Draft ETSI EN 319 522-1 V1.0.0 (2018-05)

Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture

Reference

DEN/ESI-0019522-1

Keywords

e-delivery services, registered e-delivery services, registered electronic mail

ETSI

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

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

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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

This draft European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI standards EN Approval Procedure.

The present document is part 1 of a multi-part deliverable covering the Electronic Registered Delivery Services, as identified below:

Part 1: "Framework and Architecture";

Part 2: "Semantic contents";

Part 3: "Formats";

Part 4: "Bindings":

Sub-part 1: "Message delivery bindings";

Sub-part 2: "Evidence and identification bindings";

Sub-part 3: "Capability/requirements bindings".

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

1 Scope

The present document provides a reference framework and architecture for Electronic Registered Delivery Services.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

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 necessary for the application of the present document.

Not applicable.

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) 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.2] ISO/IEC 13888-1:2009: "Information technology - Security techniques - Non-repudiation - Part 1: General".

[i.3] ISO/IEC 13888-2:2010: "Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques".

[i.4] ISO/IEC 13888-3:2010: "Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques".

[i.5] ETSI EN 319 522-2: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic Contents".

[i.6] ETSI EN 319 522-3: "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats".

[i.7] 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.8] 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".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Common Service Interface (CSI): interface of a supporting system that can provide message routing, trust management, capability management, governance functions

consignment: act of making the user content available to the recipient, within the boundaries of the electronic registered delivery service

Electronic Registered Delivery Service (ERDS): electronic service that transmits data between a sender and recipients by electronic means, 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 (as detailed in 4-corner and extended models in clauses 4.3 and 4.4).

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

NOTE: It can be a Trust Service Provider as defined in Regulation (EU) No 910/2014 [i.1].

ERD event: relevant event in the electronic delivery process, which can be attested by an ERDS evidence

ERD message: data composed of an optional user content, ERDS relay metadata and zero or more ERDS evidence

ERD User Agent/Application (ERD-UA): system consisting of software and/or hardware components by which senders and recipients participate in the exchange of data with electronic registered delivery service providers

ERDS evidence: data generated by the electronic registered delivery service, which aims to prove that a certain event has occurred at a certain time

ERDS handover metadata: data related to the user content which is generated by the electronic registered delivery service and handed over to the ERD user agent/application

ERDS Message and Evidence Retrieval Interface (ERDS MERI): interface of electronic registered delivery service used by ERD user agent/application to retrieve user content and associated metadata

ERDS Message Submission Interface (ERDS MSI): interface used by the sender's ERD user agent/application to submit original messages to the sender's electronic registered delivery service

ERDS Relay Interface (ERDS RI): interface that supports ERD message relay between different electronic registered delivery services

ERDS relay metadata: data related to the user content which is generated by the electronic registered delivery service for the purpose of relaying to another electronic registered delivery service

ERD-UA Message and Evidence Push Interface (ERD-UA MEPI): interface of ERD-UA used by ERDS to push data

handover: act of having the user content successfully cross the border of the recipient's electronic registered delivery service towards the recipient's ERD user agent/application

original message: data including user content and submission metadata

recipient: natural or legal person to which the user content is addressed

sender: natural or legal person that has submitted the user content

submission metadata: data submitted to the electronic registered delivery service together with the user content

user content: original data produced by the sender which has to be delivered to the recipient

3.2 Abbreviations

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

CSI	Common Service Interface
DNS	Domain Name System
ERD	Electronic Registered Delivery
ERDS	Electronic Registered Delivery Service
ERDS MERI	ERDS Message and Evidence Retrieval Interface
ERDS MSI	ERDS Message Submission Interface
ERDS RI	ERDS Relay Interface
ERDSP	Electronic Registered Delivery Service Provider
ERD-UA MEPI	ERD-UA Message and Evidence Push Interface
ERD-UA	Electronic Registered Delivery User Agent/Application
ERP	Enterprise Resource Planning
I-ERDS	Intermediate ERDS
R-ERDS	Recipient's ERDS
SAML	Security Assertion Markup Language
S-ERDS	Sender's ERDS
WSDL	Web Services Description Language

4 ERDS logical model

4.1 Introduction

An ERDS provides evidence about events that happen during the transfer of data between parties (e.g. evidence that the data has been delivered to the recipient), similar to well-known physical postal services for paper-based documents, such as "registered mail" and/or "return receipt". This evidence can be used to prove to third parties, if needed also in legal proceedings, that the transaction took place at the time and between the parties as indicated in the evidence. The legal requirements to an ERDS and the evidence it needs to support can vary across different domains.

An **ERDS evidence** is an **attestation** provided by an ERDS **that a specific event** related to the process of transferring some specific data between the sender and recipient (for instance, the submission of a message, the delivery of a message, the refusal of a message) **happened at a certain time**. An ERDS evidence can be immediately delivered to the sender/recipient or can be kept in a repository for later access by interested parties. It is common practice to implement ERDS evidence as digitally signed data. The concept of ERDS evidence can be assimilated to non-repudiation tokens defined in ISO/IEC 13888 [i.2], [i.3] and [i.4], with many specificities as illustrated in clause 6. Secure and reliable delivery to a recipient requires that the recipient is uniquely identified. The present document also covers the unique identification of the sender (which is a requirement, for instance, for enforcing legal accountability), even if in some cases his identity is not disclosed to the recipient. Unique identification can be achieved by one unique identifier or by a collection of attributes that together uniquely identify the actor. An important purpose of the present document is to support ERDS delivery between senders and recipients that are natural or legal persons; however, in principle any uniquely identified entity (system, service, function, etc.) that can be addressed through an ERDS can be a sender or recipient. The present document also addresses delegation, i.e. the capability of a sender or a recipient to delegate a different entity to act on their behalf. An ERDS can rely on external, trusted parties for authentication.

The ERDS concept described above can be implemented in diverse ways, using different formats for identifiers and ERDS evidence, using different protocols for messaging, and even different message delivery models. Clause 4 aims to provide a general model that includes all relevant features, while abstracting from implementation issues. For convenience, the modelling goes through three steps:

- A black-box model, dealing with a single ERDS. Internal complexities of the ERDS are not relevant as far as it can be seen as a unique system under the responsibility of a single ERDSP. The black-box model describes the interactions of the ERDS with the sender and recipients through an application layer outside of the boundary of the ERDS.

- A 4-corner model, dealing with the exchange of data and ERDS evidence between two ERDSs: one on the sender's side, the other on the recipient's side. The interaction of the ERDSs with the sender and recipient (interfaces) are the same as in the black-box model.
- An extended model, dealing with the transmission of data and ERDS evidence through a chain of ERDSs.

4.2 Black-box model

4.2.1 Functional viewpoint

In the simplest case, an ERDS can be represented as a black box, conveying messages between a sender and a recipient and producing the appropriate ERDS evidence. Figure 1 provides a simple representation.

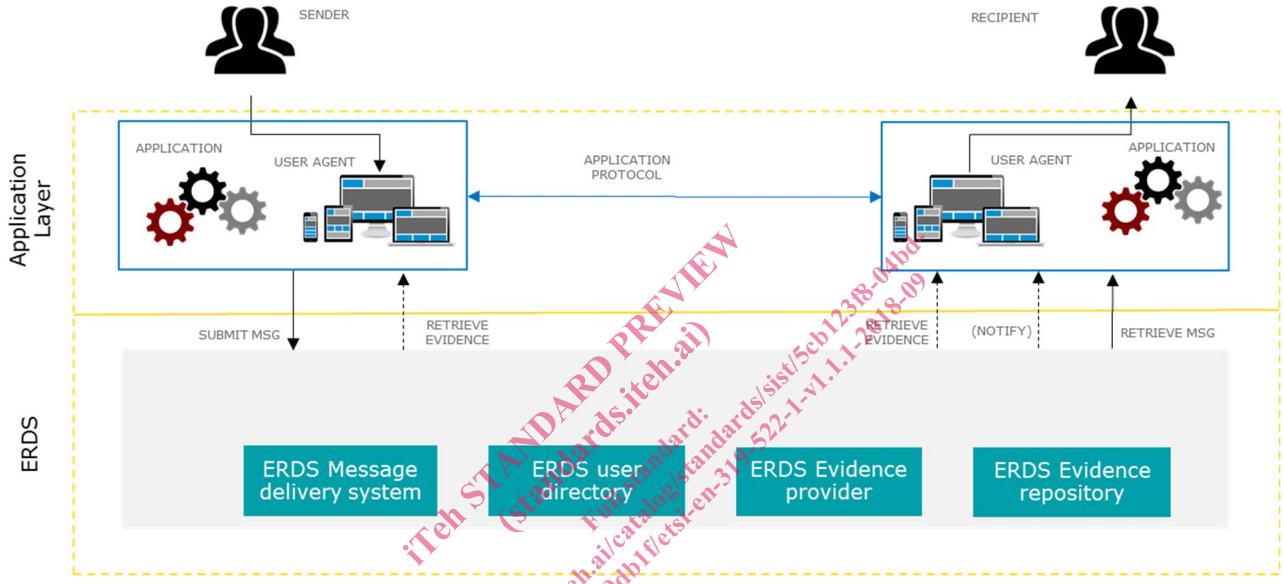

Figure 1: Black-box registered delivery service model

ERDS can be accessed by an ERD-UA, i.e. an application directly interacting with a human user or an enterprise application (an ERP, a document workflow, etc.) with or without involvement of a human user. ERDS allows to submit/receive user content plus associated metadata and to receive ERDS evidence related to the delivery process. The sender provides unique identification of the recipient, and the ERDS associates it to the correct delivery endpoint.

Between applications, an application layer protocol (e.g. a business process protocol) is executed, consisting of a sequence of one or more messages in one or both directions. Applications can belong to service providers within particular (business) areas (e.g. an e-procurement service provider or an e-health service provider). An application layer protocol can include requirements and mechanisms for application of digital signatures to message content before sending, for end-to-end encryption between sender and recipient, etc. The application protocol is out of scope of the ERDS, which needs not to possess knowledge of the application layer logic nor the relationships between different messages. From the ERDS point of view, the application-level service providers will act in this case as a sender/recipient. The ERD-UA will submit the user content, together with additional metadata (receiver identification, etc.) to the ERDS.

Breaking into the black box, figure 1 introduces some components which are typically included in an ERDS, namely:

- **ERDS Message delivery system:** this component grants that the user content submitted by the sender is made available to the intended recipient. Note that this does not necessarily imply a transfer of the data (e.g. the delivery can consist in making existing data available to the recipient).
- **ERDS User directory:** this component is used to translate the unique identification of a recipient, possibly augmented by further metadata, into a delivery endpoint. The same recipient can correspond to more delivery endpoints, depending on metadata (e.g. user content and evidence, or even different types of user content, can be directed to different endpoints).

- **ERDS Evidence provider:** this component produces the ERDS evidence upon completion of specific delivery events.
- **ERDS Evidence repository:** this component grants the persistence of ERDS evidence for a period of time which depends on the specific policies of the service. Storing of the ERDS evidence can be performed by a third party service, outside the ERDS.

4.2.2 Sequence viewpoint

In the black-box perspective, the typical electronic registered delivery flow appears as presented in figure 2. Clause 6.2 provides a precise definition of "handover" and "consignment".

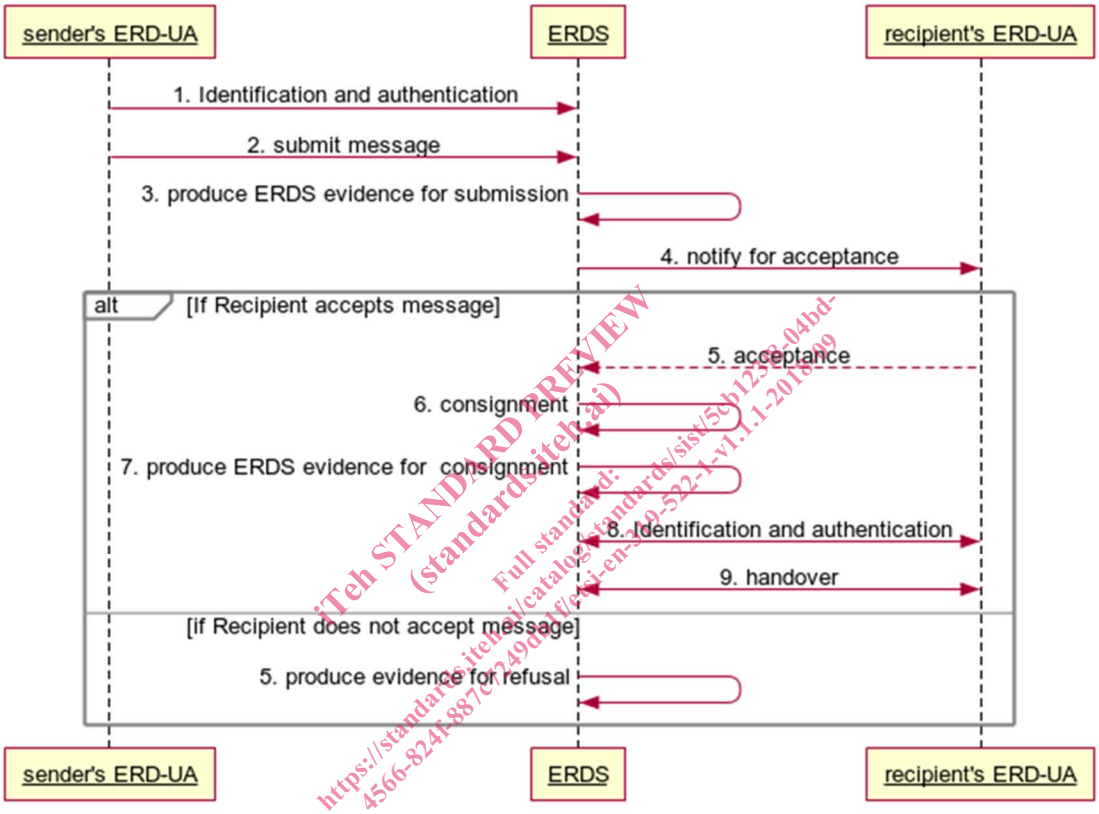

Figure 2: Black-box registered delivery basic flow

1. The sender is authenticated to the electronic registered delivery service. As mentioned above, identification and authentication can also be implemented through a trusted third party or identity federation (e.g. using OpenID Connect or SAML).
2. The sender's ERD-UA prepares the original message consisting of the user content, one or more recipients, and optionally some options on the requested registered delivery service (e.g. confidential, urgent, etc.), and submits it to the electronic registered delivery service. This step can in some case merge with step 1 (e.g. if the message is packaged together with an authentication token).
3. The electronic registered delivery service tracks the event that the original message has been submitted. This is done producing ERDS evidence ("attestation of submission"), which can take many forms as long as an attestation of the event can be extracted from the system.

Sometimes the ERDS evidence is sent back to the sender. This behaviour can be defined by a policy, or depends on a delivery option indicated by the sender. Independently from sending to the sender, the ERDS evidence can be stored for a certain amount of time by the system as specified in the service policy.

4. Optionally, a notification to the recipient (possibly on a separate channel) about the to-be-consigned user content can be sent, in a service-specific way that ensures confidentiality.