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

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 29 DECEMBER 2017

Download the template for comments:
https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

CAUTION: This DRAFT document is provided for information and is for future development work within the ETSI Technical Committee ESI only. ETSI and its Members accept no liability for any further use/implementation of this Specification. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at http://www.etsi.org/standards-search
Reproduction is only permitted for the purpose of standardization work undertaken within ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.
Intellectual Property Rights

4

Essential patents

IPRs essential or potentially essential to the present document 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

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 ESI and is now submitted for public review before approval by TC ESI and submission 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 3: "Bindings":
  - Sub-part 1: "Message delivery binding";
  - Sub-part 2: "Evidence and identification binding";
  - Sub-part 3: "Capability/requirements binding".

Proposed national transposition dates

<table>
<thead>
<tr>
<th>Proposed national transposition dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of latest announcement of this EN (doa):</td>
</tr>
<tr>
<td>Date of latest publication of new National Standard or endorsement of this EN (dop/e):</td>
</tr>
<tr>
<td>Date of withdrawal of any conflicting National Standard (dow):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3 months after ETSI publication</th>
<th>6 months after doa</th>
</tr>
</thead>
</table>

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.

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

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

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

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

Submission metadata: data submitted to the ERDS together with the user content.
ERDS relay metadata: data which is related to the user content which is generated by the ERDS for the purpose of relaying to another ERDS.

ERDS handover metadata: data which is related to the user content which is generated by the ERDS and handed over to the User Agent/Application.

ERDS evidence: data generated within/by the ERDS, which aims to prove that a certain event has occurred at a certain time.

ERD Event: a relevant step in the electronic delivery process, which may be attested by an ERDS evidence.

electronic registered delivery service: electronic service provided that makes possible to transmit data between third parties 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 unauthorised alterations.

EDITOR NOTE: THIS DEFINITION MAY NEED TO BE CHANGED

electronic registered delivery service provider: 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]

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

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

ERD user agent/application: 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 Message Submission Interface: Interface used by the sender's user agent/application to submit user content to sender's electronic registered delivery service.

ERDS Message and Evidence Retrieval Interface: interface of electronic registered delivery service used by ERD-user agent/application to retrieve data.

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

ERD Relay Interface: interface that supports ERD message relay between different ERDS

Consignment: The act of making the user content available to the recipient, within the boundaries of the ERDS

Handover: The act of having the user content successfully cross the R-ERDS border toward the recipient UA/Application.

3.3 Abbreviations

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

ERD: electronic registered delivery

ERDS: electronic registered delivery service

ERDSP: electronic registered delivery service provider

ERD-UA: electronic registered delivery user agent/application

ERDS MSI: ERDS Message Submission Interface

ERDS MERI: ERDS Message and Evidence Retrieval Interface.

ERD-UA MEPI: ERD-UA Message and Evidence Push Interface

ERDS RI: ERDS Relay Interface

I-ERDS: Intermediate ERDS

R-ERDS: Recipient’s ERDS

S-ERDS: Sender’s ERDS
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 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.

Secure and reliable delivery to a recipient requires that the recipient is uniquely identified. The present document also covers for the sender to be uniquely identified (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 identifies the actor. An important purpose of the present document is to support ERDS delivery between senders and receivers 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 receiver. The present document also addresses delegation, i.e. the capability for a recipient to delegate a different entity to act on the recipient’s behalf. To ensure that a message originates from the claimed sender, the sender is authenticated. To ensure that only the intended recipient(s) reads the message, the recipient is authenticated. 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 at providing 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.
- 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. The figure 1 below provides a simple representation.
ERDS services 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 original messages 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 a 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 evidences can be directed to different endpoints). Metadata extension points can be also used to identify different types of user content; in this case, user content belonging to different application layer protocols can be directed to different endpoints. (e.g. one endpoint for invoices and another endpoint for order).

- **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 the figure 2 below:
1. The sender’s ERD-UA is identified and authenticated to the electronic registered delivery service. As mentioned above, identification and authentication can also be implemented through a third party (e.g., using OpenID Connect or SAML).

2. The sender’s ERD-UA prepares user content, specifies one or more recipients, can dictate some options on the registered delivery service required (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 may 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.

5. Optionally, the recipient’s ERD-UA interacts with the ERDS to accept the consignment of the user content. Alternatively, the recipient needs not accept the consignment by not reacting or by explicit refusal. If the recipient rejects the user content, then the delivery process is aborted and the corresponding event is tracked by the service, otherwise the service tracks the notification event, and the delivery process is continued.

6. The consignment to the recipient(s) ERD-UA happens, meaning that the user content submitted by the sender is made available to the recipient(s) ERD-UA within the boundaries of the ERDS system, in a way that depends on the specific service implementation.
7. The electronic registered delivery service tracks the event that the user content has been made available to the recipient(s). Again, this is often done producing ERDS evidence (“attestation of consignment completed”). The attestation can be 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 attestation can also be stored for a certain amount of time by the system as specified in the service policy.

8. The recipient’s ERD-UA is identified and authenticated to the ERDS.

9. The user content is handed over to the recipient’s ERD-UA, meaning that the user content crosses the boundaries of the ERDS and reaches recipient’s ERD-UA. An ERDS evidence related to handover can be produced. Handover can also happen prior to consignment, or even in the absence of a consignment.

For the sake of simplicity, the flow ignores negative cases (failure in delivery, etc.) and different modes for consigning the user content to the recipient (e.g. push/pull, attached to the user content or separated from it), as well as other relevant events which can be tracked by the system. Only the core events “submission” and “consignment” have been explicitly tracked in the figure 2.

4.3. 4-corner model

4.3.1 Functional viewpoint

In many practical cases the sender and the recipient are subscribed to different ERDSs. In that case, when the sender’s ERDS does not have the capability to directly deliver the user content to the recipient, it can have the option to relay to a different ERDS which has this capability. This gives rise to a new scenario, which is presented in the figure 3 below.

In this scenario, the sender’s ERDS can produce the required ERDS evidence attesting the consignment only when the recipient’s ERDS completes its job and notifies the completion to the sender’s ERDS. This is rendered in figure 3 by the backward “ERDS Object relay” arrow, which is a notification of the completed tasks. The arrow is logical, since these ERDS evidences are not necessarily pushed back as separate messages, as far as they are available to the sender’s ERDS.

This scenario implies some shared background to work. Contractual agreements will usually be needed, either directly between the ERDSPs or by the ERDSPs entering an agreement that includes them in some kind of community. Service can be provided based on common static configurations, or can require a shared technological infrastructure.
Functions provided by the shared technological infrastructure can include:

- **Message routing.** The sender’s ERDS needs to know which ERDS (or ERDSs) can deliver to the recipient. In some cases, this information is embedded in the recipient’s electronic identifier (e.g. in e-mail messaging, john.doe@acme.com already contains routing information). In the general case, the association of the recipient’s electronic identifier to the recipient’s ERDS is provided by a shared infrastructure. The infrastructure can consist of a centralized directory, a distributed ledger, DNS entries, etc.

- **Trust establishment:** the sending ERDS needs to provide ERDS evidence about the delivery of the message, on which it has no control. It can however provide such ERDS evidence on the basis of a trust relationship with the recipient’s ERDS. Similarly, the recipient’s ERDS needs to trust the sender’s ERDS for producing ERDS evidence about the sending of the message.

- **Capability management.** The sender’s ERDS needs to know whether the recipient’s ERDS has the technical capabilities for interactions: it implements a common transport protocol, it deals with the required ERDS evidence, it provides user authentication at the appropriate level, etc. In closed environments, these issues are normally solved by prior off-line information sharing, while in open environments, ERDSs can dynamically expose the information (e.g. via a WSDL, Service Metadata Publishing), possibly on a shared infrastructure.

- **Governance support:** some general governance functions can be in place to deal with incident management, Service Level Agreement monitoring, configuration management, accounting and similar governance functions.

In a multi-ERDS delivery scenario, some components which are normally implemented by an ERDS (dotted boxes in the figure) can be moved to the shared infrastructure, like for instance: shared user directory and a shared ERDS evidence directory. Functions provided by the shared infrastructure need not necessarily be provided by a distinct central service; they can be individually provided by the same ERDSs (for instance in the case of capability functions) or by a distributed infrastructure whose nodes are run by the same ERDSPs providing the ERDS services.

### 4.3.2 Sequence viewpoint

While the user experience is that of an opaque black-box, the reality behind a 4-corner electronic registered delivery service is often made of several interacting domains, operated by different providers. In this case the typical sequence diagram appears as follows in figure 4:

---

**Figure 4: 4-Corner electronic registered delivery basic flow**
Differently from Figure 3, for a simplified reading the production of attestations has been removed from the figure, as well as negative cases (failure, non-acceptance) and other events. It is however assumed that any significant event has an associated attestation.

1 and 2. Message submission, as in steps 1 and 2 of the black-box model.

3. Sender’s ERDS (S-ERDS) needs to identify recipient’s ERDS (R-ERDS). In the general case, this happens through a common infrastructure (Common). This is an abstract entity, which can correspond to several distinct actors. S-ERDS needs to:
   - Identify R-ERDS: this can involve lookup to a centralized or distributed registry (e.g., DNS).
   - Establish trustworthiness of R-ERDS, possibly checking against a trust information provider such as a Trust Status List (in a restricted network, peer-to-peer agreements can be established with no central trust information provider). Since trust networks are normally stable over long time periods and not changing frequently, the process does not necessarily involve an on-line transaction.

4. Handshake with R-ERDS. This can include negotiation on different aspects (supported formats, protocols, ERDS evidence, strength of authentication of end entities, fees, etc.). Handshake needs not be necessary in closed systems where this information is defined a priori or available through a centralised infrastructure.

5. The message is relayed to R-ERDS (in case of more recipients, the message is dispatched to the respective R-ERDS). S-ERDS can add some meta-information to the message.

6. R-ERDS can check, on its turn, trustworthiness of S-ERDS via Common. This step can happen before the message relay, or even at a different time unrelated to the message delivery flow (e.g., once a day), according to the service policy.

7., 8, 9, 11, and 12., consignment and handover to the recipient’s ERD-UA, as in the respective steps of the black-box model

10 and 13. R-ERDS needs to inform S-ERDS about the successful consignment and handover of the user content to the recipient. Since the information comes from a trusted party, S-ERDS has the necessary elements to attest the consignment and handover to the recipient.

4.4 Extended model

4.4.1 Functional viewpoint

In a more general scenario, the delivery process can go through several chained ERDSs, as presented in the figure 5 below.
The scenario extends the previous one. The sender’s ERDS produces ERDS evidence of the delivery process on the base of the trusted information it gets (either directly, though a repository, or mediated by intermediate ERDSs) from the last ERDS in the chain. Intermediate nodes implement data/ERDS evidence trusted relay. They can also implement additional functionalities like:

- protocol gateway
- data/ERDS evidence validation
- data/ERDS evidence repository

### 4.4.2 Sequence viewpoint

In this case the sequence diagram would be extended as follows in figure 6.
Figure 6: Extended electronic registered delivery basic flow
It appears that, while the users still perceive the service as a black-box, several interactions take place in between. The sample flow introduces Intermediate ERDS 1 (1-ERDS) and Intermediate ERDS 2 (2-ERDS). Nodes can be either transparent (acting as message relay) or non-transparent, providing extra services like semantic conversion, signature validation, business workflow, etc.

In the sample flow different ERDSs interact via different Commons: CommonS1 is the shared infrastructure between S-ERDS and 1-ERDS, etc. This is the case when intermediate ERDSs act as gateway between different administrative/trust domains.

In steps 18, 19, 20, 23, 24, 25 the ERDS evidence of delivery flows back across the different ERDSs, since each of them needs to close their own transaction.

5 ERDS interfaces

The figure 7 presents the interfaces which emerge from the above models. The 4-corner model has been considered since it contains all the elements, while the extended model is a straightforward generalization.

**Figure 7: Interfaces**

**ERDS MSI: Message Submission Interface:** this interface is used by the sender’s ERD-UA to submit original messages to the sender’s ERDS, for them to be forwarded to the recipient(s). This interface shall require identification and authentication, either direct (e.g. through credential check) or indirect (e.g. though a token from a third party). This interface shall implement confidentiality and integrity preserving measures.

**ERDS MERI: Message and Evidence Retrieval Interface:** this interface is used to retrieve user content and the associated evidence. This interface shall require identification and authentication, either direct (e.g. through credential check) or indirect (e.g. though a token from a third party). This interface shall implement confidentiality and integrity preserving measures.
ERD-UA MEPI: Message and Evidence Push Interface: this interface is used to push user content and the associated evidence to the ERD-UA. This interface shall implement confidentiality and integrity preserving measures.

ERDS RI: Relay Interface: this interface allows ERD messages to be relayed between ERDS. This interface shall implement confidentiality and integrity preserving measures.

- CSI: Common Service Interface: this interface gives access to message routing functions, trust management functions, capability management functions, governance functions.

An ERDS shall implement ERDS MSI, ERDS MERI. These interfaces are not further specified in any part of EN 319 522.

NOTE: While standardization of interfaces ERDS MSI and ERDS MERI does not affect interoperability between different ERDS, it can however be relevant for easing the user when switching from a provider to another, especially when an application interface is involved.

An ERDS shall implement ERDS RI. It should implement ERDS RI according to the EN 319 522 parts 3 and 4 [1], [2].

An ERDS should use CSI.

6 ERDS events and evidence set

6.1 Overview

This clause describes in detail the ERDS events which may happen within an electronic delivery process and which may be relevant from a probative perspective. Other events related to the interaction with non ERDSs have been considered as well.
Table 1: ERDS Events

<table>
<thead>
<tr>
<th>N.</th>
<th>Event</th>
<th>Primary issuer of associated ERDS evidence</th>
<th>Primary target of ERDS evidence</th>
<th>ERDS event status</th>
<th>ERDS evidence status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Events related to S-ERDS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A.1 SubmissionAcceptance</td>
<td>S-ERDS</td>
<td>Sender</td>
<td>C (either A.1 or A.2 shall take place)</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>A.2 SubmissionRejection</td>
<td>S-ERDS</td>
<td>Sender</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Events related to the relay between ERDSs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>B.1 RelayAcceptance</td>
<td>Relayed ERDS</td>
<td>Relaying ERDS</td>
<td>C (in case of inter-ERDS messaging either B.1, B.2 or B.3 shall take place)</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>B.2 RelayRejection</td>
<td>Relayed ERDS</td>
<td>Relaying ERDS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>B.3 RelayFailure</td>
<td>Relaying ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Events related to the acceptance/rejection by recipient</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C.1 NotificationForAcceptance</td>
<td>R-ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>C.2 NotificationForAcceptanceFailure</td>
<td>R-ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>C.3 ConsignmentAcceptance</td>
<td>Notifying ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>C.4 ConsignmentRejection</td>
<td>Notifying ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>C.5 AcceptanceRejectionExpiry</td>
<td>Notifying ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>Events related to the consignment to recipient</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>D.1 ContentConsignment</td>
<td>R-ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>C (either D.1 or D2 shall take place if neither E.1 and E.2 take place)</td>
<td>M</td>
</tr>
<tr>
<td></td>
<td>D.2 ContentConsignmentFailure</td>
<td>R-ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>D.3 ConsignmentNotification</td>
<td>R-ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td>D.4 ConsignmentNotificationFailure</td>
<td>R-ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td></td>
<td>Events related to the handover to the recipient</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E.1 ContentHandover</td>
<td>R-ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>C (either E.1 or E.2 shall take place if neither D.1 and D.2 take place)</td>
<td>C (if no evidence on D.1 or D.2 had been produced)</td>
</tr>
<tr>
<td></td>
<td>E.2 ContentHandoverFailure</td>
<td>R-ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Events related to the connections with non ERD systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>F.1 RelayToNonERDS</td>
<td>Relaying ERDS</td>
<td>Relaying ERDS</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>F.2 RelayToNonERDSFailure</td>
<td>Relaying ERDS</td>
<td>Sender/previous ERDS in the delivery chain</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>F.3 ReceivedFromNonERDS</td>
<td>Relayed ERDS</td>
<td>Recipient/next ERDS in the delivery chain</td>
<td>O</td>
<td>R</td>
</tr>
</tbody>
</table>
On the occurrence of an ERDS events, an ERDS produces an ERDS evidence, which will contain a reference to the event as detailed in ETSI EN 319 522-2 [1]. The table 1 identifies:

- the event which triggers the production of an evidence
- the primary issuer of the evidence which is produced. This corresponds to the ERDS which witnesses the occurrence of the event
- the primary target for the evidence. The target specifies the expected consumer of the evidence. The evidence shall be made accessible to the target consumer. There is no obligation that the evidence is pushed to the target; it may suffice that the evidence is stored in such a way that it is accessible to the target on necessity.

- The status of the event:
  - “M” (mandatory) means that the event shall take place;
  - “C” (conditional) means that the event shall take place under the condition which is expressed in the table;
  - “R” means that the event should take place;
  - “O” means that the event may take place;

- The requirement on the production of the evidence:
  - “M” (mandatory) means that the evidence shall be produced whenever the corresponding event takes place;
  - “C” (conditional mandatory) means that the evidence shall be produced place under the condition which is expressed in the table;
  - “R” means that an evidence should be produced whenever the corresponding event takes place;
  - “O” means that an evidence may be produced whenever the corresponding event takes place.

### 6.2 Events and their Proof

#### 6.2.1 A. Events related to S-ERDS

**A.1. Submission Acceptance**

- The user content was successfully submitted to the S-ERDS by the sender
- The related evidence attests that the sender, suitably authenticated according to the details indicated in the evidence, has successfully submitted, at the time indicated in the evidence itself, a user content to the ERDS provider and that the ERDS provider has accepted to perform the required tasks for trying to deliver it to the intended recipient(s).

**A.2. Submission Rejection**

- The user content that was submitted to the S-ERDS by the sender was not accepted by the S-ERDS.
- The related evidence attests that the sender, suitably authenticated according to the details indicated in the evidence, has submitted, at the time indicated in the evidence itself, a user content to the ERDS provider and that the ERDS provider has rejected to perform the required tasks for trying to deliver it to the intended recipient(s).
6.2.2 B. Events related to the relay between ERDSs

B.1. Relay Acceptance

- One ERD message sent by the relaying ERDS and successfully received by the relayed ERDS, was accepted by the latter.

- The related evidence attests that, in situations where several ERDSs are co-operating for jointly offering the ERD service, an intermediate or the recipient's ERDS has accepted one ERD message sent by the previous ERDS in the aforementioned chain.

B.2. Relay Rejection

- One ERD Object sent by the relaying ERDS and successfully received by the relayed ERDS, was rejected by the latter due to policy, formal or technical reasons.

- The related evidence attests that, in situations where several ERDSs are co-operating for jointly offering the ERD service, an intermediate or the recipient's ERDS, at the time specified by the evidence, has rejected one ERD message sent by the previous ERDS in the aforementioned chain.

B.3. Relay Failure

- It was impossible to relay within a given time period an ERD Object to the target ERDS due to technical errors and/or other problems.

NOTE: This can depend on:

a) impossibility for relaying ERDS to identify the appropriate target to-be-relayed ERDS;

b) target ERDS is unreachable;

c) target ERDS rejected the communication without providing a reason.

- The related evidence attests that, at the time specified in the evidence, it was impossible to deliver an ERD message within a given time period to either an intermediate ERDS provider or to the recipient's ERDS provider due to technical errors and/or other problems.

6.2.3 C. Events related to the acceptance/rejection by recipient

C.1. Notification For Acceptance

- R-ERDS notified the recipient about the availability of a message (without necessarily disclosing its sender, content, etc.) and asked for the recipient’s willingness to accept it.

- The related evidence attests that a notification requesting the acceptance of a message has been sent to a recipient at a specific time as indicated by the evidence. The evidence may not attest that the notification reached the recipient.

C.2. Notification For Acceptance Failure:

- The recipient could not be notified within a given time period due to technical errors and/or other reasons or no proof of notification within a given period exists.

The time limit is fixed by statutory or contractual rules, or it is pre-defined by the sender, or determined by the policy of the R-ERDS.

- The related evidence attests that, a notification requesting the acceptance of a message could not be sent to the specified recipient after a certain number of attempts or a timeout as specified by the applicable policies.
C.3. ConsignmentAcceptance

- The recipient performed an explicit action by indicating to the ERDS which issued the notification the acceptance to receive a user content.

- The related evidence attests that the recipient, upon proper identification and authentication, at the time indicated by the evidence accepted to receive some user content from a sending party. The information which is made available to the recipient to decide upon accept/reject is specific to the ERDS policy.

C.4. ConsignmentRejection

- The recipient, upon proper identification and authentication, performed an explicit action indicating to the R-ERDS the rejection to receive a user content

- The related evidence attests that the recipient, upon proper identification and authentication, at the time indicated by the evidence rejected to receive some user content from a sending party. The information which is made available to the recipient to decide upon accept/reject is specific to the ERDS policy.

C.5. AcceptanceRejectionExpiry

- The ERDS sent a notification to the recipient, but they did not react to the notification with an acceptance/rejection.

- The related evidence attests that the recipient, by the time indicated by the evidence did not react to the request to accept/reject to receive some user content from a sending party within a defined time period. This time period can be determined by legislation, R-ERDS policy rules, or parameters given by the sender or by the S-ERDS.

6.2.4 D. Events related to the consignment to Recipient

D.1. ContentConsignment

- The user content was made available to the recipient within the boundaries of the ERDS.

- The related evidence attests that, the ERD message, at a specific time indicated by the evidence, was made available for the recipient - through proper identification and authentication - within the boundaries of the ERDS.

D.2. ContentConsignmentFailure

- The user content could not be made available to the recipient within a given time period due to technical errors and/or other reasons or no proof of delivery within a given period exists.

- The related evidence attests that the ERD message could not be made available to the recipient within a given time period. The issuance of this evidence may be triggered by different events:

  - The recipient's ERDS was not able to consign the user content to the recipient. In this case the evidence is produced by the R-ERDS.

  - A relaying ERDS did not receive within a given time period from the relayed ERDS an evidence of successful consignment. In this case it is the relaying ERDS that creates the evidence with the suitable reason code.

D.3. ConsignmentNotification

- A notification was sent to recipient (on a non-specified channel) about the availability of the consigned message.
- The related evidence attests that a notification about the availability of the consigned message has been sent to a recipient at a specific time as indicated by the evidence. The evidence may not attest that the notification reached the recipient.

D.4. ConsignmentNotificationFailure
- An attempt to notify the recipient about the availability of the user content failed.
- The related evidence attests that a notification about the availability of the consigned user content could not be sent to the specified recipient after a certain number of attempts or a timeout as specified by the applicable policies.

6.2.5 E. Events related to the handover to the recipient

E.1. ContentHandover
- The user content successfully crossed the R-ERDS border toward the recipient UA/Application. The event may indicate either a “pull” (i.e. the UA/Application proactively retrieved the message from the R-ERDS) or a “push” (the message was successfully pushed by the R-ERDS to the UA/Application).
- The related evidence attests that the user content at a specific time indicated by the evidence crossed the R-ERDS border and was handed to the recipient UA/Application upon proper authentication.

E.2. ContentHandoverFailure
- The user content could not cross the R-ERDS border toward the recipient UA/Application. In the “pull” case (i.e. when the UA/Application has to proactively retrieve the message from the R-ERDS), this event indicates that the message was not retrieved within a given period due to technical errors and/or other reasons.
- The related evidence attests that the user content could not cross the R-ERDS border toward the recipient’s ERD-UA after a certain number of attempts or a timeout as specified by the applicable policies.

6.2.6 F. Events related to connections with non ERD systems

F.1. RelayToNonERDS
- A certain message was successfully forwarded to a non ERDS system for delivery.
- The related evidence attests that, a certain ERD message was successfully forwarded to a non ERDS system at the time indicated in the evidence.

F.2. RelayToNonERDSFailure
- The attempt to relay a message to a non ERDS system failed due to technical errors and/or other reasons.
- The related evidence attests that, a certain ERD message failed to be forwarded to a non ERDS system at the time indicated in the evidence.

F.3. ReceivedFromNonERDS
- A certain message was received from a non ERDS, therefore all information related to its sending, like the sender's identifier and the sending time, cannot be trusted per se.
- The related evidence attests that a certain message was not received from an ERDS but from a non ERDS external system, therefore all information on message origin is not per se trustable.
Annex A (informative):
Services and providers related to ERD

EDITOR NOTE: The informative material contained in this annex is still under discussion and is subject to changes.

An electronic registered delivery service (ERDS) is generally understood to be a 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 the transmitted data against the risk of loss, theft, damage or any unauthorised alterations. An electronic registered delivery service provider (ERDSP) is a legal entity which provides ERDS. The ERDSP is usually an organization, and it is responsible for the correctness of operations and issued evidence. The users of the service are usually clients or subscribers of only one of the ERDSPs, and they can send and receive data communicating only through their chosen service provider.

Each ERDSP can implement the communication between its own subscribers internally. In real life scenarios the users also need to communicate with the subscribers of other service providers. The ERDSPs can collaborate to allow exchange of messages among all their subscribers. However, they need to make some extra effort in order to achieve this, e.g. they need to interconnect their systems, establish routing and trust relationships, etc. In the end, through all these measures they can provide a higher level of service: electronic registered delivery reaching the clients of multiple providers.

The concept of ERDS can be interpreted in two different ways.

a) From the user’s point of view the service is provided by the collaboration of multiple ERDSPs. It works just like international phone calls: when a user in Rome calls a phone number in Oslo, they do not need to know which operator that number belongs to and which countries the call will go through. Similarly, when the sender submits a message through a registered delivery service, they will receive proof of sending and receipt of that message, regardless of which service providers were involved in the performance of the service. Henceforth, this is called an electronic registered delivery end-to-end service.

b) From a compliance point of view there are certain requirements a service must fulfil in order to be considered an electronic registered delivery service. These requirements are formulated so that they apply to one single ERDSP. (Otherwise, conformance assessment would not be feasible.) Henceforth, the service provided by one single ERDSP is called an electronic registered delivery service.

In general, the service provided by one single ERDSP can perform one or more of 3 roles in the delivery process:

1) Sender’s ERDS (S-ERDS): this component service is responsible for allowing the submission of the message for the sender, with proper tracking of this event. It is also responsible for forwarding the message to the next actor, as appropriate.

2) Intermediate ERDS (I-ERDS): this component service is responsible for receiving a forwarded message and forwarding it again according to the routing rules established in the collaboration of service providers, with proper tracking of the relevant events. Multiple I-ERDS components can participate in the delivery of a particular message.

3) Recipient’s ERDS (R-ERDS): this component service is responsible for receiving a forwarded message and delivering it to the recipient, with proper tracking of the relevant events.

In special cases, some roles can be omitted or can be combined into one. When the S-ERDS and R-ERDS can communicate directly then I-ERDS is not needed. When the sender and recipient are subscribers of the same ERDSP then the ERDS provided by that ERDSP can perform the roles of both S-ERDS and R-ERDS, and there is no need for forwarding the message at all.
Figure 1 shows an example where the sender and the recipient are subscribers of different ERDSPs, and the registered message is transferred through a third ERDSP as well.

Figure 1: Services and providers related to ERD

Notations used in the figure:

- In figure 1 the grey boxes represent the service providers (ERDSPs). They might also provide other services beside ERDS, but that is not shown in the figure.
- Each green box inside a grey box represents the service provided by the enclosing ERDSP. The green boxes correspond to the interpretation b) of the ERDS concept as described above (from a compliance point of view).
- The outer red box, enclosing all three green boxes, represents the electronic registered delivery end-to-end service. This corresponds to the interpretation a) of the ERDS concept as described above (from the user’s point of view).
- The red arrows represent the external interface of the ERD end-to-end service, as it is perceived by the users.
- The green arrows represent the interface of the ERDS provided by one single provider. The figure illustrates that this interface involves communication with the users, and also communication between the service providers.

In the context of EU legislation, Regulation (EU) No 910/2014 [i.1] defines the terms ‘electronic registered delivery service’ and ‘qualified electronic registered delivery service’, and specifies requirements for the latter. The Regulation mentions the possibility of more than one provider participating in the provision of the service, but does not give any stipulations regarding the possible different interpretations of the ERDS concept, as described above. However, the requirements for a ‘qualified electronic registered delivery service’ include identification of the sender and addressee (recipient). In a general scenario, such as the one illustrated in figure 1, these requirements cannot be met by any single provider alone, but they can be fulfilled by the collaboration of the ERDSPs. In consequence, in such a multi-provider scenario, the ERD end-to-end service, as defined in interpretation a) above, could be able to satisfy the requirements of a ‘qualified electronic registered delivery service’ according to the Regulation.

In the present document, henceforth, the term ‘electronic registered delivery service’ and the acronym ‘ERDS’ are used solely in the sense of interpretation b) as described above, meaning the service provided by one single ERDSP.
## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.1</td>
</tr>
<tr>
<td>0.0.2</td>
</tr>
<tr>
<td>0.0.3</td>
</tr>
<tr>
<td>0.0.4</td>
</tr>
</tbody>
</table>