ETSI EN 319 522-1 V1.1.1 (2018-09)

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 European Standard (EN) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

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".

National transposition dates	
Date of adoption of this EN:	23 August 2018
Date of latest announcement of this EN (doa):	30 November 2018
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 May 2019
Date of withdrawal of any conflicting National Standard (dow):	31 May 2019

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.

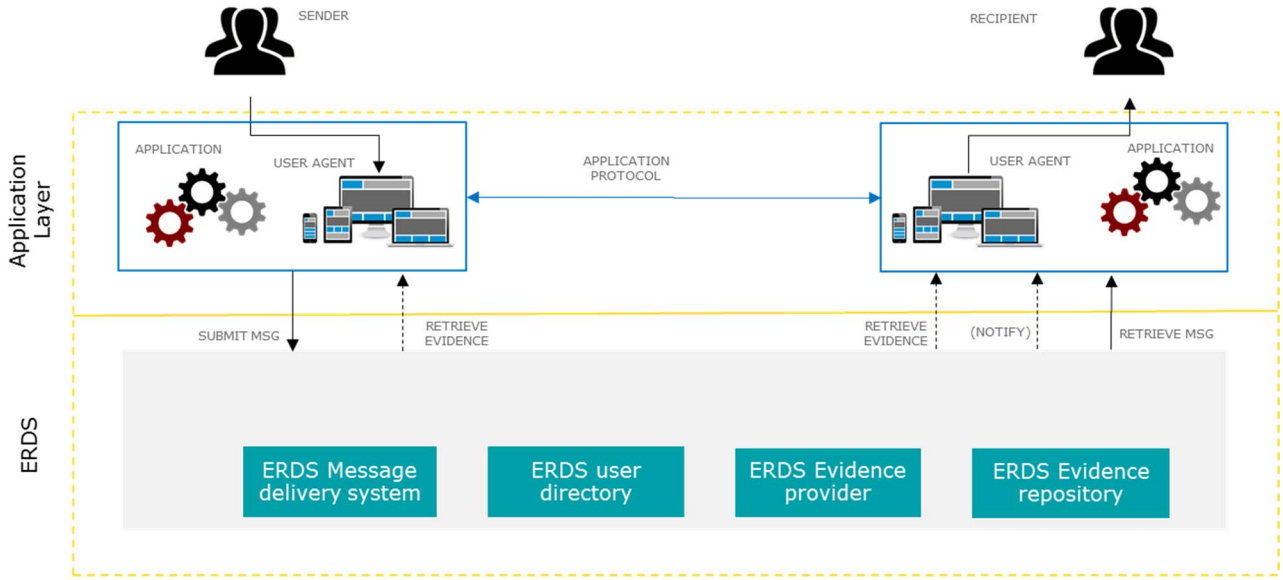

Figure 1: Black-box registered delivery service model

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".

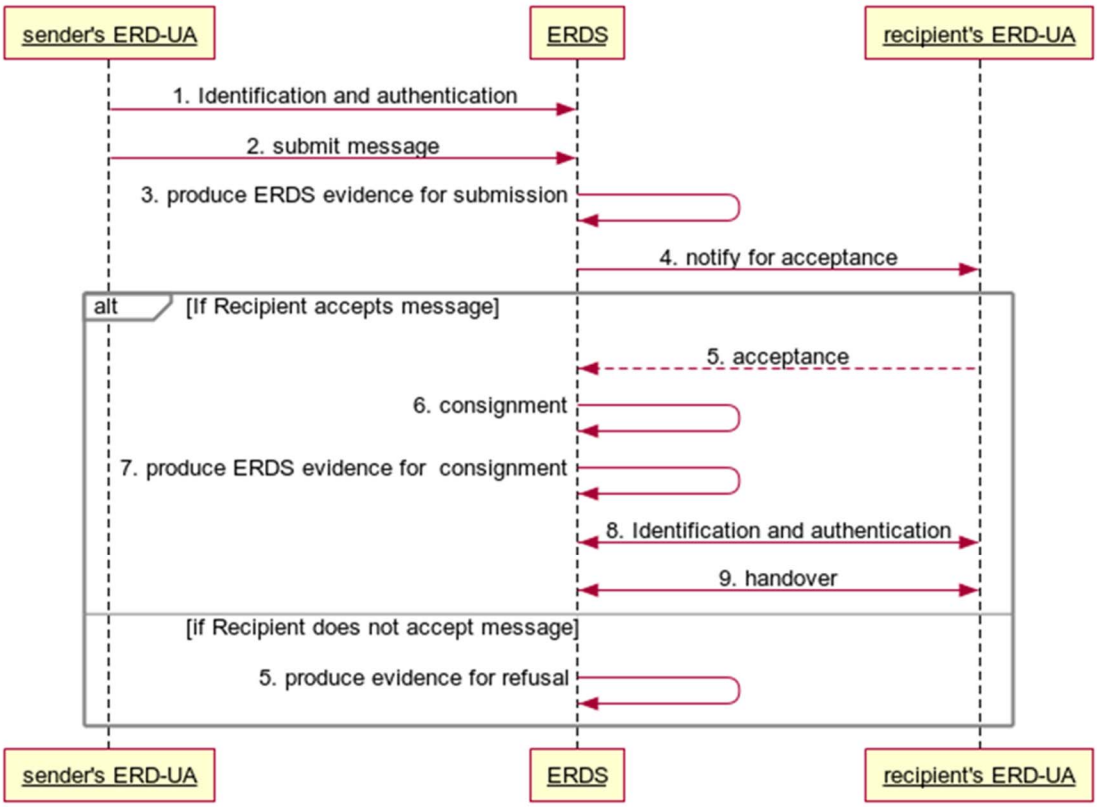

Figure 2: Black-box registered delivery basic flow

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.

5. Optionally, the recipient's ERD-UA interacts with the ERDS to accept the consignment of the user content. Alternatively, the recipient does 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) 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 is 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, in a service-specific way that ensures confidentiality. 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 handing over the user content to the recipient (e.g. push/pull, with evidence 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 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 figure 3.

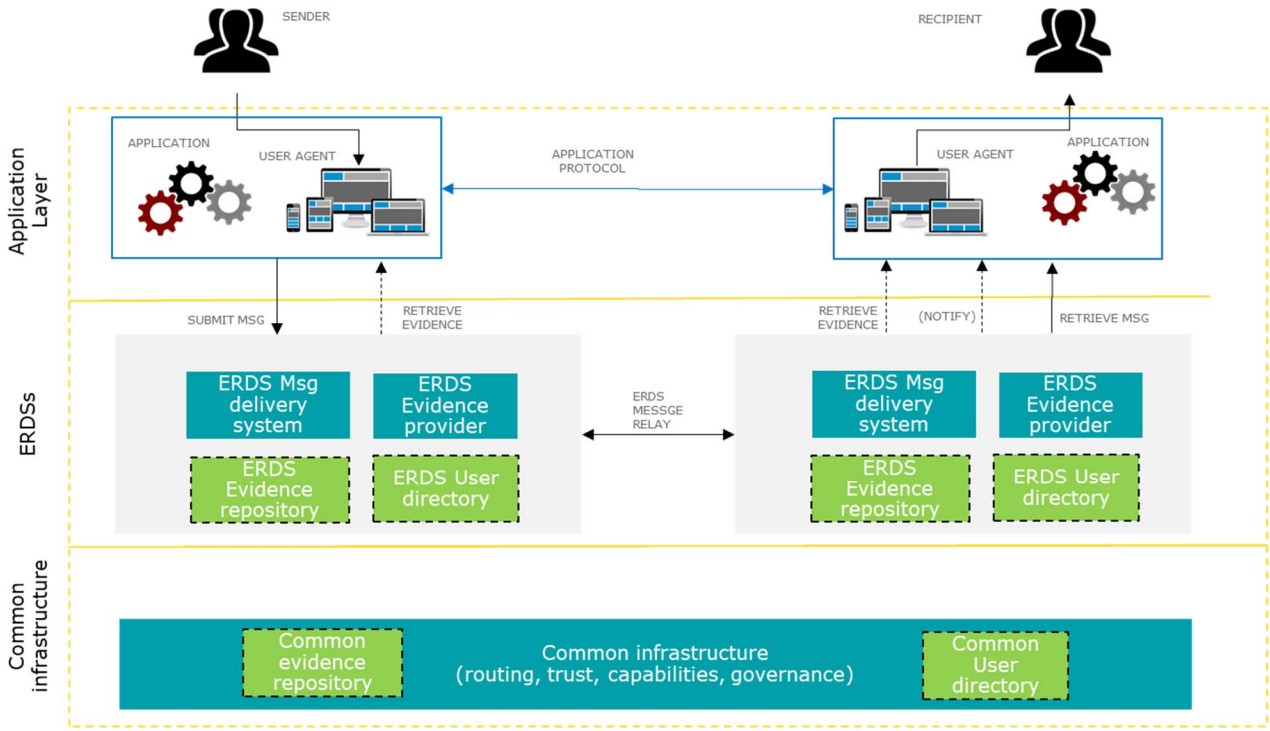

Figure 3: 4-Corner electronic registered delivery service model

In this scenario, the sender's ERDS can inform the sender about the consignment only when the recipient's ERDS has completed its job and has notified the completion to the sender's ERDS. This is rendered in figure 3 by the backward direction of the "ERDS message relay" arrow, which is a notification of the completed tasks. The arrow represents only a logical transfer, since ERDS evidence is not necessarily pushed back as separate messages, as far as it is 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 may depend on other metadata and be supported by a shared infrastructure. The infrastructure can consist of a centralized directory, a distributed ledger, DNS entries, etc.

- **Trust establishment:** to entrust the message to its counterpart, the sender's ERDS needs to rest assured that it will properly manage it. A trust relation with the recipient's ERDS will also enable the sender's ERDS to provide ERDS evidence about the delivery of the message, on which it has no control. Similarly, the recipient's ERDS needs to trust the sender's ERDS for producing ERDS evidence about the provenance 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, liability management and similar governance functions.

In a multi-ERDS delivery scenario, some components which are normally implemented by an ERDS (dotted boxes in figure 3) 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 the same as for the black-box model, the reality behind a 4-corner electronic registered delivery service is more complex due to the number of actors involved, operated by different providers. In this case the typical sequence diagram appears as follows in figure 4.

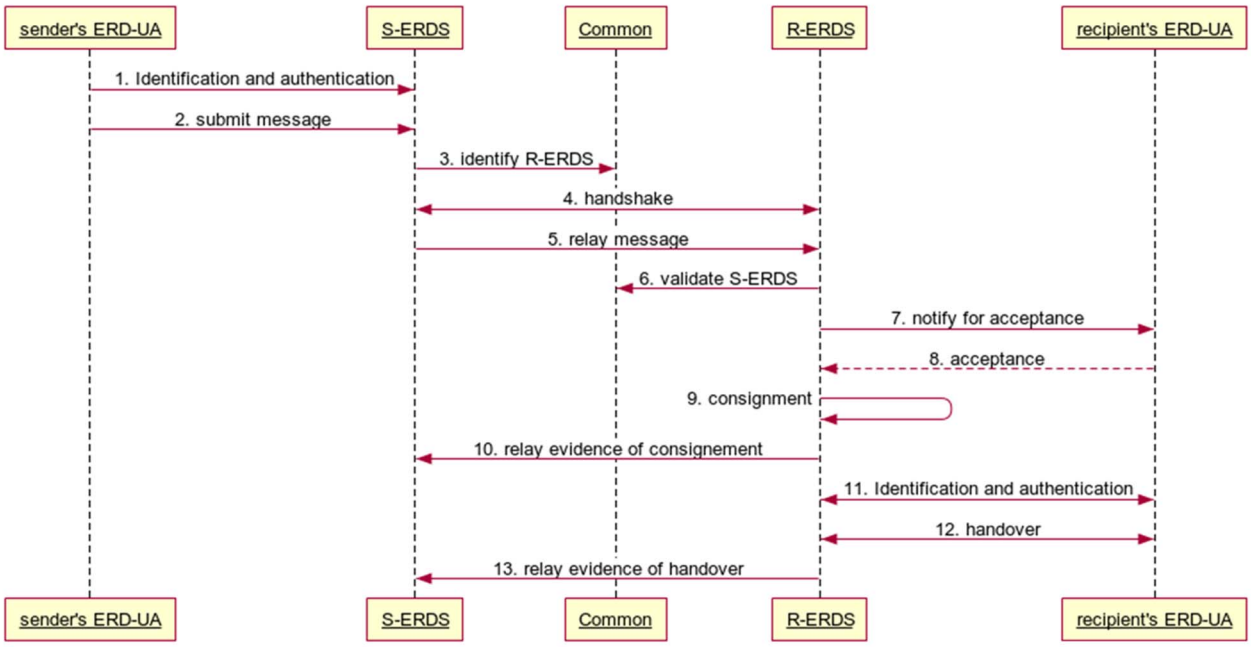

Figure 4: 4-Corner electronic registered delivery basic flow

Contrary to 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 determine the 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:

   - Determine 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 do not change 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 can be omitted in closed systems where this information is defined a priori or available through a centralized infrastructure.

5. The message is relayed to the 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. The R-ERDS can check, on its turn, trustworthiness of S-ERDS via Common. This step happens 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. The 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. The diagram hints at evidence flowing back to the S-ERDS for illustration purposes. As better specified in clause 6, the requirement is that evidence is produced and made available to S-ERDS.

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 figure 5.

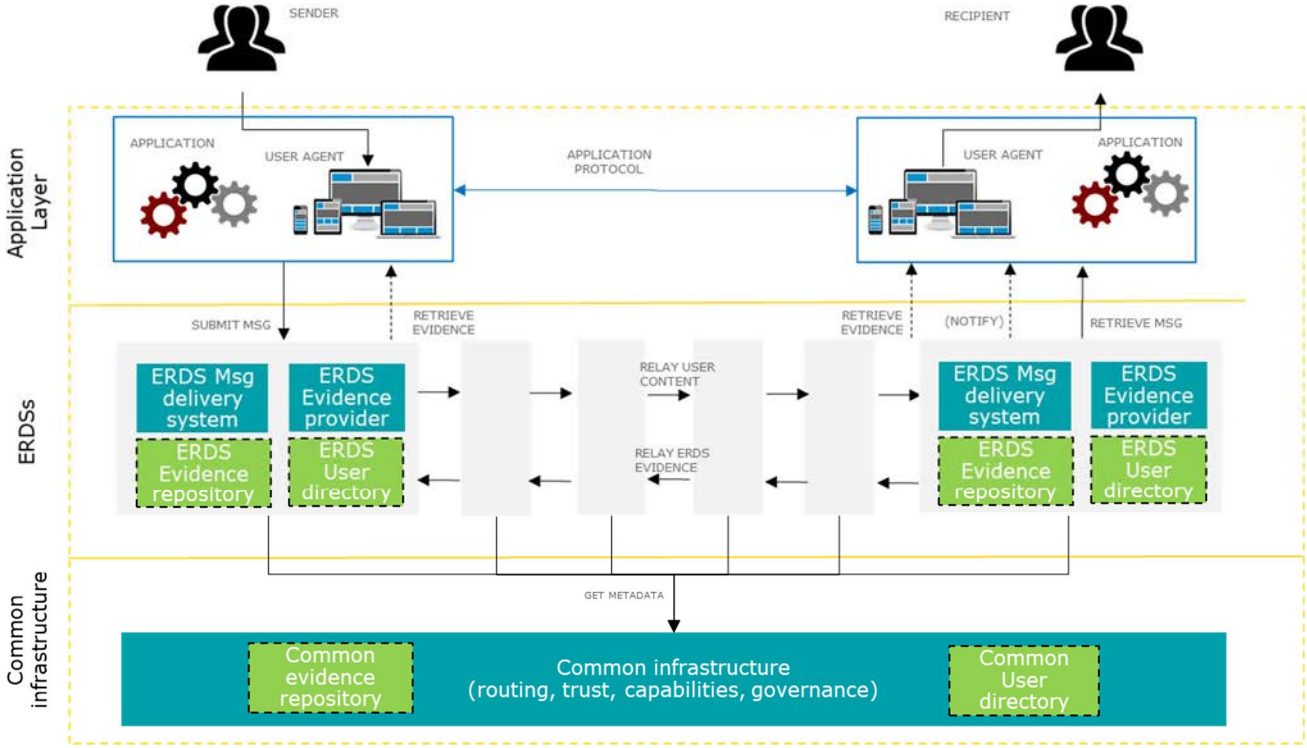

Figure 5: Extended electronic registered delivery service model

The scenario extends the previous one. The sender's ERDS informs the sender about the outcome of the delivery process on the base of the trusted information it gets (either directly, through 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.

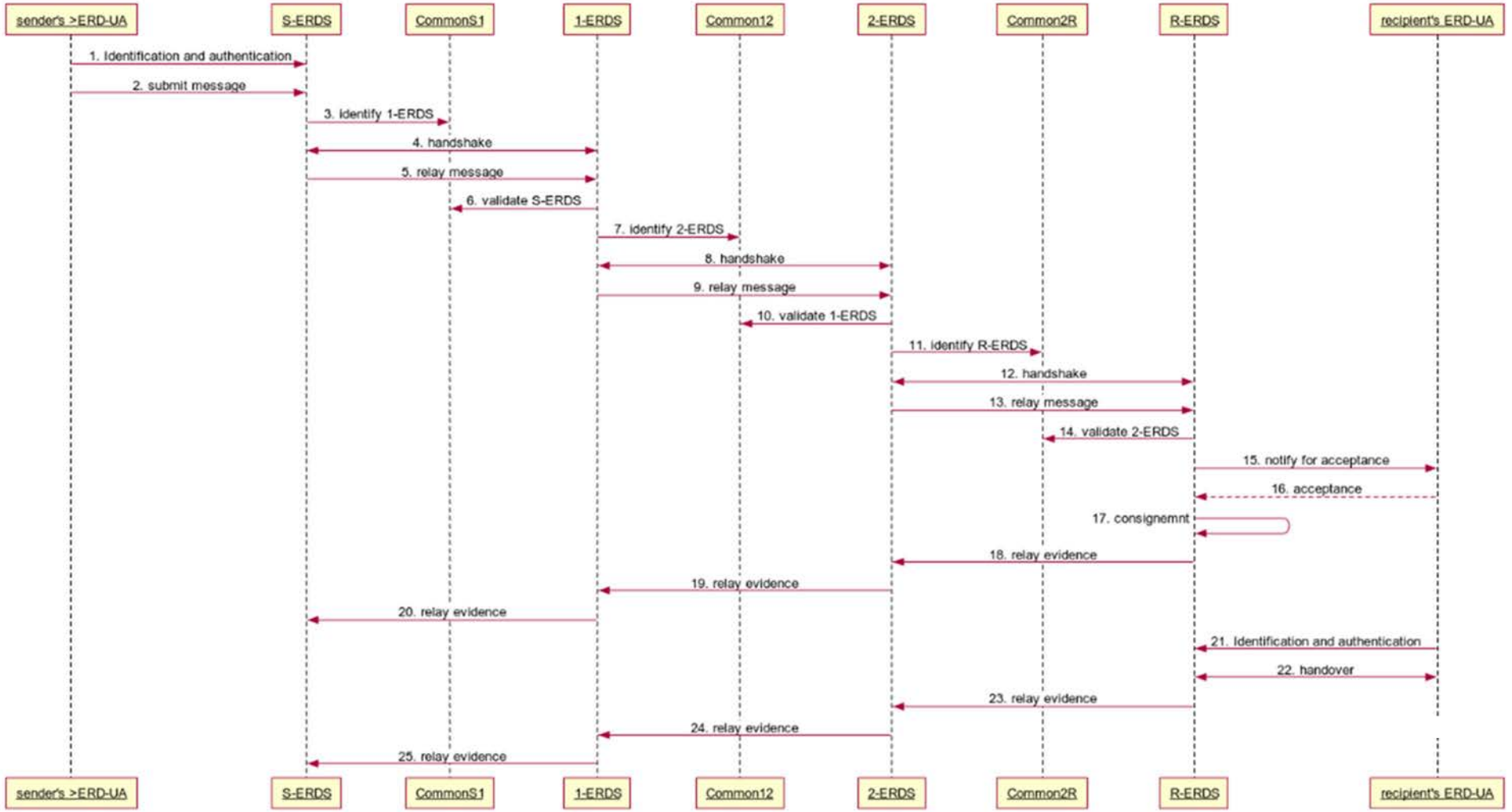

Figure 6: Extended electronic registered delivery basic flow

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). Single ERDSs only support transparent relay of messages. This architecture, however, also supports non-transparent relay, enabling extra services like semantic conversion, signature validation, business workflow, etc. In this case an application layer on top of the ERDSs will be in charge (and assume the liability) of message transformation.

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 and 25 the ERDS evidence of consignment and handover flows back across the different ERDSs, since each of them needs to close their own transaction.

5 ERDS interfaces

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.

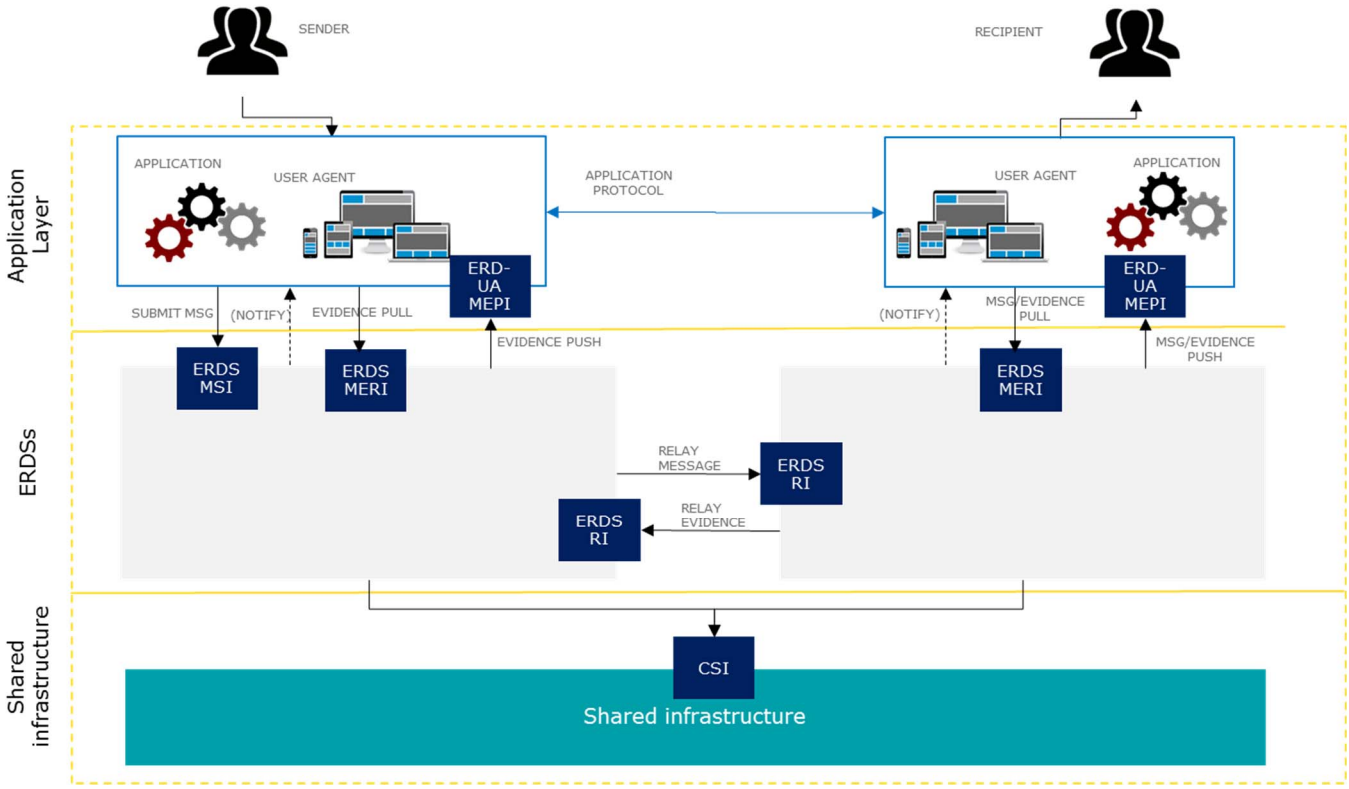

Figure 7: Interfaces

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 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 by the ERD-UA to retrieve user content, handover metadata and associated evidence (pull mode). This interface shall require 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/or associated evidence to the ERD-UA. This interface shall implement authentication, confidentiality and integrity preserving measures.

ERDS RI(Relay Interface): this interface allows ERD messages to be relayed between ERDS. This interface shall implement authentication, 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, and either ERDS MERI or ERDS MEPI (or both). These interfaces are not further specified in any part of this multi-part deliverable.

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 interoperable ERDS shall implement ERDS RI. It should implement ERDS RI according to the ETSI EN 319 522 parts 3 [i.6], 4-1 [i.7] and 4-2 [i.8].

An interoperable 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.

On the occurrence of an ERDS event, an ERDS may produce an ERDS evidence, which will contain a reference to the event as detailed in ETSI EN 319 522-2 [i.5]. This is one of the main differences with non-repudiation tokens defined in ISO/IEC 13888 [i.2], [i.3] and [i.4].

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 (but not necessarily exclusive) consumer of the evidence. Any produced 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.

Table 1: ERDS Events

N.	Event	Primary issuer of associated ERDS evidence	Primary target of ERDS evidence	ERDS event status	ERDS evidence status
Events related to the submission					
A.1	SubmissionAcceptance	S-ERDS	Sender	C (either A.1 or A.2 shall take place)	M
A.2	SubmissionRejection	S-ERDS	Sender		
Events related to the relay between ERDSs					
B.1	RelayAcceptance	Relayed ERDS	Previous ERDS in the delivery chain (see note)	C (in case of inter-ERDS messaging either B.1, B.2 or B.3 shall take place)	M
B.2	RelayRejection	Relayed ERDS	Previous ERDS in the delivery chain (see note)		
B.3	RelayFailure	Relaying ERDS	Sender or previous ERDS in the delivery chain		
Events related to the acceptance/rejection by recipient					
C.1	NotificationForAcceptance	R-ERDS	Sender or previous ERDS in the delivery chain	O	R
C.2	NotificationForAcceptanceFailure	R-ERDS	Sender or previous ERDS in the delivery chain	O	R
C.3	ConsignmentAcceptance	ERDS in charge for requesting acceptance	Sender or previous ERDS in the delivery chain	O	R
C.4	ConsignmentRejection	ERDS in charge for requesting acceptance	Sender or previous ERDS in the delivery chain	O	R
C.5	AcceptanceRejectionExpiry	ERDS in charge for requesting acceptance	Sender or previous ERDS in the delivery chain	O	R
Events related to the consignment to recipient					
D.1	ContentConsignment	R-ERDS	Sender or previous ERDS in the delivery chain	C (either D.1 or D2 shall take place if neither E.1 nor E.2 take place)	M
D.2	ContentConsignmentFailure	R-ERDS	Sender or previous ERDS in the delivery chain		
D.3	ConsignmentNotification	R-ERDS	Sender or previous ERDS in the delivery chain	O	O
D.4	ConsignmentNotificationFailure	R-ERDS	Sender or previous ERDS in the delivery chain	O	O

N.	Event	Primary issuer of associated ERDS evidence	Primary target of ERDS evidence	ERDS event status	ERDS evidence status
Events related to the handover to the recipient					
E.1	ContentHandover	R-ERDS	Sender or previous ERDS in the delivery chain	C (either E.1 or E.2 shall take place if neither D.1 nor D.2 take place)	C (if no evidence on D.1 or D.2 had been produced, then it shall be generated)
E.2	ContentHandoverFailure	R-ERDS	Sender or previous ERDS in the delivery chain		C (if no evidence on D.1 or D.2 had been produced, then it shall be generated)
Events related to the connections with non ERD systems					
F.1	RelayToNonERDS	Relaying ERDS	Sender or previous ERDS in the delivery chain	O	R
F.2	RelayToNonERDSFailure	Relaying ERDS	Sender or previous ERDS in the delivery chain	O	R
F.3	ReceivedFromNonERDS	Relayed ERDS	Recipient or next ERDS in the delivery chain	O	R
NOTE: These evidences are normally not intended for the sender.					

6.2 Events and their Proof

6.2.1 A. Events related to the submission

A.1. SubmissionAcceptance

- The original message 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. SubmissionRejection

- 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. RelayAcceptance

- One ERD message that contains user content 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 (as in 4-corner model and extended model above), an intermediate or the recipient's ERDS has accepted one ERD message sent by the previous ERDS in the aforementioned chain.

B.2. RelayRejection

- One ERD message that contains user content 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 (as in 4-corner model and extended model above), 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. RelayFailure

- It was impossible (or it is clear that it will be impossible) to relay within a given time period an ERD message that contains user content to the target ERDS due to technical errors and/or other problems. This time period can be determined by legislation, R-ERDS policy rules, or parameters given by the sender or by the S-ERDS.

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 (or it is clear that it will be 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. NotificationForAcceptance

- 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 does not attest that the notification reached the recipient.

C.2. NotificationForAcceptanceFailure

- The recipient could not be notified (or it is clear that it will be impossible to notify the recipient) within a given time period due to technical errors and/or other reasons or no proof of notification within a given period exists. This time period can be determined by legislation, R-ERDS policy rules, or parameters given by the sender or by the S-ERDS.
- 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 the recipient 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 user content, 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 user content could not be made available to the recipient within a given 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. 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 or unsuccessful 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 unspecified channel) about the availability of the user content.
- The related evidence attests that a notification about the availability of the user content has been sent to a recipient at a specific time as indicated by the evidence. The evidence does 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 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 towards 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 handed over 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 user content was successfully forwarded to a non ERDS system for delivery.
- The related evidence attests that, a user content was successfully forwarded to a non ERDS system at the time indicated in the evidence.

F.2. RelayToNonERDSFailure

- The attempt to relay a user content to a non ERDS system failed due to technical errors and/or other reasons.
- The related evidence attests that, a user content failed to be forwarded to a non ERDS system at the time indicated in the evidence.

F.3. ReceivedFromNonERDS

- A 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.

History

Document history			
V1.0.0	May 2018	EN Approval Procedure	AP 20180823: 2018-05-25 to 2018-08-23
V1.1.1	September 2018	Publication	