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

Business Driven Guidance for Trust Application Service Providers

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/...-ee7f-406d-b0b4-71ac9802ba88/etsi-tr-119-500-v1.1.1-2019-02

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Important notice

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

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

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

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.
All rights reserved.

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.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/bbd91cab-ce7f-4b6d-8bb4-7ac9802ba88/etsi-tr-119-500-v1.1.1-2019-02

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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/bad91cab-ee7f-406d-b0b4-1ac9a22bb88/etsi-tr-119-500-v1.1.1-2019-02

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/bbd91cab-ee7f-406d-b0b4-71ac9802ba88/etsi-tr-119-500-v1.1.1-2019-02

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".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/bbd91cab-ce7f-406d-b0b1-710b9802ba88/etsi-tr-119-500-v1.1.1-2019-02

[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".

iTeh STANDARD PREVIEW (standards.iteh.ai)

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b0b4-71ac9802ba88/etsi-tr-119-500-v1.1.1-2019-02

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.

iTeh STANDARD PREVIEW (standards.iteh.ai)

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.