LUXTRUST®
Enabling a digital world

Certificate Practice Statement of Qualified Electronic Registered Delivery Services

Version number: 1.0
Publication Date: 06/03/2023
Effective Date: 20/03/2023

Document O.I.D: 1.3.171.1.1.1.15

Document Information

Document title:	Certificate Practice Statement of Qualified Electronic Registered Delivery Services
Document Code	N/A
Project Reference:	LuxTrust S.A.
Document Type	Technical Specification
Document Distribution List	Any
Document Classification	Public
Document Owner	CSP Board

Version History

Version	Who	Date	Reason of modification
1.0	YNU	20/02/2023	First Version

Table of content

Intellectual Property Rights

References

[1] European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data replaced by REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (GDPR).

[2] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.

[3] Loi du 17 juillet 2020 portant modification de la loi modifiée du 14 août 2000 relative au commerce électronique.

[4] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.

[5] Règlement Grand-Ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».

[6] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.

[7] LuxTrust Time Stamping Policy, latest version in force.

[8] ETSI EN 319 521 Policy and security requirements for Electronic Registered Delivery Service Providers

[9] EN 319 401 V2.1.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016-02)

[10] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[11] European regulation N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

1 Overview

1.1 Presentation

LuxTrust S.A., having its registered office at 13-15 Parc d'Activités L-8303 Capellen, registered with the Luxembourg Trade and Companies Register under number B112233, is a Qualified Trusted Service Provider (hereinafter referred to as "QTSP") that offers "Qualified Electronic Registered Delivery Services" (QERDS) in accordance with Section 7 of REGULATION (EU) No. 910/2014 of the European Parliament. This service is provided via the LuxTrust QERDS API.
The Service Provider is the legal entity that has subscribed to the use of the service provided by the QERDS API and has signed the corresponding contract with LuxTrust.

1.2 Document Name and Identification

This document is the "Certification Practice Statement of Qualified Electronic Registered Delivery Service", hereinafter "CPS QERDS".
This document should be read in conjunction with the "LuxTrust Global Qualified CA Certification Practice Statement hereinafter "CPS LT GQCA" and provides information on the specific elements of the QERDS service.
The OID of this document is 1.3.171.1.1.1.15

1.3 PKI Participants

LuxTrust provides the qualified timestamp service and the qualified seal service used in conjunction with the QERDS service.
Please refer to the relevant section of the "CPS LT GQCA" document.

1.3.1 *Permitted uses*

The QERDS service enables legal entities or natural persons to send electronic registered mail to other legal entities or natural persons.
The QERDS generates and issues attestations for proving that there was a series of data related to the communication between a sender and a recipient and that such data were not altered at a specific point in time. Its use is restricted to customers' apps and/or systems (natural or legal persons) who has subscribed to this service.

1.3.2 *Restrictions and Prohibitions on Use*

The QERDS shall not be used for purposes other than those specified in this document. Likewise, the service shall only be used in accordance with applicable laws and regulations.

1.4 Policy administration

Please refer to the relevant section of the "CPS LT GQCA" document.

1.4.1 *Contact Person*

The contact person, designated by LuxTrust S.A., via its LuxTrust CSP Board acting as approval authority for this policy, can be reached via this email: cspboard@luxtrust.lu. For more details, please refer to the relevant section of the "CPS LT GQCA" document.

1.5 Related documents

The date and time of sending and receiving are recorded in a time-stamped report by a LuxTrust qualified electronic time-stamp and sealed by a LuxTrust qualified seal.
Reports generated by the registered mail service are sealed by a LuxTrust qualified electronic seal and time-stamped by a LuxTrust qualified time-stamp.
The applicable policy for time stamping is the "LuxTrust Time-Stamping Policy".
The qualified seal is applied according to the “LuxTrust Cloud Signature Policies”.

2 Publication

Please refer to the relevant section of the "CPS LT GQCA" document.

3 Identification and authentication

3.1 Identification

In order to use LuxTrust's QERDS service, it is necessary that the sender and the recipient of the communications are identified based on article 24 1. of the eIDAS regulation.
LuxTrust, through its compliance department, and in particular via the head of the Regulatory and Compliance department, ensures that the identification process complies with these requirements prior to their integration into ORELY / BLINK.
A regular check is carried out to ensure that the identification process remains compliant.
Once the Service Provide identity has been verified, access to the LuxTrust QERDS service is activated for this person.
Once the sender/recipient identity has been verified, access to the LuxTrust QERDS service is granted.
The authentication means provided to the sender / recipient must have at least an assurance level compatible with AAL2 NIST SP 800-63B and supported by LuxTrust's ORELY or BLINK service.

3.2 Sender’s Authentication

Sender’s authentication for sending communications will be carried out by means supported by LuxTrust's ORELY or BLINK service.

3.3 Recipient’s Authentication

The recipient’s authentication for sending communications will be carried out by means supported by LuxTrust's ORELY or BLINK service.

4 Operational Requirements

The service supports the following functions in relation to electronic registered mail

- Authentication of senders and recipients;
- Deposit for senders
- Acceptance, refusal or unclaimed for recipients
- Proof generation for senders
- Preservation of legal, time-stamped and stamped evidence associated with the operation of the service.

4.1 Access to the Service

This service is available via an API. The integration and implementation documents for this service are available on request subject to a contractual relationship between the Service Provider and LuxTrust.
Access to the QERDS API will be carried out by means of secure protocols and encrypted communications. LuxTrust ensures strong authentication of any actor using this service.

4.2 Sending process

An electronic registered mail can only be provided via a Service Provider who has signed the contract for the use of this LuxTrust service and who is duly identified and authenticated by LuxTrust.
No check is performed on the contents of the provided data.
A report with the hash of the provided data and the list of recipients is generated, sealed and timestamped. This report is made available to the Service Provider.
Service Provider guarantee the accuracy of the information they provide to the service including their identity and that of the recipient as well as the corresponding e-mail addresses.
The Service Provider also undertake to comply with applicable contractual or legal obligations imposed by this policy and/or applicable legal and regulatory requirements (in particular that relating to the protection of personal data).
The Service Provider shall take all appropriate measures to protect their own IT systems using the QERDS Service from unauthorized intrusion, destruction or alteration, and from possible contamination by viruses, Trojan or other systems causing security breaches potentially threatening the QERDS service.
Service Provider must ensure that they do not introduce viruses, worms, logic bombs or any other content that constitutes a potential threat to the security of the QERDS service.
LuxTrust is not liable for the content of the data provided by the Service Provider or the sender or any other third party, and for any IT consequences that may result from this.
Service Provider must collect and verify proof of its submissions from the service and are responsible for its safekeeping on their own behalf.
Service Provider must protect their means of authentication against loss or use by a third party. They must revoke it without delay in the event of loss, theft, compromise or suspicion of compromise.

4.3 Delivery process

Any recipient of an electronic registered mail must carry an authentication means supported by LuxTrust.
If the recipient does not take any action within the acceptance period, the electronic registered letter is considered as unclaimed.
Whatever the action taken by the recipient, rejection, acceptance, unclaimed, all actions are traced and mentioned in the report issued by LuxTrust

4.4 Acceptance period

The recipient has a determined period of days after the deposit of the data to accept or reject the electronic registered letter.

4.5 Data modification

The data, by design, are not subject to any modification during the execution of the electronic registered delivery service.
The documents are encrypted in transit and at rest.

4.6 Events and Evidences

LuxTrust's report are sealed documents that gather all the information evidencing that an event has occurred, and that they have not been modified afterwards.
Both the seal process and the time stamps are provided by LuxTrust in accordance with the eIDAS Regulation.
The report includes:

- Sender and recipient's data of electronic messages.
- The hash of the transmitted contents
- The size and type of the contents
- The deposit status
- The timestamp of the event

that ensure at least the availability of the following data

- users identification data;
- users authentication data;
- proof that the sender identity has been initially verified;
- logs of QERDS operation, identity verification of sender and recipient, and communication;
- proof of the recipient's identity verification before the consignment/handover of the user content;
- means to prove that the user content has not being modified during transmission;
- a reference to or a digest of the complete user content submitted; and

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

The Service provider will have access to all his evidences in the qualified delivery service, during the relevant safekeeping period and for a minimum period of ten years.

In the case of a failure with the integrity of the data, or any incident associated with the integrity of the content during the delivery process, LuxTrust's support service will communicate it to the interested parties.

5 Facility, management and operations security controls

Please refer to the relevant section of the "CPS LT GQCA" document.

6 Technical security controls

Please refer to the relevant section of the "CPS LT GQCA" document.

7 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Please refer to the relevant section of the "CPS LT GQCA" document.

8 OTHER BUSINESS AND LEGAL MATTERS

Please refer to the relevant section of the "CPS LT GQCA" document.