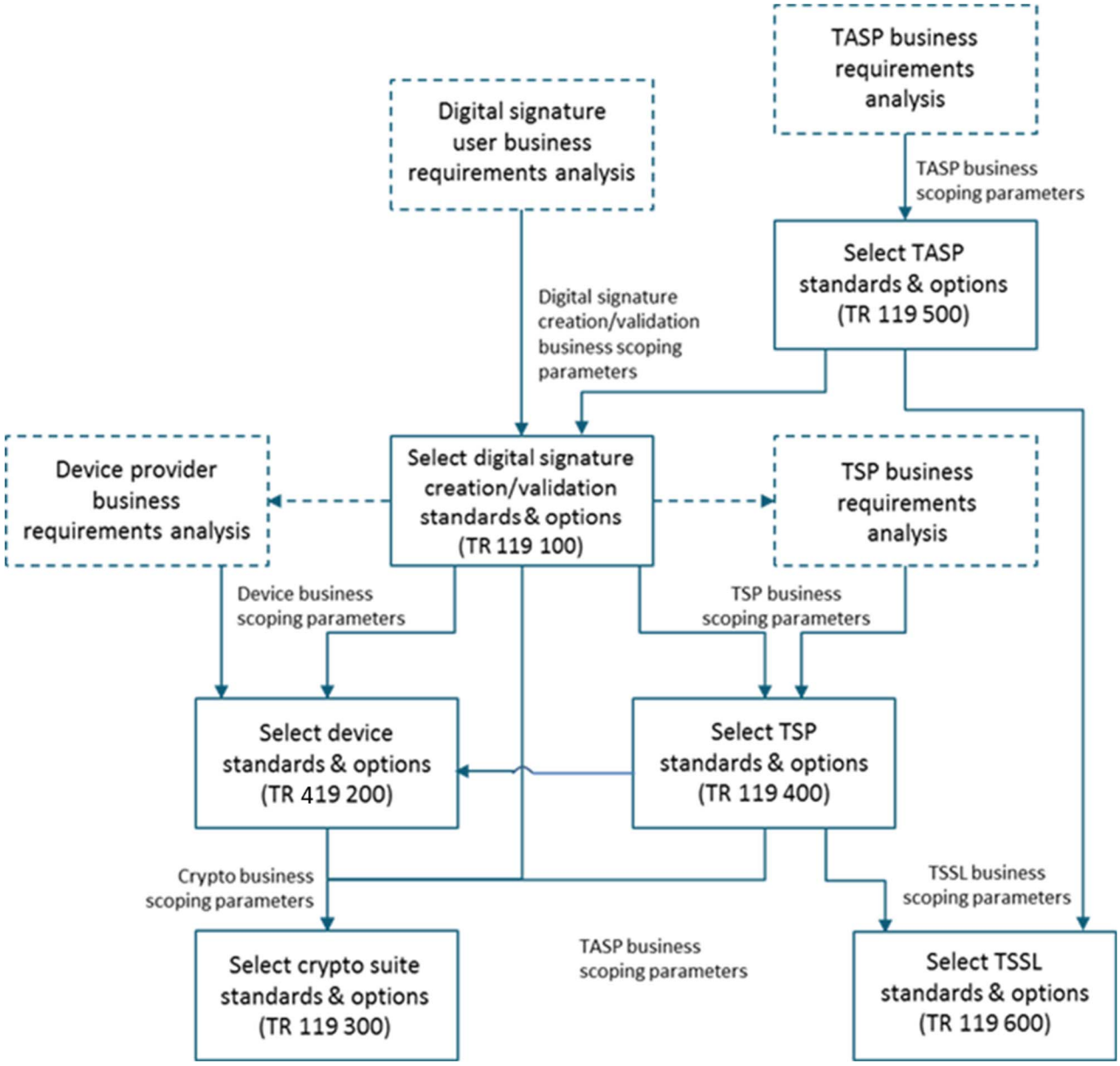

Figure 3: Dependencies of the business scoping parameters among the functional areas

4.2 The framework by area

4.2.0 Foreword

The present clause identifies per area the different standards that are part of this area and provides for each of them a short description of its content and structure. The following tables summarize the list of standards per area and indicate for each standard which standard or document it replaces when applicable and whether it is published or its planned publication date.

4.2.1 Introductory documents

The generic documents for digital signatures standardization are as summarized in table 1.

Table 1: Introductory documents of the framework for signature standardization

Introductory documents of the framework for signature standardisation						
				Sub-areas		
					Guidance	
TR	1	19	0	0	0	The framework for standardisation of signatures: overview
SR	0	19	0	2	0	The framework for standardisation of signatures: Standards for AdES digital signatures in mobile environments
TR	4	19	0	3	0	The framework for standardisation of signatures: Best practices for SMEs
TR	4	19	0	4	0	The framework for standardisation of signatures: Guidelines for citizens
SR	0	19	0	5	0	Rationalised framework of standards for electronic registered delivery applying electronic signatures
					Policies	
TR	1	19	0	0	1	The framework for standardisation of signatures: Definitions and abbreviations

Guidance

ETSI TR 119 000 [i.31] - The framework for standardization of signatures: overview

The present document describes the general structure for digital signature standardization outlining existing and potential standards for such signatures. This framework identifies six areas of standardization with a list of existing and potential future standards in each area. It also provides the basis for business guidance provided in the other areas and reference the business guidance for signature creation and validation (ETSI TR 119 100 [i.31]) as the recommended starting point for the analysis of requirements in particular for those target audiences being stakeholders wishing to introduce and implement digital signatures in a business electronic process.

ETSI SR 019 020 [i.36] - The framework for standardization of signatures: Standards for AdES digital signatures in mobile environments

This document provides details on the framework of standards (including potential architectures and relevant scenarios) required for the creation and validation of AdES digital signatures in the mobile environment.

TR 419 030 [i.37] - Rationalized structure for electronic signature standardization. Best practices for SMEs

This document provides best practices in the usage of digital signatures within the context of SMEs. It would answer to questions in relation with the use and benefits (ROI) of digital signatures to SMEs ecosystems.

TR 419 040 [i.38] - The framework for standardization of signatures: Guidelines for citizens

This document provides best practices in the usage of digital signatures within the context of citizens/consumers. It would answer to questions in relation with the use and benefits (ROI) of digital signatures to consumer's ecosystems.

ETSI SR 019 050 [i.39] - Rationalized framework of standards for electronic registered delivery applying electronic signatures

This document defines electronic delivery (e-delivery) services and investigate applicable requirements from those existing in the market (ETSI, CEN, private standards and pilots' outcome) proposing rationalised and well-organized requirements for electronic delivery applying digital signatures and its possible relation to registered electronic mail.

ETSI TR 119 001 [i.5] - The framework for standardization of signatures: Definitions and abbreviations

This document lists all definitions & abbreviations used in documents of the framework for standardization of signatures and serve as reference. Documents from the framework include definitions/abbreviations by reference to ETSI TR 119 001 [i.5] and/or by copying definitions from ETSI TR 119 001 [i.5].

4.2.2 Signature creation & validation

The standardization documents for signature creation and validation are summarized in table 2 with further details provided below.

Table 2: Standards for signature creation and validation

Signature creation and validation						
				Sub-areas		
					Guidance	
TR	1	19	1	0	0	Business driven guidance for implementing digital signature creation and validation
					Policy & Security Requirements	
TS	1	19	1	0	1	Security requirements for signature creation applications and signature validation applications
					Technical Specifications	
EN	3	19	1	0	2	Procedures for creation and validation of AdES digital signatures - Part 1: Creation and validation
TS	1	19	1	0	2	Procedures for creation and validation of AdES digital signatures - Part 2: Validation report
EN	3	19	1	2	2	CAdES digital signatures - Part 1: Building blocks and CAdES baseline signatures - Part 2: Extended CAdES signatures
TS	1	19	1	2	2	CAdES digital signatures - Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES
EN	3	19	1	3	2	XAdES digital signatures - Part 1: Building blocks and XAdES baseline signatures - Part 2: Extended XAdES signatures
TS	1	19	1	3	2	XAdES digital signatures - Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES
EN	3	19	1	4	2	PAdES digital signatures - Part 1: Building blocks and PAdES baseline signatures - Part 2: Additional PAdES signatures profiles
TS	1	19	1	4	2	PAdES digital signatures - Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)
TS	1	19	1	5	2	CBOR AdES digital signatures - Part1: Building blocks and CB-ADES baseline signatures
EN	3	19	1	6	2	Associated Signature Containers (ASiC) - Part 1: Building blocks and ASiC baseline containers - Part 2: Additional ASiC containers
TS	1	19	1	7	2	Signature policies - Part 1: Building blocks and table of contents for human readable policy documents - Part 2: XML format for signature policies - Part 3: ASN.1 format for signature policies - Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists
TS	1	19	1	8	2	JAdES digital signatures - Part1: Building blocks and JAdES baseline signatures
TS	1	19	1	9	2	AdES related Uniform Resource Identifier
					Conformity Assessment	
					Testing Conformance & Interoperability	
TS	1	19	1	2	4	CAdES Testing conformance & interoperability
TS	1	19	1	3	4	XAdES Testing conformance & interoperability
TS	1	19	1	4	4	PAdES Testing conformance & interoperability
TS	1	19	1	6	4	ASiC Testing conformance & interoperability

Guidance

ETSI TR 119 100 [i.31] - Guidance on the use of standards for signature creation and validation

This document provides business guidance for the implementation of digital signature standards from the viewpoint of signature creation and validation. This includes guidance on selection between the different signature formats. It proposes a business-driven process for implementing generation and validation of digital signatures in electronic business. Starting from their business model, stakeholders are guided for properly specifying all the relevant business scoping parameters regarding the creation and the validation of digital signatures for the specific addressed application/business processes. Finally, stakeholders are guided for making the best choice among the wide offer of standards from the framework for standardization of signatures in order to ensure the best implementation of digital signatures within the addressed application/business processes.

The process proposed by this guidance is defined in a way that ensures to stakeholders a proper and consistent treatment of all the business scoping parameters, explicitly taking into account:

a) parameters directly dependant on the specific application or business process;

b) parameters derived from the regulatory/legal framework where the business is conducted;

c) parameters inherent to the different types of signing entities; as well as

d) other aspects that do not fall within the above three listed categories but are important to be addressed when implementing digital signatures.

The purported audience of this document is rather wide and includes different readers' profiles, such as enterprise/business process architects or managers, business process standardization bodies, application architects, application developers, and signature policy issuers.

Policy and security requirements

ETSI TS 119 101 [i.117] - Policy and security requirements for applications for signature creation and signature validation

This document [i.5] provides security requirements for applications creating and/or validating digital signatures. This includes procedural aspects that are not directly machine processable, as well as aspects which can be defined in a machine processable way (see part 1 [i.53], part 2 [i.54], part 3 [i.55] and part 4 [i.56] of ETSI TS 119 172). This includes requirements for the secure operation of signature creation and validation applications such as might be provided by an information security management system.

This document includes a standardized table of contents for a human readable document stating the signature application practices applied by signature creation applications and/or signature validation applications in a considered business e-process environment.

NOTE: This takes into account the standards for information security management systems in ISO/IEC 27000 [i.6] family and templates for practice statements as in IETF RFC 3647 [i.7].

Technical Specifications

ETSI EN 319 102-1 [i.40]/ETSI TS 119 102-2 [i.41] - Procedures for creation and validation of AdES digital signatures

- Part 1 (EN [i.40]): **Creation and validation:** This document specifies procedures for:

  - the creation of AdES digital signatures as specified in CAdES (see ETSI EN 319 122 parts 1 [i.42] and 2 [i.43]), XAdES (see ETSI EN 319 132 parts 1 [i.47] and 2 [i.48]), PAdES (see ETSI EN 319 142-1 [i.45] and ETSI EN 319 142-2 [i.46]) respectively; and

  - establishing whether an AdES digital signature is technically valid;

  within a given policy context, and whenever the AdES digital signature is based on public key cryptography and supported by public key certificates.

This document specifies support for validation of XAdES, CAdES, PAdES, AdES in Mobile environments and ASiC (Associated Signature Containers) signatures taking into account use of trusted lists (see ETSI TS 119 612 **[**i.44**]**).

- Part 2 (TS [i.41]): **Validation report:** This document specifies a general structure and an XML format for reporting the validation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.42], ETSI EN 319 132-1 [i.47], ETSI EN 319 142-1 [i.45] respectively), in alignment with the requirements specified in ETSI EN 319 102-1 [i.40].

ETSI TR 119 112 [i.112] - Most significant differences between AdES/ASiC ENs and previous TSs

This document summarizes:

a) The most relevant differences between the CAdES digital signatures specified in ETSI EN 319 122-1 [i.42] and ETSI EN 319 122-2 [i.43], and the CAdES signatures specified in ETSI TS 101 733 (V2.2.1) [i.14] and ETSI TS 103 173 (V2.2.1) [i.15].

b) The most relevant differences between the PAdES digital signatures specified in ETSI EN 319 142-1 [i.45] and ETSI EN 319 142-2 [i.46], and the PAdES signatures specified in the latest versions of the different parts ETSI TS 102 778 ([i.16]) and ETSI TS 103 172 (V2.2.2) [i.17].

c) The most relevant differences between the XAdES digital signatures specified in ETSI EN 319 132-1 [i.47] and ETSI EN 319 132-2 [i.48], and the XAdES signatures specified in ETSI TS 101 903 (V1.4.2) [i.18] and ETSI TS 103 171 (V2.1.1) [i.19].

d) The most relevant differences between the ASiC containers specified in ETSI EN 319 162-1 [i.51] and ETSI EN 319 162-2 [i.52] and the ASiC containers specified in ETSI TS 102 918 (V1.3.1) [i.20] and ETSI TS 103 174 (V2.2.1) [i.21].

ETSI EN 319 122 parts 1 [i.42] and 2 [i.43]/ETSI TS 119 122 part 3 [i.113] - CAdES digital signatures

This multi-part document contains all the specifications related to CAdES digital signatures built on top of CMS signatures [i.8] by incorporation of signed and unsigned attributes. It includes specifications for baseline and for extended CAdES digital signatures:

- Part 1 (EN) [i.42]: **Building blocks and CAdES baseline signatures:** This document specifies the ASN.1 definitions for the signed and unsigned attributes that are added to CMS signatures to become CAdES signatures and their usage when incorporating them in CAdES signatures building from CMS signatures. This document specifies formats for CAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of digital signatures on electronic documents. Four levels of CAdES baseline signatures are defined addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Each level requires the presence of certain CAdES attributes, suitably profiled for reducing the optionality as much as possible.

- Part 2 (EN) [i.43]: **Extended CAdES signatures**: This document specifies a number of CAdES signature levels addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Those CAdES extended signatures offer a higher degree of optionality than the CAdES baseline signatures specified in ETSI EN 319 122-1 [i.42].

- Part 3 (TS) [i.113]: **Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES**: ERS allows to cover different data objects with a single time-stamp, and subsequently augment the lifetime of the evidence record by adding validation data to the previous time-stamp and adding new time-stamps. The document aims to provide clear indications how to bind an ERS to a CAdES signature which is covered by the ERS.

NOTE 1: The baseline profile takes into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the European Services Directive [i.4].

NOTE 2: When no specific use case would have requirements not satisfied by the baseline profile, no other specific profile will be added. Should it be otherwise, new profiles would be built on the baseline profile, unless the actual requirements would avoid it.

ETSI EN 319 132 parts 1 [i.47] and 2 [i.48]/ETSI TS 119 132 [i.50] - XAdES digital signatures

This multi-part document contains all the specifications related to AdES built on top of XML signatures [i.9] by incorporation of signed and unsigned properties. It includes specifications for baseline signatures and for extended XAdES digital signatures:

- Part 1 (EN) [i.47]: **Building blocks and XAdES baseline signatures:** This document specifies the XML Schema definitions for the signed and unsigned qualifying properties that are incorporated into XML signatures to become XAdES signatures and the mechanisms to incorporate them into XAdES signatures. This document specifies formats for XAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of digital signatures on electronic documents. Four levels of XAdES baseline signatures are defined addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Each level requires the presence of certain XAdES qualifying properties, suitably profiled for reducing the optionality as much as possible.

- Part 2 (EN) [i.48]: **Extended XAdES signatures:** This document specifies a number of XAdES signature levels addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Those CAdES extended signatures offer a higher degree of optionality than the XAdES baseline signatures specified in ETSI EN 319 132-1 [i.47].

NOTE 1: The baseline profile takes into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the European Services Directive [i.4].

NOTE 2: When no specific use case would have requirements not satisfied by the baseline profile, no other specific profile will be added. Should it be otherwise, new profiles would be built on the baseline profile, unless the actual requirements would avoid it.

- Part 3 (TS) [i.50]: **Incorporation of Evidence Record Syntax (ERS) mechanisms in XAdES:** This document specifies the semantics and the syntax for a new unsigned XAdES qualifying property able to contain evidence records. It specifies the rules that govern the incorporation of evidence records within a XAdES signature or a legacy XAdES signature and specifies a new level for XAdES signatures, incorporating one or more than one of the aforementioned qualifying properties. The signatures specified in this document are not baseline XAdES signatures.

ETSI EN 319 142 parts 1 [i.45] and 2 [i.46]/ETSI TS 119 142 [i.49] - PAdES digital signatures

This multi-part document contains all the specifications related to digital signatures embedded within PDF documents. It includes PAdES baseline signature specifications and additional profiles, and in particular:

- Part 1 (EN) [i.45]: **Building blocks and PAdES baseline signatures:** This document specifies PAdES digital signatures building on PDF signatures specified in ISO 32000-1 [i.10] with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES as specified in ETSI EN 319 122-1 [i.42], by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures) in a number of use cases.

  It specifies formats for PAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of digital signatures used in electronic documents.

  Four levels of PAdES baseline signatures are defined addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Each level requires the presence of certain PAdES attributes, suitably profiled for reducing the optionality as much as possible.

- Part 2 (EN) [i.46]: **Additional PAdES signatures profiles:** This document defines multiple profiles for PAdES digital signatures which are digital signatures embedded within a PDF file.

This document contains a profile for the use of PDF signatures, as described in ISO 32000-1 [i.10] and based on CMS digital signatures [i.8], that enables greater interoperability for PDF signatures by providing additional restrictions beyond those of ISO 32000-1 [i.10]. This first profile is not related to ETSI EN 319 142-1 [i.45].

It also contains a second set of profiles that extend the scope of the profile in ETSI EN 319 142-1 [i.45], while keeping some features that enhance interoperability of PAdES signatures. Those profiles define three levels of PAdES extended signatures addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. These PAdES extended signatures offer a higher degree of optionality than the PAdES baseline signatures specified in ETSI EN 319 142-1 [i.45].

A third profile is defined for usage of an arbitrary XML document signed with XAdES signatures that is embedded within a PDF file.

- Part 3 (TS) [i.49]: **PAdES Document Time-stamp digital signatures (PAdES-DTS):** This document specifies a type of PDF digital signatures, as specified in ISO 32000-1 [i.10], based on time-stamps. It specifies a format for PAdES digital signatures using a Document Time-stamp (as defined in ETSI EN 319 142-1[i.45]) as a digital signature intended to specifically prove the integrity and existence of a PDF document, rather than proving any form of authentication or proof of origin. This format does not meet the requirements of advanced electronic signature and advanced electronic seal as defined in Regulation (EU) No 910/2014 [i.1], as it is not capable of identifying the signer.

NOTE 1: The baseline profile takes into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the EU Services Directive [i.4].

NOTE 2: When no specific use case would have requirements not satisfied by the baseline profile, no other specific profile will be added. Should it be otherwise, new profiles would be built on the baseline profile, unless the actual requirements would avoid it.

ETSI TS 119 152 [i.114] - CBOR AdES digital signatures

- Part 1: **Building blocks and CB-ADES baseline signatures:** This document specifies CBOR signatures baseline profiles offering similar features as the ones offered by JAdES in their corresponding baseline profiles.

NOTE: This document is under development at the time of the publication of the present document.

ETSI EN 319 162 parts 1 [i.51] and 2 [i.52] - Associated Signature Containers (ASiC)

This multi-part document contains all the specifications related to the so-called Associated Signature Containers. That is containers that bind together into one single digital container based on ZIP [i.11], [i.12] either detached digital signatures or time-assertions, with a number of data objects (e.g. documents, XML structured data, spreadsheet, multimedia content) to which they apply. It includes specifications for ASiC baseline containers and for additional containers, and in particular:

- Part 1 [i.51]: **Building blocks and ASiC baseline containers:** This document specifies the format for a single container binding together a number of signed objects (e.g. documents, XML structured data, spreadsheet, multimedia content) with either AdES or time-stamps. This uses package formats based on ZIP and supports the following signature and time-stamp token formats: CAdES signature(s) as specified in ETSI EN 319 122 parts 1 [i.42] and 2 [i.43], XAdES detached signature(s) as specified in ETSI EN 319 132 parts 1 [i.47] and 2 [i.48] and IETF RFC 3161 [i.13] time-stamp tokens.

- Part 2 [i.52]: **Additional ASiC containers:** Specific communities or use cases may have additional requirements that are not addressed by the baseline containers defined in part 1 that can be built using the building blocks defined there or additional ones. The document references such specific additional use of ASiC and aims to be used for containers that collects together electronic documents including those supported by OCF, ODF and UCF describing how these container formats can be used to associate digital signatures with any data objects in the container.

NOTE 1: The baseline containers take into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the European Services Directive [i.4].

NOTE 2: When no specific use case would have requirements not satisfied by the baseline containers, no specific profile will be added. Should it be otherwise, new profiles would be built on the baseline containers, unless the actual requirements would avoid it.

ETSI TS 119 172 parts 1 [i.53], 2 [i.54], 3 [i.55] and 4 [i.56] - Signature policies

This document addresses signature policies usable in the management of digital signatures within extended business models. This is a multi-part document whose internal structure is shown below:

- Part 1 [i.53]: **Building blocks and table of contents for human readable signature policy documents:** This document defines the building blocks of signature policy and specifies a table of contents for human readable signature policy documents.
- Part 2 [i.54]: **XML format for signature policies:** This document specifies an XML format for those parts of the signature policy that may be structured and are worth to be automatically processed by both signing and validating applications.
- Part 3 [i.55]: **ASN.1 format for signature policies:** This document specifies an ASN.1 format for those parts of the signature policy that may be structured and are worth to be automatically processed by both signing and validating applications.
- Part 4 [i.56]: **Signature validation policy for European qualified electronic signatures/seals using trusted lists:** This document will specify a signature validation policy using trusted lists that may be used for European qualified electronic signatures/seals and advanced electronic signatures/seals supported by qualified certificates in Europe.

ETSI TS 119 182 part 1 [i.57] - JAdES digital signatures

- Part 1 [i.57]: **Building blocks and JAdES baseline signatures:** This document specifies JAdES signatures baseline profiles offering similar features as the ones offered by CAdES/XAdES in their corresponding baseline profiles.

ETSI TS 119 192 [i.58] - AdES related Uniform Resource Identifier

This document describes the root Uniform Resource Identifier (URI) http://uri.etsi.org/ades and sub branches that allow to define URI applicable for more than one AdES signature formats and/or the ASiC signature containers. It will also describe how to define URIs to reference a specific version and/or specific attribute/property of an AdES format.

Testing Conformance & Interoperability

ETSI TR 119 124-1 [i.92]/ETSI TS 119 124 parts 2 [i.93], 3 [i.94], 4 [i.95] and 5 [i.96] - CAdES digital signatures - Testing Conformance and Interoperability

This document defines test suites for testing interoperability and conformance of CAdES signatures. This is a multi-part document made of five parts. Part 1, produced as a technical report (TR) [i.92], provides an overview of the set of test suites for testing interoperability and conformance of CAdES signatures. The set of Technical Specifications consist of four documents. The test suites for testing interoperability of CAdES baseline signatures (Part 2 [i.93]) and the specifications required for building software tools for testing technical conformance of CAdES baseline signatures (Part 4 [i.95]) are defined against ETSI EN 319 122-1 [i.42]. The test suites for testing interoperability of extended CAdES signatures (Part 3 [i.94]) and the specifications required for building software tools for testing technical conformance of extended CAdES signatures (Part 5 [i.96]) are defined against ETSI EN 319 122-2 [i.43].

ETSI TR 119 134-1 [i.97]/ETSI TS 119 134 parts 2 [i.98], 3 [i.99], 4 [i.100] and 5 [i.101] - XAdES digital signatures - Testing Conformance and Interoperability

This document defines test suites for testing interoperability and conformance of XAdES signatures. This is a multi-part document made of five parts. Part 1 [i.97], produced as a Technical Report (TR), provides an overview of the set of test suites for testing interoperability and conformance of XAdES signatures. The set of Technical Specifications consist of four documents. The test suites for testing interoperability of XAdES baseline signatures (Part 2 [i.98]) and the specifications required for building software tools for testing technical conformance of XAdES baseline signatures (Part 4 [i.100]) are defined against ETSI EN 319 132-1 [i.47]. The test suites for testing interoperability of extended XAdES signatures (Part 3 [i.99]) and the specifications required for building software tools for testing technical conformance of extended XAdES signatures (Part 5 [i.101]) are defined against ETSI EN 319 132-2 [i.48].

ETSI TR 119 144-1 [i.102]/ETSI TS 119 144 parts 2 [i.103], 3 [i.104], 4 [i.105] and 5 [i.106] - PAdES digital signatures - Testing Conformance and Interoperability

This document defines test suites for testing interoperability and conformance of PAdES signatures. This is a multi-part document made of five parts. Part 1 [i.102], produced as a technical report (TR), provides an overview of the set of test suites for testing interoperability and conformance of PAdES signatures. The set of Technical Specifications consist of four documents. The test suites for testing interoperability of PAdES baseline signatures (Part 2 [i.103]) and the specifications required for building software tools for testing technical conformance of PAdES baseline signatures (Part 4 [i.105]) are defined against ETSI EN 319 142-1 [i.45]. The test suites for testing interoperability of additional PAdES signatures (Part 3 [i.104]) and the specifications required for building software tools for testing technical conformance of additional PAdES signatures (Part 5 [i.106]) are defined against ETSI EN 319 142-2 [i.46].

ETSI TR 119 164-1 [i.107]/ETSI TS 119 164 parts 2 [i.108], 3 [i.109], 4 [i.110] and 5 [i.111] - Associated Signature Containers (ASiC) - Testing Conformance and Interoperability

This document defines test suites for testing interoperability and conformance of ASiC containers. This is a multi-part document made of five parts. Part 1 [i.107], produced as a Technical Report (TR), provides an overview of the set of test suites for testing interoperability and conformance of PAdES signatures. The set of Technical Specifications consist of four documents. The test suites for testing interoperability of ASiC baseline containers (Part 2 [i.108]) and the specification required for building software tools for testing technical conformity of ASiC baseline containers (Part 4 [i.110]) are defined against ETSI EN 319 162-1 [i.51]. The test suites for testing interoperability of additional ASiC containers (Part 3 [i.109]) and the specification required for building software tools for testing technical conformity of additional ASiC containers (Part 5 [i.111]) are defined against ETSI EN 319 162-1 [i.51] and ETSI EN 319 162-2 [i.52].

4.2.3 Signature creation and other related devices

The standardization documents for signature creation and other related devices are summarized in table 3 with further details provided below.

Table 3: Standards for signature creation and other related devices

				Sub-areas		
					Guidance	
TR	4	19	2	0	0	Business driven guidance for signature creation and other related devices
					Policy & Security Requirements	
EN	4	19	2	1	0	Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS)
EN	4	19	2	1	1	Protection profiles for secure signature creation device - Part 1: Overview - Part 2: Device with key generation - Part 3: Device with key import - Part 4: Extension for device with key generation and trusted communication with certificate generation application - Part 5: Extension for device with key generation and trusted communication with signature creation application - Part 6: Extension for device with key import and trusted communication with signature creation application
TS/ EN	4	19	2	2	1	Protection Profiles for TSP cryptographic modules - Part 1 (TS): Overview - Part 2 (TS): Cryptographic Module for CSP signing operations with backup – Protection Profile (CMCSOB-PP) - Part 3 (TS): Cryptographic module for CSP key generation services – Protection Profile (CMCKG-PP) - Part 4 (TS): Cryptographic module for CSP signing operations without backup – Protection Profile (CMCSOPP) - Part 5 (EN): Cryptographic module for trust services - Part 6 (TS): Conditions for use of EN 419221-5 as a qualified electronic signature or seal creation device
EN	4	19	2	3	1	Protection profile for trustworthy systems supporting time stamping
EN	4	19	2	4	1	Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements - Part 2: Protection profile for QSCD for Server Signing
EN	4	19	2	5	1	Security requirements for device for authentication - Part 1: Protection profile for core functionality - Part 2: Protection profile for extension for trusted channel to certificate generation application - Part 3: Additional functionality for security targets
EN	4	19	2	6	1	Security requirements for trustworthy systems managing certificates for electronic signatures
					Technical Specifications	
EN	4	19	2	1	2	Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction - Part 2: Basic services - Part 3: Device authentication - Part 4: Privacy specific protocols - Part 5: Trusted eServices
					Conformity Assessment	
						Protection profiles are assessed through the Common Criteria - ISO/IEC 15408
					Testing Conformance & Interoperability	
-		-	-	-	-	*no requirement identified*

Guidance

TR 419 200 [i.83] - Business driven guidance for signature creation and other related devices

This document provides guidance for the selection of standards for signature creation and other related devices for given business requirements.

TR 419 210 [i.84] - Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS)

This document considers requirements of the eIDAS regulation (Regulation 910/2014 [i.1]) and use cases for qualified electronic seal creation devices and how these requirements may be met by standards. These use cases will take into account differences in articles 26 and 36 of eIDAS on (sole) control of the signatory and seal creator on its signature/seal creation data, whilst also recognizing the commonalities.

Policy & Security Requirements

Policy and Security Requirements for Signature Creation Devices

No requirement has been identified for this type of document as requirements for the use of signature creation devices is addressed as part of the security requirements of the signing environment in ETSI TS 119 101 [i.117].

EN 419 211 [i.85] - Protection profiles for secure signature creation device

This document specifies the security requirements for a SSCD that is the target of evaluation. It follows the rules and formats of the Common Criteria v3 [i.3].

This is a multi-part document [i.85] covering the following topics:

- Part 1: **Overview:** An introduction to the SSCD protection profiles.
- Part 2: **Device with key generation:** This document specifies a protection profile for an SSCD that performs its core operations including the generation of signature keys in the device. This profile can be extended through extensions specified in other parts.

NOTE 1: This part has been superseded by part 5.

- Part 3: **Device with key import:** This document specifies a protection profile for an SSCD that performs its core operations including import of the signature key generated in a trusted manner outside the device.

NOTE 2: This part has been superseded by part 5.

- Part 4: **Extension for device with key generation and trusted communication with certificate generation application:** This document specifies an extension protection profile for an SSCD with key generation that support establishing a trusted channel with a certificate-generating application. This profile can be extended through extensions specified in other parts.

NOTE 3: This part has been superseded by part 5.

- Part 5: **Extension for device with key generation and trusted communication with signature creation application:** This document specifies an extension protection profile for an SSCD with key generation that additionally supports establishing a trusted channel with a signature-creation application.
- Part 6: **Extension for device with key import and trusted communication with signature creation application:** This document specifies an extension protection profile for an SSCD with key import that additionally supports establishing a trusted channel with a signature-creation application.

A companion document for EN 419 211 [i.85] will be produced to match the terminology between Directive 1999/93/EC [i.4] and Regulation 910/2014/EU [i.1], since EN 419 211 [i.85] has been delivered before the publication of that Regulation.

TS/EN 419 221 [i.86] - Protection profiles for TSP cryptographic modules

This multi-part document [i.86] specifies protection profiles for cryptographic devices used by trust service providers. It covers the following topics:

- Part 1 (TS): **Overview:** This part provides an overview of the protection profiles specified in other parts of EN 419 221.
- Part 2 (TS): **Cryptographic module for CSP signing operations with backup - Protection Profile (CMCSOB-PP):** This part specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93/EC [i.4]) for signing operations, with key backup, at a high level of security. Target applications include root certification authorities (certification authorities who issue certificates to other CAs and who are at the top of a CA hierarchy) and other certification service providers where there is a high risk of direct physical attacks against the module.
- Part 3 (TS): **Cryptographic module for CSP key generation services - Protection Profile (CMCKG-PP):** This part specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93/EC [i.4]) for generating signing keys for use by other parties, at a high level of security. Target applications include root certification authorities and other certification service providers where there is a high risk of direct physical attacks against the module.
- Part 4 (TS): **Cryptographic module for CSP signing operations without backup - Protection Profile (CMCSOPP):** This part specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93/EC [i.4]) for signing operations, without key backup, at a high level of security. Target applications include root certification authorities (certification authorities which issue certificates to other CAs and is at the top of a CA hierarchy) and other certification service providers where there is a high risk of direct physical attacks against the module.
- Part 5 (EN): **Cryptographic module for trust services:** This part specifies a protection profile for cryptographic modules used by trust service providers for providing trust services (e.g. signing operations and authentication services) at a moderate level of security. This protection profile includes support for protected backup of keys. The target of this part is:

  a) provision of cryptographic support for TSP signing operations including applications such as certification authorities who issue qualified and non-qualified certificates to end users, level 1 signing services as identified in EN 419 241 parts 1 and 2 [i.88], data "sealing" by or on behalf of a legal entity, time-stamping services and validation services; and

  b) provision of both symmetric and asymmetric cryptographic support for TSP authentication services, for example for authenticating users of signing services as specified in EN 419 241[i.88].

  This profile assumes that the cryptographic module is in a physically secured environment and that there is a low risk of untrusted personnel having direct physical access to the device.
- Part 6 (TS): Conditions for use of EN 419 221-5 [i.86] as a qualified electronic signature or seal creation device: This part specifies conditions for use of an EN 419 221-5 [i.86] certified device in the case the signatory or seal creator has direct local control of the cryptographic module with the aim of being recognised as a qualified seal and/or signature creation device as defined in Regulation EU 910/2014 [i.1]. This document is aimed at use by entities other than trust service providers. Trust service providers can use EN 419 221-5 [i.86] directly without the need to take into account specific conditions as specified in this document.

While parts 2, 3 and 4 are Directive 1999/93/EC [i.4] oriented, but eIDAS Regulation [i.1] compliant, part 5 is focused on cryptographic modules used by TSP to provide signing operations (remote or server signing) and authentication services.

EN 419 231 [i.87] - Protection profile for trustworthy systems supporting time stamping

This document defines protection profiles for a time-stamping trustworthy system that consists of at least a time-stamping unit (namely a set of hardware including an internal clock and software creating time-stamp tokens) and of administration and auditing facilities used to provide time-stamping services.

EN 419 241 [i.88] - Security requirements for trustworthy systems supporting server signing

This document is a multi-part document including general security requirements and protection profiles for trustworthy systems supporting server signing:

- Part 1: **General system security requirements**.
- Part 2: **Protection Profile for QSCD for Server Signing**.

The document is intended for use by developers and evaluators of a server signing application and of its components.

EN 419 251 [i.89] - Security requirements for device for authentication

This multi-part document defines protection profiles for conformity of an authentication hardware device (such as, for example, a smart card or USB token) from the perspective of a security evaluation.

This multi-part document covers the following aspects:

- Part 1: **Protection profile for core functionality**.
- Part 2: **Protection profile for extension for trusted channel to certificate generation application**.
- Part 3: **Additional functionality for security targets**: that can be added to part 1 or part 2 in order to define a new PP with enhanced features.

NOTE: This document may be superseded by standards for EU Digital Identity Wallet under the revision to EU Regulation 910/2014 [i.1].

TS 419 261 [i.90] - Security requirements for trustworthy systems (incl. managing certificates for electronic signatures)

This document establishes security requirements for trustworthy systems and technical components that can be used by a TSP in order to issue EU qualified and non-qualified certificates.

Technical specifications

EN 419 212 [i.91] - Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services

This document describes an application interface and behaviour of the SSCD in the context of Identification, Authentication and Signature (IAS) services.

This multi-part document covers the following topics:

- Part 1: **Introduction:** This part introduces the different parts of the series and gives the main notions and common definitions.
- Part 2: **Basic services:** This part describes the specifications for signature (and seal) generation, including user verification, password-based authentication protocols, establishment of a secure channel and key generation. A specific annex deals with seal, and another one with remote signature.
- Part 3: **Device authentication:** This part describes device authentication protocols, including data structures, Card-Verifiable (CV) certificates and key management.
- Part 4: **Privacy specific protocols:** This document describes privacy specific protocols.
- Part 5: **Trusted eServices:** This document describes additional trusted e-services in the context of signature including Client/Server authentication, role authentication, symmetric key transmission between a remote server and a SE, signature cryptographic verification.

Conformity Assessment

Protection profiles are assessed through the Common Criteria for Information Technology Security Evaluation ISO/IEC 15408 [i.30].

Technical Conformance & Interoperability Testing

No requirements identified so far for such documents.

4.2.4 Cryptographic suites

The standardization documents for cryptographic suites are summarized in table 4 with further details provided below.

Table 4: Standards for cryptographic suites

						Cryptographic suites
						Sub-areas
						Guidance
TR	1	19	3	0	0	Business guidance on cryptographic suites
						Technical Specifications
TS	1	19	3	1	2	Cryptographic suites
TS	1	19	3	2	2	Schema for machine-readable cryptographic algorithms, and cipher suites catalogues
						Testing Conformance & Interoperability
-		-	-	-	-	*no requirement identified*

Guidance

ETSI TR 119 300 [i.32] - Business guidance on cryptographic suites

This document provides business driven guidance on the use of standards for cryptographic suites, and in particular for digital signature creation algorithms.

It explains the concept of security parameters that helps to choose a proper cryptographic suite for digital signature creation. It also gives an overview how to analyse the business needs and how to select a system that satisfies these needs.

The purported audience of this document is mainly the application designers and implementers. It provides recommendations to trust service providers and manufacturers of security devices.

Technical Specifications

ETSI TS 119 312 [i.135] - Cryptographic Suites

This document lists cryptographic suites recommended for the creation and validation of digital signatures and electronic time stamps and related certificates. It builds on the agreed cryptographic mechanisms from SOG-IS [i.22]. It can be used also for electronic registered delivery services in the future.

The document focuses on interoperability issues and does not duplicate security considerations given by other standardization bodies, security agencies or supervisory authorities of the Member States. It instead provides guidance on the selection of concrete cryptographic suites that use agreed mechanisms. The use of SOG-IS agreed mechanisms is meant to help ensure a high level of security in the recommended cryptographic suites, while the focus on specific suites of mechanisms is meant to increase interoperability and simplify design choices. There is no normative requirement on selection among the alternatives for cryptographic suites given here but for all of them normative requirements apply to ensure security and interoperability.

It also provides guidance on hash functions, (digital) signature schemes and (digital) signature suites to be used with the data structures used in the context of digital signatures and seals.

ETSI TS 119 322 [i.136] - Schema for machine-readable cryptographic algorithms, and cipher suites catalogues

This document will define a generic schema for a machine-readable cryptographic algorithm and cipher suite catalogues to reflect requirements posed by existing human-readable algorithm (and cipher suites) catalogues, increase interoperability, and support backwards compatibility for long-term preservation systems.

Conformity Assessment

No requirements identified so far for such documents.

Technical Conformance & Interoperability Testing

No requirements identified so far for such documents.

4.2.5 TSPs supporting digital signatures and related services

The standardization documents for TSPs supporting digital signatures and related services are summarized in table 5 with further details provided below.

Table 5: Standards for TSPs supporting digital signatures and related services

TSPs supporting digital signatures and related services						
				Sub-areas		
					Guidance	
TR	1	19	4	0	0	Business driven guidance for TSPs supporting digital signatures
					Policy & Security Requirements	
EN	3	19	4	0	1	General policy requirements for trust service providers
EN	3	19	4	1	1	Policy and security requirements for trust service providers issuing certificates - Part 1: General requirements - Part 2: Requirements for TSP issuing EU qualified certificates
TR	1	19	4	1	1	Policy & security requirements for trust service providers issuing certificates - Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2 - Part 5: Guidelines for the coexistence of web browser and EU trust controls
EN	3	19	4	2	1	Policy & security requirements for trust service providers issuing time-stamps
EN	3	19	4	3	1	Policy and security requirements for trust service providers providing AdES digital signature generation services
EN	3	19	4	4	1	Policy and security requirements for trust service providers providing AdES digital signature validation services
TS	1	19	4	6	1	Policy and security requirements for trust service components providing identity proofing of trust service subjects
					Technical Specifications	
EN	3	19	4	1	2	Certificate profiles - Part 1: Overview and common data structures - Part 2: Certificate profile for certificates issued to natural persons - Part 3: Certificate profile for certificates issued to legal persons - Part 4: Certifcate profile for web site certificates issued to organisations - Part 5: QCStatements
EN	3	19	4	2	2	Time-stamping protocol and time-stamp profiles
EN	3	19	4	3	2	Protocol profiles for trust service providers providing AdES digital signature generation services
EN	3	19	4	4	2	Protocol profiles for trust service providers providing AdES digital signature validation services
					Conformity Assessment	
EN	3	19	4	0	3	Trust Service Provider Conformity Assessment - Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers
TS	1	19	4	0	3	Trust Service Provider Conformity Assessment - Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificate - Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers
					Testing Conformance & Interoperability	
-	-	-	-	-	-	*no requirement identified for such a document*
					Sector Specific requirements	
TS	1	19	4	9	5	Certificate Profiles and TSP Policy Requirements for Open Banking

Guidance

ETSI TR 119 400 [i.33] - Guidance on the use of standards for trust service providers supporting digital signatures and related services

This document provides guidance on the selection of standards and options for the trust service provider supporting digital signatures and related services (area 4) as identified in clause 4.1.1. It describes the business scoping parameters relevant to this area (see clause 5 of ETSI TR 119 400 [i.33]) and how the relevant standards and options for this area can be identified given the business scoping parameters (see clause 6 of ETSI TR 119 400 [i.33]).

Policy & Security Requirements

ETSI EN 319 401 [i.73] - General policy requirements for trust service providers

This document specifies policy requirements for TSPs that are independent of the type of TSP whether certificate issuer (qualified or otherwise), timestamp issuer, signature verifier, e-delivery provider or other form of trust service provider. It defines policy requirements on the operation and management practices of TSPs.

ETSI EN 319 411 parts 1 [i.68] and 2 [i.69]/TS/TR 119 411 parts 4 [i.124] and 5 [i.125] - Policy and security requirements for trust service providers issuing certificates

This multi-part document specifies policy and security requirements for TSPs issuing certificates. It references ETSI EN 319 401 [i.73] for generic requirements.

This is a multi-part document including the following topics:

- Part 1 (EN) [i.68]: **General requirements:** This EN part specifies generally applicable policy and security requirements for TSPs issuing public key certificates, including trusted web site certificates. The policy and security requirements are defined in terms of requirements for the issuance, maintenance and life-cycle management of certificates. These policy and security requirements support a number of reference certificate policies (LCP, NCP, NCP+, EVCP, OVCP, DVCP, IVCP).

- Part 2 (EN) [i.69]: **Requirements for trust service providers issuing EU qualified certificates:** This EN part specifies policy and security requirements for the issuance, maintenance and life-cycle management of EU qualified certificates as defined in Regulation 910/2014/EU [i.1]. These policy and security requirements support reference certificate policies for the issuance, maintenance and life-cycle management of EU qualified certificates issued to natural persons (QCP-n, QCP-n-qscd), including natural persons associated with a legal person, to legal persons (QCP-l, QCP-l-qscd) and to web sites (QCP-w), respectively.

- Part 3: Not used.

- Part 4 (TR) [i.124]: **Checklist supporting audit of TSP against ETSI EN 319 411-1 [i.68] or ETSI EN 319 411-2 [i.69]:** This Technical Report provides a check-list for self-assessment or independent conformity assessment of TSPs issuing certificates according to ETSI EN 319 411-1 [i.68] and/or issuing EU qualified certificates according to ETSI EN 319 411-2 [i.69]. It also aims to facilitate the preparatory activities the trust service provider undertakes.

- Part 5 (TR) [i.125]: **Guidelines for the coexistence of web browser and EU trust controls:** This technical report provides guidance on how a single TLS certificate can support both Browser Vendor controls and EU trust controls for website authentication, commonly referred to as "server authentication".

ETSI EN 319 421 [i.126] - Policy and security requirements for trust service providers issuing time-stamps

This document specifies policy and security requirements relating to the operation and management practices of TSPs issuing time-stamps and references ETSI EN 319 401 [i.73] for generic requirements. Those policy requirements are applicable to TSPs issuing time-stamps. Such time-stamps can be used in support of digital signatures or for any application requiring to prove that a datum existed before a particular time. The document can be used by independent bodies as the basis for confirming that a TSP can be trusted for issuing time-stamps.

An informative annex provides check lists that can be used by the TSP to prepare an assessment of its practices against the document and/or by the assessor when conducting the assessment for confirming that a TSP meets those requirements.

ETSI TS 119 431 parts 1 [i.115] and 2 [i.116] - Policy and security requirements for trust service providers [providing remote signatures]

This multi-part document specifies policy and security requirements for TSPs providing remote signature It references ETSI EN 319 401 [i.73] for generic requirements.

This is a multi-part document including the following topics:

- Part 1 **[**i.115]: **TSP service components operating a remote QSCD/SCDev:** This part specifies policy and security requirements for TSP service components operating a digital signature creation device, including a QSCD (Qualified Signature/Seal Creation Device) as defined in Regulation (EU) No 910/2014 [i.1] to create a digital signature value on behalf of a remote signer. These requirements are based on the general policy requirements specified in ETSI EN 319 401 [i.73] and take into account related requirements for certificate issuance in ETSI EN 319 411-1 [i.68]. The requirements of this document are aligned with the requirements specified in EN 419 241-1 [i.88].

- Part 2 **[**i.116]: **TSP service components supporting AdES digital signature creation:** This part specifies policy and security requirements for TSP service components creating AdES digital signatures. The TSP service component relies either on remote server signing or on a signature creation device in the user's environment to create digital signature. These requirements are based on the general policy requirements specified in ETSI EN 319 401 [i.73] and consider related requirements from ETSI TS 119 101 [i.117].

ETSI TS 119 441 [i.118] - Policy requirements for TSP providing signature validation services

This document, based on the general policy requirements specified in ETSI EN 319 401 [i.73], specifies policy and security requirements for signature validation services operated by a TSP. It is aimed at trust services supporting the validation of digital signatures in accordance with ETSI TS 119 102-1 [i.119]. It takes into account the relevant requirements for signature validation application specified in ETSI TS 119 101 [i.117] as they relate to TSPs. It is aimed at supporting the validation of digital signatures in European and other regulatory frameworks.

The user's interface is outside the scope of the main TSP service. However, the document provides in annexed recommendations for the user's interfaces (for inputting the request and to visualize the validation report).

The TSP has connections with external (trust) services that can be contacted for provisioning validation information, or to relay the validation request. The document does not put requirements on the trust service policies applied by such external services.

The document identifies specific controls needed to address specific risks associated with validation services.

An informative annex provides a checklist for self-assessment or independent conformity assessment of TSPs offering signature validation services according to ETSI TS 119 102-1 [i.119] and ETSI TS 119 101 [i.117] where applicable. It also aims to facilitate the preparatory activities the trust service provider undertakes.

ETSI TS 119 461 [i.120] - Policy and security requirements for trust service components providing identity proofing of trust service subjects

This document, based on the general policy requirements specified in ETSI EN 319 401 [i.73], will specify policy and security requirements for a trust service component providing identity proofing of trust service subjects. It can be used for conformity assessment of a trust service provider which includes this service component as part of its service or can be used for conformity assessment of a specialised provider of identity proofing supporting other trust service providers.

Technical Specifications

ETSI EN 319 412 - Certificate profiles

This document provides specifications for specific profiles for use by TSPs issuing certificates including EU qualified and other forms of certificates. It provides certificate profiles and a set of specific statement extensions which aim to facilitate interoperability of (EU qualified) certificates issued to natural person, legal person or to organization as website certificate, for the purposes of (EU qualified) electronic signatures, (EU qualified) electronic seals, peer entity authentication, data authentication, as well as data confidentiality.

This is a multi-part document including the following topics:

- Part 1 [i.63]: **Overview and common data structures**.

- Part 2 [i.64]: **Certificate profile for certificates issued to natural persons**.
- Part 3 [i.65]: **Certificate profile for certificates issued to legal persons**.
- Part 4 [i.66]: **Certificate profile for web site certificates**.
- Part 5 [i.67]: **QCStatements**.

ETSI EN 319 422 [i.121] - Time-stamping protocol and time-stamp profiles

This document defines a profile for the time-stamping protocol and the time-stamp token defined in IETF RFC 3161 [i.13] including optional ESSCertIDv2 update in IETF RFC 5816 [i.23]. It defines what a time-stamping client supports and what a time-stamping server supports. Time-stamp validation is out of scope and is defined in ETSI EN 319 102-1 [i.40].

ETSI TS 119 432 [i.122] - Protocols for remote digital signature creation

This document specifies protocols and interfaces applicable when the process of creating AdES digital signatures (as defined by ETSI TS 119 102-1 [i.119]) and/or digital signature values, as result of Data To Be Signed Representations signatures, is carried out by a distributed solution comprised of two or more systems/services/components. It is limited to remote server signing, i.e. the signing key is held in a remote shared service.

The document specifies two bindings, each one in a different syntax (XML and JSON), for each of the protocols mentioned above.

The authorized signer's use of its key for signing requires users to provide multiple proofs of their claimed identity before being granted access to the needed set of resources. The way in which the user identity verification process is carried out by the service provider or any suggestion concerning the usage of multi-factor authentication mechanisms is out of the scope of this document.

ETSI TS 119 442 [i.123] - Protocol profiles for trust service providers providing AdES digital signature validation services

This document specifies the semantics of several protocols, namely:

a) a protocol for requesting to a remote server (and for receiving the corresponding response) the validation of AdES digital signatures compliant with the following ETSI deliverables: ETSI EN 319 122 parts 1 [i.42] and 2 [i.43] ETSI EN 319 132 parts 1 [i.47] and 2 [i.48], ETSI EN 319 142-1 [i.45] and ETSI EN 319 142-2 [i.46], ETSI TS 101 733 [i.14], ETSI TS 102 778 [i.16], ETSI TS 101 903 [i.18], ETSI TS 103 171 [i.19], ETSI TS 103 172 [i.17] and ETSI TS 103 173 [i.15];

b) a protocol for requesting the augmentation of AdES digital signatures compliant with the aforementioned ETSI deliverables;

c) a protocol for requesting the validation and augmentation of AdES digital signatures compliant with the aforementioned ETSI deliverables.

Finally, this document specifies two bindings, each one in a different syntax (XML and JSON), for each of the aforementioned protocols.

Conformity Assessment

ETSI EN 319 403-1 [i.59]/ETSI TS 119 403 parts 2 [i.60] and 3 [i.61] - Trust service provider conformity assessment

This is a multi-part document including the following topics:

- Part 1 (EN) [i.59]: **Requirements for conformity assessment bodies assessing Trust Service Providers:** This EN part ETSI EN 319 403-1 [i.59] specifies requirements for the competence, consistent operation and impartiality of conformity assessment bodies assessing and certifying the conformity of Trust Service Providers (TSPs) and the trust services they provide towards defined criteria against which they claim conformance. It also contains requirements for the conformity assessment of trust services component services, which later forms part of a separate conformity assessment of a TSP. Requirements and guidance set out in this document are independent of the class of trust service provided.

- Part 2 (TS) [i.60]: **Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates:** This TS part specifies supplementary requirements to those defined in ETSI EN 319 403-1 [i.59] in order to provide additional dedicated requirements for CABs performing audits based on ETSI EN 319 411-1 [i.68]and those from CA/Browser Forum, [i.24] and [i.25]. In particular, the document defines the requirements for audit attestations, including their content.

- Part 3 (TS) [i.61]: **Additional requirements for conformity assessment bodies assessing EU qualified trust service providers:** This TS part (ETSI TS 119 403-3 [i.61])specifies supplementary requirements to those defined in ETSI EN 319 403-1 [i.59] in order to provide additional dedicated requirements for CABs performing certification of qualified trust service providers and the qualified trust services they provide towards the requirements of Regulation (EU) No 910/2014 [i.1]. In particular, the document defines requirements for conformity assessment reports, including their content. It aims supporting NABs for the accreditation of CABs in line with Article 3.18 of Regulation (EU) No 910/2014 [i.1].

Testing Conformance & Interoperability

Not applicable so far.

NOTE: At the current date, no requirement for such documents has been identified. It may however be the case that specifications for conformity checker tools could be identified in the future such as conformity checker for generated trust service tokens such as qualified certificates, public key certificates against a specific profile, or time-stamp tokens.

Sector specific Requirements

ETSI TS 119 495 [i.62] - Certificate Profiles and TSP Policy Requirements for open banking

This document specifies profiles of certificates for electronic seals and website authentication, to be used by payment service providers in order to meet the requirements of the PSD2 Regulatory Technical Standards [i.26] or equivalent national regulations for Open Banking. Certificates for electronic seals can be used for providing evidence with legal assumption of authenticity (including identification and authentication of the source) and integrity of a transaction. Certificates for website authentication can be used for identification and authentication of the communicating parties and securing communications. These profiles are based on ETSI EN 319 412-1 [i.63], ETSI EN 319 412-1 [i.63], ETSI EN 319 412-3 [i.65], ETSI EN 319 412-4 [i.66], IETF RFC 3739 [i.27] and ETSI EN 319 412-5 [i.67] (by indirect reference).

It also specifies additional TSP policy requirements for the management (including verification and revocation) of additional certificate attributes as required by the above profiles. These policy requirements extend the requirements in ETSI EN 319 411-1 [i.68] and ETSI EN 319 411-2 [i.69].

4.2.6 Trust application service providers

The documents for trust application service providers are summarized in table 6 with further details provided below.

Table 6: Standards for trust application service providers

Trust application service providers						
				Sub-areas		
					Guidance	
TR	1	19	5	0	0	Business driven guidance for trust application service providers
SR	0	19	5	1	0	Scoping study and framework for standardization of long term data preservation services, including preservation of/with digital signatures
TR	1	19	5	3	0	(REM) Feasibility study: Interoperability profile between ETSI EN 319 532-based REM systems and PReM-based systems
					Policy & Security Requirements	
TS	1	19	5	1	1	Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
EN	3	19	5	2	1	Policy and security requirements for electronic registered delivery service providers
EN	3	19	5	3	1	Policy and security requirements for Registered Electronic Mail Service Providers
					Technical Specifications	
TS	1	19	5	1	2	Protocols for trust service providers providing long-term data preservation services
EN	3	19	5	2	2	Electronic registered delivery services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Bindings
EN	3	19	5	3	2	Registered electronic mail (REM) services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Interoperability profiles
					Conformity Assessment	
-	-	-	-	-		*no requirement identified for such a document - relying on TS 119 403 / EN 319 403*
					Testing Conformance & Interoperability	
TS	1	19	5	2	4	Testing conformance and interoperability of electronic registered delivery services: - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of electronic registered delivery service providers
TS	1	19	5	3	4	Testing conformance & interoperability of registered electronic mail services. - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of providers using same format and transport protocols

Guidance

ETSI TR 119 500 [i.34] - Business driven guidance for trust application service providers

This document provides guidance for the selection of standards for trusted application service providers for given business requirements. It identifies a number of relevant trusted application services using digital signatures in different business areas, and whose provision has already been standardized. Additionally, for each of the services, it provides guidance for the use of the suitable standards, ensuring in this way their correct provision and interoperability across the European Union.

ETSI SR 019 510 [i.70] - Scoping study and framework for standardization of long term data preservation services, including preservation of/with digital signatures

This document provides a scoping study for long-term data preservation (including preservation of/with digital signatures). It aims at supporting preservation services in different regulatory frameworks.

The document covers two main cases:

1) The preservation of the validity status of the digital signatures (using time-stamps, Evidence Records, etc.) and of the associated signed data.

2) Preservation of the integrity of bits of digital objects, whether they are signed or not, using digital signature techniques (digital signatures, time-stamp tokens, Evidence Records, etc.

In addition, this document provides an inventory of existing standards and selected legal frameworks on the topic of preservation service. It provides as well a proposal for a framework of standards.

ETSI TR 119 530 [i.71] - Registered Electronic Mail (REM); Feasibility study: Interoperability profile between ETSI EN 319 532-based REM systems and PReM-based systems

This document represents a feasibility study for an interoperability profile between systems based on ETSI EN 319 522 [i.127], [i.128], [i.129], [i.130]/ETSI EN 319 532 [i.131], [i.132], [i.133], [i.134] ERDS/REMS specification and UPU S52-2 PReM specification [i.28].

Policy & Security Requirements

ETSI TS 119 511 [i.72] - Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

This document, building on the general policy requirements specified in ETSI EN 319 401 [i.73], specifies policy and security requirements for trust service providers providing long-term preservation of digital signatures and of general data, i.e. signed data or unsigned data, using digital signature techniques. It aims at supporting preservation services in different regulatory frameworks, including but not limited to Regulation (EU) No 910/2014 [i.1].

The document addresses two main cases:

1) The preservation over long periods of time, using digital signature techniques, of the ability to validate a digital signature, of the ability to maintain its validity status and of the ability to get a proof of existence of the associated signed data as they were at the time of the submission to the preservation service even if later the signing key becomes compromised, the certificate expires, or cryptographic attacks become feasible on the signature algorithm or the hash algorithm used in the submitted signature.

2) The provision of a proof of existence of digital objects, whether they are signed or not, using digital signature techniques (digital signatures, time-stamp tokens, evidence records, etc.).

The document identifies specific controls needed to address specific risks associated with preservation services.

The transformation of the original data into another data object with equivalent object content and semantic to avoid the risk that the original data object/viewer system is becoming obsolete is out of the scope of ETSI TS 119 511 [i.72].

ETSI EN 319 521 [i.74] - Policy and security requirements for electronic registered delivery service providers

This document, building on the general policy requirements specified in ETSI EN 319 401 [i.73], specifies generally applicable policy and security requirements for Electronic Registered Delivery Services Providers (ERDSP), including the services they provide.

This document is applicable to:

a) the policy and security requirements of the ERDSP and EU qualified ERDSP;

b) the general and security requirements of Electronic Registered Delivery Services (ERDS) and EU qualified ERDS in terms of message integrity; protection against loss, theft, damage or any unauthorized alteration of the data transmitted; sender and recipient strong identification; time reference; and proof of data's sending and receiving.

The document does not specify interconnection requirements.

ETSI EN 319 531 [i.75] - Policy and security requirements for Registered Electronic Mail Service Providers

This document, building on the general policy requirements specified in ETSI EN 319 401 [i.73], specifies generally applicable policy and security requirements for Registered Electronic Mail Service Provider (REMSP), including the services they provide.

This document is applicable to:

a) The policy and security requirements of REMS and EU qualified REMS providers.

b) The general and security requirements of REMS and EU qualified REMS.

The document does not specify interconnection requirements.

It aims to cover the common and worldwide-recognized requirements to address electronic registered delivery in a secure and reliable way. Particular attention is paid to the Regulation (EU) No 910/2014 [i.1]. However, the legal effects of services implemented according to this document are outside the scope of ETSI EN 319 531 [i.75].

Technical Specifications

ETSI TS 119 512 [i.76] - Protocols for trust service providers providing long-term data preservation services

This document builds upon existing work studied in ETSI SR 019 510 [i.70] and ETSI TS 119 511 [i.72] and specifies protocols for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.

A preservation service can achieve one or more of the following preservation goals:

- extending the validity status of a digital signature over long periods of time; and/or
- providing proofs of existence of general data over long periods of time whether this data is signed or not; and/or
- augmenting externally provided preservation evidences.

The preservation protocol includes:

- a general concept (e.g. Architecture, Goals, different storage models);
- the specification of the protocol in a generic fashion; and
- the specification of the concrete protocol syntax of the conveyed data elements for XML/SOAP and JSON/REST. ensuring at least the submission, retrieval, deletion of data objects and also related evidences.

ETSI EN 319 522 parts 1 [i.127], 2 [i.128], 3 [i.129] and 4 [i.130] - Electronic registered delivery services

This document contains technical specifications for the provision of electronic registered delivery services. This is a multi-part document:

- Part 1 [i.127]: **Framework and architecture:** It provides an overview of the multi-part EN. It also includes an overall view of the standardized service, addressing the following aspects:
  - Logical model, including an overview of the different entities, components and events involved in an electronic delivery transaction.
  - Interfaces between the different roles and providers.
  - Relevant events in the data object flows and the corresponding evidence.
  - Trust building among providers pertaining to the same or to different administrative domains.
- Part 2 [i.128]: **Semantic contents:** This part specifies the semantic contents to be produced and managed in electronic registered delivery transactions. It deals with:
  - **Message delivery content**. Specifications of the semantic of the meta-information that will possibly be associated to the transmission of the payload.

- **Evidence and identification content**. Specifications of the set of evidence managed in the context of the service provision. The document will fully specify the semantics, the components, and the components' semantics for all the evidence. The document will also specify the content related to end user identity to be managed in the transactions.

- **Service discovery content**. Specifications of the information related to the identification of the remote electronic registered delivery management domain, the negotiation of capabilities and requirements that a service supports and the information related to the establishment of trust of a service (e.g. the content that will appear in an appropriate TSL extension for electronic registered delivery services).

- Part 3 [i.129]: **Formats:** This part specifies the formats for the different contents to be produced and managed in electronic registered delivery transactions. It deals with:

  - **Message delivery formats**. Specifications of the format/formats for the meta-information specified by "Semantic contents" part. Meta-information could come either in attached (as an envelope including the payload) or detached format.

  - **Evidence and identification formats**. Specifications of the syntax for the set of evidence and user identity information specified in "Semantic contents" part.

  - **Service discovery formats**. Specifications of the format/formats for capabilities, requirements and trust information specified in the "Semantic contents" part.

- Part 4 [i.130]: **Bindings:** This part is itself split into sub-parts. Each part fully specifies the binding to a messaging protocol that is supporting electronic delivery services provision. The messaging protocols are defined. This includes specification on how to transport evidence within the protocol messages, how to include signature's provider within the protocol's message, etc. Each sub-part specifies anything that is required to ensure interoperability among providers of the service being compliant with that part. Sub-parts are covering the following topics:

  - **Message delivery bindings;**

  - **Evidence and identification bindings;**

  - **Capability/requirements bindings.**

ETSI EN 319 532 parts 1 [i.131], 2 [i.132], 3 [i.133] and 4 [i.134] - Registered Electronic Mail (REM) Services

This document contains technical specifications for the provision of registered electronic mail. It exclusively specifies those aspects that are particular to the provision of electronic registered delivery services using SMTP and SMIME as transport protocol and data formats respectively. This is a multi-part EN organized as follows:

- Part 1 [i.131]: **Framework and architecture:** This part provides an overview of the multi-part EN. It normatively refers to ETSI EN 319 522-1 [i.127] whenever applicable and includes aspects of the provision of registered electronic mail standardized services, which are not common to the provision of other types of electronic delivery provision, but specific to REM.

- Part 2 [i.132]: **Semantic contents:** This part specifies semantic contents to be produced and managed in REM transactions. It normatively refers to ETSI EN 319 522-2 [i.128] whenever applicable and specifies semantics which are not common to the provision of other types of electronic delivery services, but specific to the provision of REM services.

- Part 3 [i.133]: **Formats:** This part specifies the formats for the different messages to be produced and managed in REM transactions using SMIME on SMTP. It normatively refers to ETSI EN 319 522-3 [i.129] whenever applicable and specifies issues which are specific to REM.

- Part 4 [i.134]: **Interoperability profiles:** This part specifies profile(s) for seamless exchange of data objects across providers that use the same or different formats and/or transport protocols.

Conformity Assessment

Not applicable so far.

Testing Conformance & Interoperability

ETSI TS 119 524 parts 1 [i.77] and 2 [i.78] - Testing conformance and interoperability of electronic registered delivery services

This document defines test suites that support interoperability tests among entities providing electronic registered delivery services. It also specifies tests assertions for checking conformance against relevant specifications of ETSI EN 319 522 parts 1 [i.127], 2 [i.128], 3 [i.129] and 4 [i.130]. It is a multipart document organized as follows:

- Part 1 [i.77]: **Testing conformance:** This part specifies test assertions for checking conformance against relevant specifications of ETSI EN 319 522 parts 1 [i.127], 2 [i.128], 3 [i.129] and 4 [i.130].
- Part 2 [i.78]: **Test suites for interoperability testing of electronic registered delivery service providers:** This document applies to those providers that implement the service provision using the same combination of format and transport protocols.

ETSI TS 119 534 parts 1 [i.79] and 2 [i.80] - Testing conformance and interoperability of registered electronic mail services

This document defines test suites that support interoperability tests among entities providing registered electronic mail services. It also specifies tests assertions for checking conformance against relevant specifications of ETSI EN 319 532 parts 1 [i.131], 2 [i.132], 3 [i.133] and 4 [i.134]. It is a multipart document organized as follows:

- Part 1 [i.79]: **Testing conformance:** This document specifies the tests to be performed for checking conformance against ETSI EN 319 532 parts 1 [i.131], 2 [i.132], 3 [i.133] and 4 [i.134].
- Part 2 [i.80]: **Test suites for interoperability testing of providers using same format and transport protocols:** This document applies to those providers that implement the service provision using the same combination of format and transport protocols.

4.2.7 Trust service status lists providers

Table 7: Standards for trust service status lists providers

Trust service status lists providers						
				Sub-areas		
				Guidance		
TR	1	19	6	0	0	Guidance on the use of standards for trust service status lists providers
				Policy & Security Requirements		
-	-	-	-	-		*no requirement identified for such a document*
				Technical Specifications		
TS	1	19	6	1	2	Trusted lists
				Conformity Assessment		
-	-	-	-	-		*no requirement identified for such a document - relying on TS 119 403 / EN 319 403*
				Testing Conformance & Interoperability		
TS	1	19	6	1	4	Testing conformance & interoperability of trusted lists: - Part 1: Specifications for testing conformance of XML representation of trusted lists
				Sector Specific Requirements		
TS	1	19	6	1	5	Procedures for using and interpreting European Union Member States national trusted lists

Guidance

ETSI TR 119 600 [i.35] - Guidance on the use of standards for trust service status lists providers

This document provides guidance for the use of standards for trusted service status lists providers for given business requirements.

Technical Specifications

ETSI TS 119 612 [i.44] - Trusted lists

This document contains the specifications related to trusted lists in particular as they are defined in the applicable legislation, including but not limited to the European legislation.

NOTE: Version 2.1.1 is referenced by EU secondary legislation specifying formats for trusted lists applicable for the purposes of eIDAS Regulation 910/2014/EU [i.1].

Testing Conformance & Interoperability

ETSI TS 119 614 part 1 [i.81] - Testing Conformance and Interoperability of Trusted Lists

- Part 1 [i.81]: **Specifications for testing conformance of XML representation of trusted lists:** This document defines the set of checks to be performed for testing conformance of Trusted Lists as specified in ETSI TS 119 612 [i.44]. Checks specified by the document are exclusively constrained to elementsspecified by ETSI TS 119 612 [i.44], certain elements defined in ETSI TS 101 903 [i.18], and certain elements specified in XMLSig [i.29]. Regarding XML elements, the document explicitly differentiates between structural requirements that are defined by the different XML Schemas where the tested elements are defined, and the rest of the requirements specified by ETSI TS 119 612 [i.44].

Sector Specific Requirements

ETSI TS 119 615 [i.82] - Procedures for using and interpreting European Union Member States national trusted lists

This document specifies procedures for using and interpreting EUMS national trusted lists when validating EU qualified trust service outputs against them (e.g. validating EU qualified certificates, EU qualified time stamps, evidences created by qualified electronic registered delivery services, EU electronic signatures or seals on EU qualified validation reports on EU qualified electronic signatures or seals).

History

Document history		
V1.1.1	September 2015	Publication
V1.2.1	April 2016	Publication
V1.3.1	May 2023	Publication