ETSI TR 119 500 V1.1.1 (2019-02)

Business Driven Guidance for
Trust Application Service Providers

Reference
DTR/ESI-0019500

Keywords
electronic registered delivery, electronic signature, registered electronic mail, security, trust services

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

Modal verbs terminology

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

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

Introduction

ETSI TR 119 000 [i.1] provides a general structure for electronic signatures standardization outlining existing and potential standards for digital signatures. This identifies six areas of standardization with a list of existing and potential future standards in each area.

This guide is one of a series of guidance documents on selection of standards and options for digital signatures to assist users and their suppliers in identifying the standards and options relevant to their need. Each guide addresses a particular area as identified in the ETSI TR 119 000 [i.1].

This series is based on the process of selecting Business Scoping Parameters for each area of standardization based on an analysis of the business requirements. The selection of these scoping parameters is based on a process involving an analysis of the business requirements and associated risks leading to an identification of the policy and security requirements and the resulting Business Scoping Parameters from which the appropriate standards and options can be selected. Having identified the requirements in terms of Business Scoping Parameters for an area, each guidance document provides assistance in selecting the appropriate standards and options for that area.

This guidance does not include any normative requirements but provides guidance on addressing the Trust Application Service Providers (TASP) area, on the selection of applicable standards and their options for a particular business implementation context and associated business requirements.

TASP covers Trust Service Providers offering value added services applying digital signatures and that rely on the generation/validation of digital 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 electronic signatures are identified.

This general process of the selection of standards and options is described further in ETSI TR 119 000 [i.1], clause 4.2.6.

1 Scope

The present document provides guidance on the use of standards for Trust Application Service Providers (area 5) as identified in the framework for standardization of signatures: overview [i.1].

The present document then describes the Business Scoping Parameters relevant to this area (see clause 6) and how the relevant standards and options for this area can be identified given the Business Scoping Parameters (clause 7).

The target audience of the present document includes:

1) Business managers who potentially require support from digital signatures in their business will find here an understandable explanation of how services applying digital signatures standards can be used to meet their business needs.

2) Application architects who will find here material that will guide them throughout the difficult process of designing a system that fully and properly satisfies all the business and legal/regulatory requirements specific to services applying digital signatures, and will gain a better understanding on how to select the appropriate standards to be implemented and/or used.

3) Developers of the systems who will find an understanding of a good part of the ultimate reasons that led the systems to be designed as they were, as well as a proper knowledge of the standards that exist in the field and to be known in detail for a proper development.

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] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.2] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.3] ETSI EN 319 522-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture".

[i.4] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents".

[i.5] ETSI EN 319 522-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats".

[i.6] ETSI EN 319 522-4-1: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings".

[i.7] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers".

[i.8] ETSI EN 319 532-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and architecture".

[i.9] ETSI EN 319 532-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic Contents".

[i.10] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats".

[i.11] ETSI EN 319 532-4: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles".

[i.12] Regulation (EU) N 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.13] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation".

[i.14] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.15] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.16] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.17] ETSI EN 319 522-4-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings".

[i.18] ETSI EN 319 522-4-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings".

[i.19] ETSI TS 119 524-1: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 1: Testing conformance".

NOTE: Defines the set of checks to be performed for testing conformance in the provision of ERD Services against the specific technical requirements defined in ETSI EN 319 522-3, Part 3, ETSI EN 319 522-4-1 and ETSI EN 319 522-4-2.

[i.20] 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.21] ETSI TS 119 534-1: "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 1: Testing conformance".

[i.22] 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.23] ETSI SR 001 604: "Rationalised Framework for Electronic Signature Standardisation".

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.14] and the following apply:

Electronic Registered Delivery Service (ERDS): electronic service that makes it possible to transmit data between the sender and recipients by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations

NOTE: An electronic registered delivery service is provided by one ERDSP. ERDSPs can cooperate in transferring data from a sender to a recipient when they are subscribed to different ERDSPs.

Electronic Registered Delivery Service (ERDS) evidence: data generated within the electronic registered delivery service, which aims to prove that a certain event has occurred at a certain time

Electronic Registered Delivery Service (ERDS) practice statement: statement of the practices that an electronic registered delivery service provider employs in providing its services

NOTE: See clause 4 for further information on practice statement.

Electronic Registered Delivery Service Provider (ERDSP): trust service provider which provides electronic registered delivery service

NOTE: It can be a Trust Service Provider as defined in Regulation (EU) No 910/2014 [i.12].

Qualified Electronic Registered Delivery Service (QERDS): As specified in Regulation (EU) No 910/2014 [i.12].

Qualified Electronic Registered Delivery Service Provider (QERDSP): trust service provider which provides qualified electronic registered delivery service

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CAB	Certification Authority Browser (Forum)
CAB	Conformity Assessment Body
DPS	Data Preservation Service
ERD	Electronic Registered Delivery
ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
OASIS	Organization for the Advancement of Structured Information Standards
QERDS	Qualified Electronic Registered Delivery Service
QERDSP	Qualified Electronic Registered Delivery Service Provider
REM	Registered E-Mail
REMS	Registered Electronic Mail Service
REMSP	Registered Electronic Mail Service Provider
SMTP	Simple Mail Transfer Protocol
TASP	Trust Application Service Provider
TS	Trust Service
TSP	Trust Service Provider

4 Overview of this area of standardization

4.1 What is a Trust Application Service Provider

A Trust Application Service Provider (TASP) operates a value added Trust Service offering value added services applying digital signatures that rely on the generation/validation of digital signatures in normal operation. This covers services like registered electronic mail and other type of e-delivery services, as well as long term storage services assuring object data's integrity by means of digital signatures. Trust Application Service Providers are Trust Service Providers.

4.2 Types of Trust Application Service

4.2.1 ERDS

Business and administrative relationships among companies, public administrations and private citizens are more and more implemented electronically. Trust is essential for their success and continued development of electronic services. It is therefore important that any entity using electronic services have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their partners.

Digital signatures are commonly used worldwide to ensure authenticity and integrity of electronic documents, making it possible to transform traditional paper-based processes into electronic ones providing a comparable or even higher level of assurance. As communication is becoming predominantly internet-based, secure and provable exchange of documents is essential to the full digital transformation.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [i.16] provides a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework aims to open new market opportunities for European Union trust service providers to offer new pan-European electronic registered delivery services. The Regulation defines the so-called Qualified Electronic Registered Delivery Service (QERDS), which is a special type of ERDS, where both the service and its provider need to meet a number of additional requirements that the regular ERDSs and their providers do not need to meet.

An Electronic Registered Delivery Service (ERDS) provides secure and reliable delivery of electronic messages between parties, producing evidence of the delivery process for legal accountability. Evidence can be seen as a declaration by a trusted party that a specific event related to the delivery process (submission of a message, relay of a message, delivery of a message, refusal of a message, etc.) happened at a certain time. Evidence can be immediately delivered to the interested party (together with the message or separately) or can be kept in a repository for later access.

Without the definition of common standards there will be no consistency in the services provided, making it difficult for users to compare them. Under these circumstances, users might be prevented from easily changing to alternative providers, damaging free competition. Lack of standardization might also adversely affect interoperability between implementations which are based on different models.

The framework of ERDS standards aims to cover the common and worldwide-recognized requirements to address electronic registered delivery in a secure and reliable way, independent of the applicable legislative framework.

At the same time, the framework of ERDS standards aims to support demonstrating compliance to the Regulation (EU) No 910/2014 [i.12] (and related secondary legislation), both for non-qualified and qualified electronic registered delivery services. Specific clauses are included defining requirements applicable only to qualified electronic registered delivery services, especially in ETSI EN 319 521 [i.2] covering policy and security requirements.

Standards covering ERDS are as follows:

- ETSI EN 319 521 [i.2] specifies the policy and security requirements of the ERDSP and EU qualified ERDSP; and 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.

- ETSI EN 319 522-1 [i.3] provides a reference framework and architecture for Electronic Registered Delivery Services.
- ETSI EN 319 522-2 [i.4] specifies the semantic content that flows across the interfaces of ERD services which are specified in ETSI EN 319 522-1 [i.3], clause 5.
- ETSI EN 319 522-3 [i.5] specifies the format for the semantic content (metadata, evidence, identification, and Common Service Infrastructure) that flows across the different interfaces of an Electronic Registered Delivery Service (ERDS) as defined in ETSI EN 319 522-2 [i.4].
- ETSI EN 319 522-4-1 [i.6] defines the binding of the ERD messages, whose semantics is defined in ETSI EN 319 522-2 [i.4] and whose format is defined in ETSI EN 319 522-3 [i.5], to the specific transmission protocol AS4.
- ETSI EN 319 522-4-2 [i.17] specifies the binding of the ERD evidence and identification, whose semantics is defined in ETSI EN 319 522-2 [i.4] and whose format is defined in ETSI EN 319 522-3 [i.5], to the specific transmission protocol AS4.
- ETSI EN 319 522-4-3 [i.18] provides the binding of the Common Service Interface information, whose semantics is defined in ETSI EN 319 522-2 [i.4] and whose format is defined in ETSI EN 319 522-3 [i.5] to the specific services provided by OASIS Business Metadata Service Location and the OASIS Service Metadata Publishing
- ETSI TS 119 524-1 [i.19] defines the set of checks to be performed for testing conformance in the provision of ERD Services against the specific technical requirements defined in ETSI EN 319 522-3 [i.5], ETSI EN 319 522-4-1 [i.6] and ETSI EN 319 522-4-2 [i.17].
- ETSI TS 119 524-2 [i.20] defines a test suite for supporting interoperability tests within the field of ERD services as specified in ETSI EN 319 522 parts 1 [i.3], 2 [i.4], 3 [i.5], 4-1 [i.6], 4-2 [i.17] and 4-3 [i.18] and a mechanism for documenting new test cases and expanding the aforementioned test suite.

4.2.2 REM

Registered Electronic Mail (REM hereinafter) is a specific type of electronic registered delivery, which builds on the formats, protocols and mechanisms used in ordinary e-mail messaging. The basic purpose of Registered E-Mail service is to provide users, in addition to the usual services supplied by the ordinary e-mail service providers, with a set of evidence suitable to uphold assertions of acceptance (i.e. of "shipment"), of delivery/non-delivery, of retrieval, etc. of e-mails sent/delivered through such service.

A range of Registered E-Mail ("REM") services are already established and their number is set to grow significantly over the last few years.

Since REM is a specific type of electronic registered delivery, the documents covering REM service build on the corresponding documents covering ERDS by referencing the necessary provisions, and define the interpretation and specific requirements which apply only to registered electronic mail.

Standards covering REM are as follows:

- ETSI EN 319 531 [i.7] specifies generally applicable policy and security requirements for Registered Electronic Mail Service Provider (REMSP), including the services they provide. It includes policy and security requirements of REMS and EU qualified REMS providers and general and security requirements of REMS and EU qualified REMS.
- ETSI EN 319 532-1 [i.8] specifies the logical model and basic concepts of REM service, and relies on ETSI EN 319 522-1 [i.3] for all concepts and requirements which are generally applicable to all ERDS, and defines the interpretation and specific requirements which apply only to registered electronic mail.
- ETSI EN 319 532-2 [i.9] defines the semantic content of messages and evidence used in REM service and relies on ETSI EN 319 522-2 [i.4] for all semantic contents and requirements which are generally applicable to all electronic registered delivery services, and defines the interpretation and specific requirements which apply only to REM.

- ETSI EN 319 532-3 [i.10] specifies the formats for messages that are produced and handled by a REM service according to the concepts and semantic defined in ETSI EN 319 522-1 [i.3] and ETSI EN 319 522-2 [i.4] and ETSI EN 319 532-1 [i.8] and ETSI EN 319 532-2 [i.9]. More specifically the present document specifies how the general ERDS concepts like user content and metadata are identified and mapped in the standard email structure; how these concepts are mapped in the REM service messaging structures; how the ERDS evidence set is plugged inside the REM service messaging structures; and additional mechanisms like digital signature and other security controls.

- ETSI EN 319 532-4 [i.11] specifies the interoperability profiles of REM messages according to the formats defined in ETSI EN 319 532-3 [i.10] and the concepts and semantic defined in ETSI EN 319 532-1 [i.8] and ETSI EN 319 532-2 [i.9]. It deals with issues relating authentication, authenticity and integrity of the information, with the purpose to address the achievement of interoperability across REM service providers. More specifically the present document defines generalities on profiling and constraints for SMTP profile.

- ETSI TS 119 534-1 [i.21] defines the set of checks to be performed for testing conformance in the provision of REM Services against the specific technical requirements defined in ETSI EN 319 532-3 [i.10] and against technical requirements for the provision of the service defined in ETSI EN 319 532-1 [i.8].

ETSI TS 119 534-2 [i.22] defines a test suite for supporting interoperability tests within the field of REM hereinafter) as specified in ETSI EN 319 532 parts 1 [i.8], 2 [i.9], 3 [i.10] and 4 [i.11], and a mechanism for documenting new test cases and expanding the aforementioned test suite.

4.2.3 Data Preservation Service (DPS)

Data Preservation Service (DPS) can provide a sound basis for maintaining data object ensuring integrity, authenticity and legibility throughout an entire storage period.

4.2.4 Other potential Trust Application Services

No other service has been identified so far.

4.3 Aspects of TASP Service Requiring Standardization

4.3.1 Policy & security Requirements

In order to ensure the trustworthiness of a TASP's service, it is important that it is provided in a way that the security and business practices of the TASP meet the recognized best practices for such services, and in the case of qualified TASPs also meet the requirements laid out in the applicable regulation. Any weakness in the TASP practices can potentially lead to significant risk of compromise to the TASP's services and so break the trust that the TASP users have in being able to ensure the security of their own transactions based on the TASP's services.

Through standardization of such best practice there is a recognized level of trust on which the users can base their decision to use the services of a TASP. These standards are laid out in a way which can be related to TASP Policies and TASP Practices which are the basis on which all TASPs are expected to specify their operations.

A TASP service makes use of system components (e.g. cryptographic devices, computer systems) which need to be secure for the overall operation of the TASP service to be secure.

4.3.2 Technical Specifications

TASP provide trust services by securing transactions between parties or preserving archived data, providing evidence relating to the handling of the transmitted or stored information.

Data should be protected against the risk of loss, theft, damage or any unauthorized alterations in order to ensure legal validity, secure identifications, and reliable transactions. ETSI EN 319 401 [i.15] establishes general policy requirements and security controls for TSP that are also applicable to TASPs.

4.3.3 Conformity Assessment

In order to gain assurance that a TASP's service applies the best practices expected for it to be trustworthy the TASP need to be checked that its policies and practices meet the standard criteria for its services. This is done through an independent body assessing whether the TASP's policies and practices meet the requirement laid out in the standard criteria and their internal procedures are implemented accordingly, and that the policies and practices are being effectively applied.

This independent body is called a conformity assessment body (CAB), and employs auditors to visit the TASP regularly to check that the standard criteria are being met. Conformity assessment standards lay out the required capabilities of the conformity assessment and how the assessment is carried out.

Such conformity assessment generally is required to get formal recognition of the "trustworthiness" of the TASP by:

- a legal entity, such a supervisory body as identified in Regulation (EU) N° 910/2014 [i.12], concerned with regulating the operation of TSPs;
- by a commercial or governmental organization, which can use the services of a TASP; or
- a commercial association, such as the CAB Forum, which represents the interests of a community of users.

5 Introduction to the Selection Process

The general approach to the provision of business guidance is to firstly analyse the overall business requirements for digital signature in terms of Business Scoping Parameters.

It is recognized that guidance is needed to assist in the selection of standards for TASP and their implementation in an electronic business process. Once the stakeholder (users, suppliers, regulators, etc.) conducted his/her analysis on the business requirements for the use for Trust Application Services, he/she first needs to identify Trust Application Services scoping parameters when implementing them and, based on this, select the most appropriate effective solution.

Having identified the Business Scoping Parameters applicable to the business context, the implementer needs to map the applicable scoping parameters into the selection of the appropriate standards and the technical rules for their implementation (potentially including initialization and parameter configuration of those standards and their options).

The process regarding the analysis of the practices and policy requirements as well as the conduction of a risk analysis relating to TASPs and to the provision of trust services is addressed in the relevant policy and security requirements documents (e.g. ETSI EN 319 401 [i.15]), as identified in clause 7 below. Moreover, a complete digital signatures solution will need to address requirements in most of the areas. Providers of components of an overall solution may only need to consider a specific guidance document, for example providers of REM need only consider guidance for trust application service providers area 5 (TASP for digital signatures) of the rationalized framework (ETSI SR 001 604 [i.23]). However, even in such cases the goal of the Business Scoping Parameter will be to meet its customer's needs, which will be to address the overall requirement.

These Business Scoping Parameters analyse the trust service to be provided and its particular implementation and help in selecting the applicable standards. Having identified the requirements in terms of Business Scoping Parameters for each area, the guidance documents provide assistance in selecting the appropriate standards and options.

6 Business Scoping Parameters

6.1 Overview

The general approach to business guidance is based on the process described in ETSI TR 119 100 [i.13].

The Business Scoping Parameters selection process for each area of standardization is based on an analysis of the business requirements and associated risks. This leads to an identification of the policy and security requirements and the selection of the appropriate standards. Having identified the requirements in terms of Business Scoping Parameters for an area, each guidance document provides assistance in selecting the appropriate standards and options for that area.

Where standards and options within one area make use of another area this is stated in terms of Scoping Parameters of that other area.

6.2 Scoping the trust application processes and/or services

Based on this scoping approach (requirements analysis, identification of Business Scoping Parameters, selection of standards and technical rules for their implementation), a set of Business Scoping Parameters will be of particular relevance. These may include:

1) organizational parameters: the organization may determine external and internal issues that are relevant to its purpose and that affects its ability to perform the application trust service. There is also a need to understand the needs and expectations of interested parties identifying those that are relevant to the application trust service and the requirements of these interested parties to the application trust service. These parameters may include legal and regulatory requirements and contractual obligations and the following:

    i) the business context parameters, including but not limited to:

        a) the business application domain and its underlying technology;

        b) the business process;

        c) the business risks;

    ii) the budgetary constraints;

    iii) the associated organizational or application or other security policies;

    iv) the associated legal requirements;

    v) the mitigation measures resulting from a risk assessment; and

    vi) the community within which the service is to be provided whether global, European, national or sector specific. This may influence the need to adopt standards appropriate to that community;

2) trust application services parameters: when determining the scope of the application trust service and its boundaries, the organization may consider i.e. the business process and/or products affected; assets, technical and human resources involved; interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations; and/or roles and components;

3) organization's security parameters: once the organization identifies the trust application services assets and their associated information security requirements, it may assess the trust application services security risks and treat the security risks selecting and implementing relevant controls to manage unacceptable risks, monitoring, maintaining and improving the effectiveness of controls associated with the trust service's assets;

4) digital signature specific parameters: within the overall strategy and business objectives of the organization, its size and geographical spread, trust application services digital signatures parameters can be identified through an understanding of the signature specific parameters that are described further in ETSI TR 119 100 [i.13].

7 Selecting the Most Appropriate Standards and options

7.1 Introduction

The selection of standards and their options for a TASP depends on the result of applying the scoping factors to the service or the specific service process. Depending on this result, the TASP selects the appropriate standardization requirements, taking account of the scoping process results, and determines all controls and requirements that are necessary to implement the trust service.

7.2 Illustration of Application of Standard

7.2.1 ERDS

Given the selection choices the standards defined in the rationalized framework [i.23] for ERDS (Area 5) should be used where indicated by an "x".

Table 1

		Elements				
Standard	**Conformity Assessment**	**Provision on policy and practices (including security requirements)**	**Provisions on ERDSP**	**Provisions on EU qualified ERDSP**	**Evidence: semantics and format**	**Interoperability profiles, formats and bindings**
ETSI EN 319 401 [i.15]	X	X				
ETSI EN 319 521 [i.2] Policy and security requirements for Electronic Registered Delivery Service Providers	X	X	X	X		
ETSI EN 319 522-1 [i.3] Framework and Architecture			X	X	X	X
ETSI EN 319 522-2 [i.4] Semantic contents					X	
ETSI EN 319 522-3 [i.5] Formats					X	X
ETSI EN 319 522-4-1 [i.6] Message delivery bindings						X

7.2.2 REM

Given the selection choices the standards defined in the rationalized framework [i.23] for REM (Area 5) should be used where indicated by an "x".

Table 2

		Elements				
Standard	**Conformity Assessment**	**Provision on policy and practices (including security requirements)**	**Provisions on REMSP**	**Provisions on EU qualified REMSP**	**Evidence: semantics and format**	**Interoperability profiles, formats and bindings**
ETSI EN 319 401 [i.15]	X	X				
ETSI EN 319 531 [i.7]: Policy and security requirements	X	X	X	X		
ETSI EN 319 532-1 [i.8]: Framework and architecture			X	X	X	X
ETSI EN 319 532-2 [i.9]: Semantic contents					X	
ETSI EN 319 532-3 [i.10]: Formats					X	X
ETSI EN 319 532-4 [i.11]: Interoperability profiles						X

7.2.3 Data Preservation Service

This will be described in a future version of the present document.

History

Document history		
V1.1.1	February 2019	Publication