Draft ETSI EN 319 521 V0.0.4 (2017-10)

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

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

0

1

2

Reference

DEN/ESI-0019521

Keywords

e-commerce, electronic signature, extended validation certificat, public key, 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

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 server (http://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.

Foreword

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

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):	12 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

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.

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.

Regulation (EU) No 910/2014 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.

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.

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 qualified and non qualified ERDSPs;
- the general and security requirements of the qualified and non qualified Electronic Registered Delivery Services (ERDS) 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 http://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 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements".

[i.3.] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.4] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps".

3 Definitions and abbreviations

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:

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 unauthorised alterations

electronic registered delivery service provider: Trust Service Provider which provides electronic registered delivery services

electronic registered delivery service practice statement: statement of the practices that an electronic registered delivery service provider employs in providing an electronic delivery service

NOTE: See clause 4 for further information on practice statement

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

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

qualified electronic registered delivery service: As specified in Regulation (EU) No 910/2014 [i.1]

qualified electronic registered delivery service provider: 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.

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
QERDS	Qualified Electronic Registered Delivery Service
QERDSP	Qualified Electronic Registered Delivery 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> - <4-5 letters type of service, whether qualified (QERDS) or non-qualified (ERDS)> < the clause number> - <2 digit number - incremental>.optional<1 lowercase letter) to distinct elements from a list>

All ERDS and ERDSP requirements shall apply to QERDS and QERDSP.

4 General provision on policies and practices

4.1 ERDS Practice statement

REQ-ERDS-4.1-01 All requirements from EN 319 401[1] clause 6.1 shall apply.

REQ- ERDS-4.1-02 The ERDSP shall have a management body with overall responsibility for the ERDSP with final authority for approving the ERDSP practice statement.

REQ- ERDS-4.1-03 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 4.1-04 The ERDSP shall have a ERDS practice statement publicly available on its website or any other electronic means of 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-4.1-05 The ERDSP shall make available to subscribers and relying parties its ERDS practice statement.

REQ- ERDS-4.1-06 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-4.1-07 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-4.1-08 The ERDS practice statement shall specify the means used to report any modifications to user content before relay and delivery.

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

REQ-QERDS-4.1-01 The QERDS practice statement shall Include a clear statement indicating that the policy is for qualified ERDS a per Regulation (EU) No 910/2014 [i.1];

REQ-QERDS-4.1-02 The QERDS practice statement shall Include the complete list of TSPs and QTSPs involved in the provision of the QERDS;

EXAMPLE: Time-stamping service, TSPs issuing certificates…

REQ-QERDS-4.1-03 The QERDS practice statement shall Include a description on how the security of transmission against any risk of loss, theft, damage or any unauthorised alterations, is ensured.

REQ-QERDS-4.1-04 The QERDS practice statement shall Include any limitations on the use of the QERDS;

REQ-QERDS-4.1-05 The QERDS practice statement shall Include the sender, recipient and other relying parties obligations;

REQ-QERDS-4.1-06 The QERDS practice statement shall Describe how sender and recipient are identified and authenticated to the sevice;

REQ-QERDS-4.1-07 The QERDS practice statement shall Include information on how to get evidence relating to the handling of the transmitted data

REQ-QERDS-4.1-08 The QERDS practice statement shall Include any possible limitations on the evidence validity period;

REQ-QERDS-4.1-09 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; and

REQ-QERDS-4.1-10 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 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 expiracy 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 sender of the terms and conditions regarding the ERDS.

i) **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.
ii) **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 sender.

4.3 Information security policy

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

5 General provision on ERDS

5.1 User content integrity and confidentiality

REQ-ERDS-5.1-01 The ERDS shall ensure that availability, integrity, and confidentiality of the user content is adequately guaranteed from the sending to the reception of the user content.
REQ- EDRS-5.1-02 The confidentiality of sender/recipient identification shall be protected, especially when exchanged with the sender/recipient or between distributed ERDS system components.

In addition, the following QERDSP and QERDS-specific requirements and guidance apply.

- **REQ-QERDS-5.1-01** 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-5.1-02** The integrity of user content shall be protected, especially when exchanged with the sender/recipient or between distributed ERDS system components.
- **REQ-QERDS-5.1-03** [Conditional] If applicable, user content should be securely retained to meet statutory requirements
- **REQ-QERDS-5.1-04** [Conditional] If the ERDSP has generated a qualified electronic seal or signature on the user content, then the ERDSP shall be clearly identified in the certificate used for generating such seal or signature.
- **REQ-QERDS-5.1-05** [Conditional] If the qualified 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 TSP generating the signature or seal is still qualified.

- **REQ-QERDS-5.1-06** [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.

  EXEMPLE: In case of format conversion.

5.2. Users Identification and Authentication

5.2.1. Initial identity verification

REQ-QERDS-5.2.1-01 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 authorised representative of the legal person; or

b) remotely, using electronic identification means, for which a physical presence of the natural person or of an authorised 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 a qualified electronic signature or of a qualified electronic seal issued in compliance with point a) or b); or

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

REQ-QERDS-5.2.1-02 [Conditional] If after initial identity verification, the QERDSP has not bound an authentication means to the sender or the recipient, identity verification shall be carried out each time a user’s content is sent or received.

5.2.1.1. Recipient identification and consignment of user content

REQ-QERDS-5.2.1.1-01 The QERDSP shall consign or hand over the user content to the recipient only after a successful authentication of the recipient.

REQ-QERDS-5.2.1.1-02 [Conditional] If the authentication of the recipient is based on an advanced electronic signature, the signature validation shall precede the consignment or handing over of the user content.

REQ-QERDS-5.2.1.1-03 [Conditional] If the authentication of the recipient is based on an QEDRS internal authentication process, the QEDRSP should conduct the whole process in a secured and controlled environment. All evidence of authentication and consignment or handing over process shall be gathered and protected.

5.2.2 Authentication

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

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

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

REQ-QERDS-5.2.2-02 [Conditional] Authentication means to QEDRSPs shall be of one of the following:

a) Multi-factor user authentication; or

EXEMPLE: at a level compatible with ISO 29115 LoA3, NIST AAL2, IA 1502/2015 Substantial, remote q-signature auth. level

b) Mutual authentication based on certificates; or

c) An authentication mean with a equivalent security level to the above.

REQ-QERDS-5.2.2-03 [Conditional] If the user does not have a mean of authentication, identity verification shall be carried out at each time a user's content is sent.

REQ-QERDS-5.2.2-04 [Conditional] If applicable, the mean of authentication shall be under the exclusive control of the user.

5.3 Time reference

REQ-EDRS-5.3-01 The Time reference shall be in line with the one defined within the Terms and Conditions.

In addition, the following QERDSP and QERDS-specific requirements and guidance apply.

- **REQ-QEDRS-5.3-01** The date and time of sending, receiving and any change of user content shall be indicated by a qualified electronic time-stamp.
- **REQ-QEDRS-5.3-02** Proof of sending and proof of receiving shall be linked to user content and time-stamped by a qualified electronic time-stamp.
- **REQ-QEDRS-5.3-03** [Conditional] In case a QERDSP relies on a third-party qualified time-stamp service provider, the validity of the qualified electronic time-stamp shall be verified once the qualified time-stamp service provider generates it.
- **REQ-QEDRS-5.3-04** [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

REQ-EDRS-5.4-01 The ERDS shall provide evidence of user content sending and receiving to the users.

REQ-EDRS-5.4-02 [Conditional] if applicable, the ERDS shall provide evidence of user content consignment of handing over to the users.

REQ-EDRS-5.4-03 The ERDS shall generate an evidence of submission of the user content by the sender.

REQ-EDRS-5.4-04 The ERDS shall generate an evidence of consignment or handing over of the user content to the recipient

REQ-EDRS-5.4-05 The ERDSP shall keep at least:

a) Users identification data;

b) Users authentication level;

c) Proof that the sender identity has been initially verified;

d) Logs of ERDS operation, identification validation of sender and recipient, and communication;

e) Proof of the recipient's identity verification before the handover of the user content;

f) Proof that the user content has been made available only after the recipient identity verification;

g) Proof that the user content has been received by the recipient, if applicable:

h) Means to prove that the user content has not being modified during transmission;

i) A reference to or a digest of the complete user's content submitted; and

j) Time-stamp tokens corresponding to the date and time of sending, consigning and handing over and modifying the user content, as appropriate.

REQ-EDRS-5.4-06 The ERDSP shall ensure the confidentiality, integrity and availability of the logs defined in the present clause.

In addition, the following QERDSP and QERDS-specific requirements and guidance apply.

- **REQ-QEDRS-5.4-01** All events related to sender initial identity verification and further authentication shall be logged.
- **REQ-QEDRS-5.4-02** All events related to recipient initial identity verification and/or further authentication shall be logged.
- **REQ-QEDRS-5.4-03** [Conditional] If provided, the initial and renewed identity verification information shall be recorded.

  EXEMPLE: This may 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.

5.4.1 Retention period

REQ-EDRS-5.4.1-01 The ERDS provider shall archive for the national legal period applicable after the date of sending all relevant evidence.

6 Risk Assesment

REQ-ERDS-6-01 All requirements from 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 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 EN 319 401[1] clause 7.1.2 shall apply.

7.2 Human resources

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

In addition, the following QERDSP-specific requirements and guidance apply.

REQ- QERDSP-7.2-01 The ERDSP shall appoint an identity verification officer.

REQ- QERDSP-7.2-02 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 EN 319 401[1] clause 7.3.1 shall apply.

7.3.2 Media handling

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

7.4 Access control

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

7.5 Cryptographic controls

REQ-ERDS-7.5-01 All requirements from EN 319 401[1] clause 7.5 shall apply.

[CONDITIONAL] In case the ERDSP generates the signature or seal certificates, the following ERDSP-specific requirements and guidance apply:

REQ- ERDSP-7.5-02 The ERDSP' signature or seal certificate private 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 sealing/signing private key shall be held and used within a secure cryptographic device.

REQ- ERDSP-7.5-04 The ERDS sealing/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 sealing/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 sealing/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 sealing/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 sealing/signing private key stored on the ERDSP secure cryptographic device shall be destroyed upon device retirement.

NOTE: This destruction does not necessarily affect all 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 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 EN 319 401[1] clause 7.7 shall apply.

7.8 Network security

REQ-ERDS-7.8-01 All requirements from 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 non-qualified 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 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 EN 319 401[1] clause 7.10 shall apply.

REQ- ERDSP-7.10-02 The EDRSP shall log events relating to the sending and consigning/handing over the user content.

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 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, the ERDSP shall notify it at least to all senders/receivers, 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 sender/recipients and relying parties with whom the ERDSP has agreement or other form of established relations for the provision of the ERDS; and

b) schedule a re-signing and re-time-stamping of all evidences.

7.12 ERDSP termination and ERDS termination plans

REQ-ERDS-7.12-01 All requirements from 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 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		
V0.0.0.1	January 2017	For STF contributions and comments
V.0.0.01.B	April 2017	First draft
v.0.0.01.d	June 2017	First stable draft
v.0.0.0.2	June 2017	For submittion to #ESI59
v.0.0.0.2.a	July 2017	Addressing comments received
v.003	September 2017	Addressing comments received
V0.0.4	October 2017	Stable draft for public review