Draft ETSI EN 319 521 V1.0.0 (2018-05)

Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for
Electronic Registered Delivery Service Providers

Reference
DEN/ESI-0019521

Keywords
e-delivery services, policy requirements, registered e-delivery services, security, trust services

ETSI

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

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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

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

Modal verbs terminology

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

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

Introduction

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

The above stated ERDS concept can be implemented in diverse ways, using different formats for identifiers and evidences, using different protocols for messaging, and even different message delivery models.

It is expected that the provision of these kind of services and the providers themselves will be suitably regulated within different regulatory or legal framework.

Particularly within the European Union 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 (Regulation (EU) No 910/2014 hereinafter) [i.1] provides a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework aims to open new market opportunities for European Union trust service providers to offer new pan-European electronic registered delivery services.

Regulation (EU) No 910/2014 [i.1] defines the so-called Qualified Electronic Registered Delivery Services (QERDS hereinafter). QERDS is a special type of ERDS. Both the service and the provider providing it meet a number of additional requirements that the regular ERDS and its providers do not need to meet.

1 Scope

The present document specifies generally applicable policy and security requirements for Electronic Registered Delivery Services Providers (ERDSP), including the services they provide.

The present document is applicable to:

- the policy and security requirements of the ERDSP and EU ERDSP qualified;
- the general and security requirements of EU Electronic Registered Delivery Services (ERDS) and EU ERDS qualified and non in terms of message integrity; protection against loss, theft, damage or any unauthorised alteration of the data transmitted; sender and recipient strong identification; time reference; and proof of data's sending and receiving.

The present document does not specify interconnection requirements.

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 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

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] ETSI EN 319 102-1: " Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.3] ISO 29115: "Information technology -- Security techniques -- Entity authentication assurance framework".

[i.4] NIST SP 800-63B: "Digital Identity Guidelines Authentication and Lifecycle Management".

[i.5] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [1] and the following apply:

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 makes possible to transmit data between the sender and recipients by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations

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

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

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

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

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

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

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

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

Qualified Electronic Registered Delivery Service (QERDS): As specified in Regulation (EU) No 910/2014 [i.1].

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

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

sender: natural or legal person that submits the user content

NOTE: In the present document, recipients and senders are assumed to be natural or legal persons.

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:

ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QERDSP	Qualified Electronic Registered Delivery Service Provider
QTSP	Qualified Trust Service Provider
REQ	REQuirement
TLS	Transport Layer Security
TSP	Trust Service Provider

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any ERDSP and ERDS provided. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

d) <the 3 letters REQ> - <4-6 letters type of service, whether EU qualified (QERDS / QERDSP) or non EU (ERDS / ERDSP)> < the clause number> - <2 digit number - incremental>.optional<1 lowercase letter) to distinct elements from a list>.

All ERDS and ERDSP requirements apply to QERDS and QERDSP.

4 General provision on policies and practices

4.1 ERDSP Practice statement

4.1.1 Common provisions

- **REQ-ERDS-4.1.1-01** All requirements from ETSI EN 319 401 [1], clause 6.1 shall apply.
- **REQ-ERDS-4.1.1-02** The ERDS set of policies and practices shall be approved by the ERDSP management, published and communicated to its employees and external parties as relevant.
- **REQ-ERDS-4.1.1-03** The ERDSP shall have an ERDS practice statement publicly available on its website or any other electronic means, containing the practices and procedures used to address the requirements on both the ERDSP and the ERDS provided.

NOTE: The ERDSP is not obliged to disclose any aspects containing sensitive information.

- **REQ-ERDS-4.1.1-04** The ERDSP shall define a review process for the practices including responsibilities for maintaining the ERDS practice statement and a process to notify changes it intends to make in its ERDS practice statement.
- **REQ-ERDS-4.1.1-05** The ERDS practice statement shall identify the obligations of all external organizations supporting the provision of ERDS including the applicable policies and practices.
- **REQ-ERDS-4.1.1-06** The ERDS practice statement shall specify the means used to report any modifications to user content before consignment/ handover.

- **REQ-ERDS-4.1.1-07** The ERDS practice statement shall describe how sender and recipient are identified and authenticated to the service.
- **REQ-ERDS-4.1.1-08** The ERDS practice statement shall include information on how to get evidence relating to the handling of the transmitted data.
- **REQ-ERDS-4.1.1-09** The ERDS practice statement shall include any possible limitations on the evidence validity period.
- **REQ-ERDS-4.1.1-10** The ERDS practice statement shall include a description on how the ERDS provision ensures the security of transmission against any risk of loss, theft, damage or any unauthorised alterations.
- **REQ-ERDS-4.1.1-11** The ERDS practice statement shall include the sender, recipient and other relying parties obligations.

4.1.2 Practice statement for EU QERDSP

In addition, for EU QERDSP and EU QERDS, the following specific requirements apply:

- **REQ-QERDS-4.1.2-01** The QERDS practice statement shall include a clear statement indicating that the policy is for qualified ERDS as per Regulation (EU) No 910/2014 [i.1].
- **REQ-QERDS-4.1.2-02** The QERDS practice statement shall include the complete list of QTSPs involved in the provision of the QERDS.

EXAMPLE: Time-stamping service, TSPs issuing certificates, etc.

- **REQ-QERDS-4.1.2-03** The QERDS practice statement shall include any limitations on the use of the QERDS.
- **REQ-QERDS-4.1.2-04** The QERDS practice statement shall include the retention period actually applied to the evidence as per clause 5.4.1 and, where applicable, the modalities of reversibility and portability.
- **REQ-QERDS-4.1.2-05** The QERDS practice statement shall state the provisions made for termination of service.

4.2 Terms and conditions

- **REQ-ERDS-4.2-01** All requirements from ETSI EN 319 401 [1], clause 6.2 shall apply.
- **REQ-ERDS-4.2-02** The terms and conditions shall indicate what is deemed to constitute a delivery of the user content to the recipient.
- **REQ-ERDS-4.2-03** The terms and conditions shall indicate if any expiry of data availability to the recipient is handled and, if applicable, how long the data are available.
- **REQ-ERDS-4.2-04** Before entering into a contractual relationship with an ERDSP customer, the ERDSP shall inform the customer of the terms and conditions regarding the ERDS.
- **REQ-ERDS-4.2-05** The ERDSP shall communicate the terms and conditions through a durable (i.e. with integrity over time) mean of communication, and in a human readable form.
- **REQ-ERDS-4.2-06** The terms and conditions may be transmitted electronically.
- **REQ-ERDS-4.2-07** The ERDSP shall have evidence that the terms and conditions have been accepted by the ERDSP custom.

4.3 Information security policy

- **REQ-ERDS-4.3-01** All requirements from ETSI EN 319 401 [1], clause 6.3 shall apply.

5 General provision on ERDS

5.1 User content integrity and confidentiality

5.1.1 Common provisions

- **REQ-ERDS-5.1.1-01** The ERDS shall ensure that availability, integrity, and confidentiality of the user content is adequately guaranteed from the submission to the consignment or handover of the user content.
- **REQ- EDRS-5.1.1-02** The confidentiality of sender/ recipient identity shall be protected, especially when exchanged with the sender/recipient or between distributed ERDS system components.
- **REQ-ERDS-5.1.1-03** The integrity of user content and associated metadata shall be protected in transmission, especially when exchanged with the sender/recipient or between distributed ERDS system components, and in storage.
- **REQ-ERDS-5.1.1-04** [CONDITIONAL] If the user content needs to be modified by the ERDS, the changes shall be clearly indicated to the sender, the recipient and any third party involved.

EXAMPLE: In case of format conversion.

5.1.2 Provisions for EU QERDSP

In addition, the following EU QERDSP and EU QERDS-specific requirements apply:

- **REQ-QERDS-5.1.2-01** User content shall be protected by an advanced electronic seal or signature issued by a QTSP in such a manner as to preclude the possibility of the data being changed undetectably.
- **REQ-QERDS-5.1.2-02** [CONDITIONAL] If applicable, user content should be securely retained to meet statutory requirements.
- **REQ-QERDS-5.1.2-03** [CONDITIONAL] If the advanced electronic seal or signature on the user content is generated by another QTSP, then the ERDSP shall verify the validity of the generated signature or seal, and check that the QTSP generating the signature or seal is still qualified.

5.2 Users Identification and Authentication

5.2.1 Provisions for EU QERDSP initial identity verification

5.2.1.1 General

- **REQ-QERDS-5.2.1.1-01** The QERDSP shall verify the identity of the sender and the recipient either directly or by relying on a third party:

  a) by the physical presence of the natural person or of an authorized representative of the legal person; or

  b) remotely, using electronic identification means, for which a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in Article 8 of the Regulation (EU) N° 910/2014 [i.1] with regard to the assurance levels 'substantial' or 'high'; or

  c) by means of a certificate of an advanced electronic signature or of an advanced electronic seal; or

d) by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalence of the assurance level shall be confirmed by a conformity assessment body.

NOTE: The third party verifying the identity of the sender and the recipient can be another QERDSP in the case that the sender or the recipient or both are subscribed to another QERDSP.

- **REQ-QERDS-5.2.1.1-02** [CONDITIONAL] If after initial identity verification, the QERDSP has not found an authentication means to the sender or the recipient, identity verification shall be carried out each time a user content is sent or handed over.

5.2.1.2 Recipient identification and handover of user content

- **REQ-QERDS-5.2.1.2-01** The QERDSP shall hand over the user content to the recipient only after a successful identification of the recipient.

- **REQ-QERDS-5.2.1.2-02** [CONDITIONAL] If the identification of the recipient is based on an advanced electronic signature, the signature validation shall precede the handover of the user content.

NOTE: For verification see ETSI EN 319 102-1 [i.2].

- **REQ-QERDS-5.2.1.2-03** [CONDITIONAL] If the identification of the recipient is based on an QERDS internal process, the QERDSP should conduct the whole process in a secured and controlled environment.

- **REQ-QERDS-5.2.1.2-04** [CONDITIONAL] If the identification of the recipient is based on an QERDS internal process, all evidence of identification and consignment or handover process shall be gathered and protected.

5.2.2 Provisions for EU QERDS authentication

- **REQ-QERDS-5.2.2-01** The sender, the recipient or both shall use the mean of authentication accepted by the QERDSP as per its Practice Statement in the authentication process before submitting the user content or before it hands over to the recipient.

NOTE: The QERDSP can issue a mean of authentication either for the sender, the recipient or both to be used in the authentication process.

- **REQ-QERDS-5.2.2-02** [CONDITIONAL] When the QERDSP issues a mean of authentication, it shall be one of the following:

a) multi factor authentication mechanisms; or

EXAMPLE 1: At a level of assurance compatible with LoA3 ISO 29115 [i.3], or AAL2 NIST SP 800-63B [i.4] or Substantial IA 1502/2015 [i.5] or an equivalent level in a different assurance framework.

b) mutual TLS authentication, which includes advanced user's certificate; or

c) advanced electronic signature; or

d) an authentication mean with an equivalent security level to the above.

- **REQ-QERDS-5.2.2-03** [CONDITIONAL] When machine-to-machine mutual authentication between the customer and the QERDSP is established, single factor authentication mechanisms may be adopted for user authentication.

EXAMPLE 2: At a level of assurance corresponding to LoA2 ISO 29115 [i.3], or AAL1 NIST SP 800-63B [i.4] or Low IA 1502/2015 [i.5] or an equivalent level in a different assurance framework.

- **REQ-QERDS-5.2.2-04** [CONDITIONAL] If the QERDSP does not provide users with a mean of authentication, the identity of the sender shall be verified each time the sender submits the user content, and the identity of the recipient shall be verified before the QERDS consigns or hands over the user content to the recipient.

5.3 Time reference

5.3.1 Common provisions

- **REQ-EDRS-5.3.1-01** The time reference shall be in line with the one defined within the Terms and Conditions.

5.3.2 Provisions for EU QERDS

In addition, the following EU QERDSP and EU QERDS-specific requirements apply:

- **REQ-QERDS-5.3.2-01** The date and time of sending, receiving and any change of user content shall be indicated by a qualified electronic time-stamp.
- **REQ-QERDS-5.3.2-02** Proof of sending and proof of receiving shall be linked to user content and time-stamped by a qualified electronic time-stamp.
- **REQ-QERDS-5.3.2-03** [CONDITIONAL] In case a QERDSP relies on a third-party qualified time-stamp service provider, the QERDSP shall check regularly that the time-stamp service provider is still qualified.

5.4 Events and evidence

5.4.1 Common provisions

- **REQ-ERDS-5.4.1-01** The ERDS shall make available evidence of user content consignment or handover or both to the sender of the user content.
- **REQ-ERDS-5.4.1-02** The ERDS shall generate an evidence of submission of the user content by the sender.
- **REQ-ERDS-5.4.1-03** The ERDSP shall archive at least:
  a) users identification data;
  b) users authentication data;
  c) proof that the sender identity has been initially verified;
  d) logs of ERDS operation, identity verification of sender and recipient, and communication;
  e) proof of the recipient's identity verification before the consignment/handover of the user content;
  f) means to prove that the user content has not being modified during transmission;
  g) a reference to or a digest of the complete user content submitted; and
  h) time-stamp tokens corresponding to the date and time of sending, consigning and handing over and modifying the user content, as appropriate.
- **REQ-ERDS-5.4.1-04** The ERDSP shall ensure the confidentiality, integrity and availability of the logs defined in the present clause.
- **REQ-ERDS-5.4.1-05** The ERDSP shall archive for the national legal period applicable after the date of sending all relevant evidence.

5.4.2 Provisions for EU QERDS

In addition, the following EU QERDSP and EU QERDS-specific requirements apply:

- **REQ-QERDS-5.4.2-01** All events related to sender initial identity verification and further authentication shall be logged.

- **REQ-QERDS-5.4.2-02** All events related to recipient initial identity verification and/or further authentication shall be logged.
- **REQ-QERDS-5.4.2-03** [CONDITIONAL] If provided, the initial and subsequent identity verification information shall be recorded.

EXAMPLE: This can include the type of document(s) presented by the applicant to support identification (e.g. applicant's identity card or passport); any record referring to a unique identification data, numbers, or a combination thereof; or copies of applications and identification documents, including the signed sender agreement.

5.5 Interoperability

- **REQ-ERDS-5.5-01** The ERDSP shall verify that service(s) with which it interoperates are at least a ERDS.
- **REQ-ERDS-5.5-02** The ERDSP shall authenticate others ERDSP before consignment or handing over the user content.
- **REQ-ERDS-5.5-03** The ERDSP shall verify that the communications are protected to ensure integrity and confidentiality of user content.

6 Risk Assessment

- **REQ-ERDS-6-01** All requirements from ETSI EN 319 401 [1], clause 5 shall apply.

7 ERDSP management and operation

7.1 Internal organization

7.1.1 Organization reliability

- **REQ-ERDS-7.1.1-01** All requirements from ETSI EN 319 401 [1], clause 7.1.1 shall apply.

7.1.2 Segregation of duties

- **REQ-ERDS-7.1.2-01** All requirements from ETSI EN 319 401 [1], clause 7.1.2 shall apply.

7.2 Human resources

7.2.1 Common provisions

- **REQ-ERDS-7.2.1-01** All requirements from ETSI EN 319 401 [1], clause 7.2 shall apply.

7.2.2 Provisions for EU QERDS

In addition, the following EU QERDSP-specific requirements apply:

- **REQ-QERDSP-7.2.2-01** The QERDSP shall appoint an identity verification officer.
- **REQ-QERDSP-7.2.2-02** The identity verification officer shall be in charge of ensuring that the actual processes conducted for verifying the identity of the sender and recipient are compliant with the initial identity verification process specified.

7.3 Asset management

7.3.1 General requirements

- **REQ-ERDS-7.3.1-01** All requirements from ETSI EN 319 401 [1], clause 7.3.1 shall apply.

7.3.2 Media handling

- **REQ-ERDS-7.3.2-01** All requirements from ETSI EN 319 401 [1], clause 7.3.2 shall apply.

7.4 Access control

- **REQ-ERDS-7.4-01** All requirements from ETSI EN 319 401 [1], clause 7.4 shall apply.

7.5 Cryptographic controls

The following requirements only applies when the ERDSP generates signing certificates and/or generates the signing private keys and/or creates the digital signature:

- **REQ-ERDS-7.5-01** All requirements from ETSI EN 319 401 [1], clause 7.5 shall apply.
- **REQ-ERDSP-7.5-02** The ERDS signing keys shall be held physically isolated from normal operations in such a way that only designated trusted personnel have access to the keys for use in signing user content and/or evidence.
- **REQ-ERDSP-7.5-03** The ERDS signing private key shall be held and used within a secure cryptographic device.
- **REQ-ERDSP-7.5-04** The ERDS signing private key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.
- **REQ-ERDSP-7.5-05** The ERDS signing private key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the ERDS practices.
- **REQ-ERDSP-7.5-06** The copies of the ERDS signing private key shall be subject to the same or greater level of security controls as keys currently in use.
- **REQ-ERDSP-7.5-07** [CONDITIONAL] If the ERDS signing private key and any copies are stored in a dedicated secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device.
- **REQ-ERDSP-7.5-08** The secure cryptographic device shall not be tampered with during shipment and storage.
- **REQ-ERDSP-7.5-09** The secure cryptographic device shall be functioning correctly.
- **REQ-ERDSP-7.5-10** The ERDS signing private key stored on the ERDSP secure cryptographic device shall be destroyed upon device retirement.

NOTE: This destruction does not necessarily affect all physical copies of the private key. Only the physical of the key stored in the secure cryptographic device under consideration will be destroyed.

7.6 Physical and environmental security

- **REQ-ERDS-7.6-01** All requirements from ETSI EN 319 401 [1], clause 7.6 shall apply.

- **REQ-ERDSP-7.6-02** The ERDSP's physical and environmental security policy for systems concerned with the provision of the ERDS shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.
- **REQ-ERDSP-7.6-03** The ERDSP shall implement controls to protect against equipment, information, media and software related to the provision of the ERDS being taken off-site without authorization.
- **REQ-ERDSP-7.6-04** Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.
- **REQ-ERDSP-7.6-05** Any parts of the premises shared with other organizations shall be outside ERDS system and communication perimeter.
- **REQ-ERDSP-7.6-06** Every logical access shall be logged.
- **REQ-ERDSP-7.6-07** Every entry to the physically secure area shall be subject to oversight and securely logged.
- **REQ-ERDSP-7.6-08** Non-authorized person shall be accompanied by an authorized person whilst in the secure area.

7.7 Operation security

- **REQ-ERDS-7.7-01** All requirements from ETSI EN 319 401 [1], clause 7.7 shall apply.

7.8 Network security

- **REQ-ERDS-7.8-01** All requirements from ETSI EN 319 401 [1], clause 7.8 shall apply.
- **REQ-ERDSP-7.8-02** The ERDSP shall monitor capacity demands.
- **REQ-ERDSP-7.8-03** Projections of future capacity requirements shall ensure that adequate processing power and storage are available.
- **REQ-ERDSP-7.8-04** The ERDSP shall use state of the art protocols and algorithms for encryption on transport layer level.
- **REQ-ERDSP-7.8-05** The ERDSP shall use website authentication certificates for Transport Layer Security if data is sent outside internal networks.

7.9 Incident management

- **REQ-ERDS-7.9-01** All requirements from ETSI EN 319 401 [1], clause 7.9 shall apply.

7.10 Collection of evidence for ERDSP internal services

- **REQ-ERDS-7.10-01** All requirements from ETSI EN 319 401 [1], clause 7.10 shall apply.
- **REQ-ERDSP-7.10-02** The ERDSP shall log events relating to the submission and consignment and handover of the user content for at least 2 years.
- **REQ-ERDSP-7.10-03** All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.

7.11 Business continuity management

- **REQ-ERDS-7.11-01** All requirements from ETSI EN 319 401 [1], clause 7.11 shall apply.
- **REQ-ERDSP-7.11-02** The ERDSP's data systems necessary to resume ERDS operations shall be backed up and stored in safe places suitable to allow the ERDSP to timely go back to operations in case of incident/disasters.
- **REQ-ERDSP-7.11-03** The ERDSP shall back-up copies regularly of essential information and software.
- **REQ-ERDSP-7.11-04** Adequate recovery facilities shall be provided to ensure that all essential information and software can be recovered following a disaster or media failure.
- **REQ-ERDSP-7.11-05** Recovery arrangements shall be regularly tested to ensure that they meet the requirements of business continuity plans.
- **REQ-ERDSP-7.11-06** [CONDITIONAL] If risk analysis identifies information requiring dual control for management then dual control shall be applied to recovery.

EXAMPLE: Keys are an example of information requiring dual control for management.

- **REQ-ERDSP-7.11-07** The ERDSP's business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of an ERDSP private key as a disaster and the planned processes shall be in place.
- **REQ-ERDSP-7.11-08** Following a disaster, the ERDSP shall, where practical, take steps to avoid repetition of a disaster.
- **REQ-ERDSP-7.11-09** [CONDITIONAL] In the case of compromise of the ERDSP services, the ERDSP shall notify it at least to all its customers, and relying parties and other entities with which the ERDSP has agreements or other form of established relations for the provision of the ERDS. The information to be provided shall indicate that evidence information issued using the compromised key may no longer be valid from the known time of compromise.
- **REQ-ERDSP-7.11-10** [CONDITIONAL] If any of the algorithms, or associated parameters, used by the ERDSP become insufficient for its remaining intended usage then the ERDSP shall:

  a) inform all its customers and relying parties with whom the ERDSP has agreement or other form of established relations for the provision of the ERDS; and

  b) secure the existing evidential material with new time-stamps.

7.12 ERDSP termination and ERDS termination plans

- **REQ-ERDS-7.12-01** All requirements from ETSI EN 319 401 [1], clause 7.12 shall apply.
- **REQ-ERDSP-7.12-02** The ERDSP shall keep the collected evidence for the national statutory time.

7.13 Compliance

- **REQ-ERDS-7.13-01** All requirements from ETSI EN 319 401 [1], clause 7.13 shall apply.
- **REQ-ERDSP-7.13-02** [CONDITIONAL] Where feasible, ERDS and end-user products used in the provision of the service shall be made accessible for persons with disabilities.

History

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