evicertia
EVIDENCIAS CERTIFICADAS

Policy and Practice Statement of Qualified Electronic Registered Delivery Services

Trust Services

Evicertia
May 2021

Public

1 Table of Contents

2 Introduction

2.1 Presentation

Evicertia, S.L. (Evicertia) is a Certification Service Provider (hereinafter referred to as “CPS”) that offers “Qualified Electronic Registered Delivery Services” (QERDS) in accordance with Section 7 of REGULATION (EU) No. 910/2014 of the European Parliament and of the Council of 23th July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

2.2 Document Name and Identification

This document is the "Policy and Practice Statement of Qualified Electronic Registered Delivery Service", hereinafter "PPSQERDS".

This document must be read along with Evicertia Trusted Services CSP, it is subsidiary to. Throughout this PPSQERDS, reference is made to sections of said CPS that will serve to complete this document.

2.3 Participants in the certification services

Review this section in Evicertia's CPS.

2.4 Use of qualified electronic registered delivery service

2.4.1 Permitted uses

The QERDS generates and issues *affidavits*[1] for the purpose of proving that there was a series of data related to the communication between a sender and a receiver 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 hired these services

2.4.2 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 law.

2.5 Policy management

2.5.1 Organization that manages the document

The details of the company are the following:

- Evicertia, S.L. (Evicertia)
- VAT#: ESB86021839

[1] *Affidavit*: a legal document that serves as a proof or statement made under oath before a Court, or as a surety or guarantee in other cases. Ⓒ Diccionario panhispánico del español jurídico (Pan-Hispanic Dictionary of Legal Spanish).

- Madrid Mercantile Registry Volume: 28127, Book: 0, Folio 11, Section 8, Sheet M-506734, Registration 1.

2.5.2 Contact details of the organization

The contact details of Evicertia, S.L., are the following:

- Web: https://www.evicertia.com
- Email address: info@evicertia.com
- Phone: +34914237080
- Fax: +34911410144
- Postal address: Lagasca 95. 28006 Madrid. SPAIN.

2.5.3 Document management procedures

The documentary and organizational system of Evicertia guarantees, through the existence and application of the corresponding procedures, the correct maintenance of this document and the related service specifications.

3 Versions control

Version	Date	Comments
1.0	12/05/2021	The first version of this document is approved.

4 Publication and preservation

4.1 Repository

Evicertia has a Repository, in which information relating to the trust service is published. The publication repository can be reviewed at https://www.evicertia.com/.

This service is available 24 hours a day, 7 days a week and, in case of a failure in the system outside of Evicertia's control, it will make its best for the service to be available again according to the deadlines and established procedures regarding business continuity.

4.2 Publication of information of the certification services provider

Evicertia will publish the following information in its repository:

- Evicertia's Certification Practice Statement (CPS).
- The Policy Disclosure Statements, hereinafter "PDS" of the qualified delivery service.
- The public keys of the certificates used for QERDS.

4.3 Publication frequency

The information of the CSP, including the CPS, PDS and this PPSQERDS is published as soon as it is available.

Changes in the PPSQERDS are governed by the provisions of the management procedure of this document and in accordance with the applicable regulations.

4.4 Access control

Review this section in Evicertia's CPS.

5 Identification and authentication

5.1 Identification

In order to use Evicertia's QERDS, it is necessary that both the sender and the receiver of the communications have gone through Evicertia's identity verification process, and both parties must be subscribers to the service.

The process of verification of the identity of subscribers will be by physical presence at any of Evicertia's registration offices.

It will be necessary to submit the documentation (ID number, Passport) confirming that the person is who he says will be delivered, or in case of a legal person (companies, entities, corporations) the information of the legal representative (public deed or power of attorney) .

Once the person’s identity has been verified, the corresponding features of Evicertia QERDS will be activated for this user.

5.2 Sender’s Authentication

Sender’s authentication for sending communications will be carried out by means of a username (linking to his email) and a password, by providing the Service with means to apply complex password policies and secure resets of the same.

5.3 Receiver’s Authentication

The receiver’s authentication is carried out using a two-factor authentication with a random and temporary URL, and an OTP (One-Time Password) which will be sent to the receiver’s mobile phone or e-mail.

6 Operational Requirements

6.1 Access to the Service

Access to the several QERDS URLs will be carried out by means of secure protocols and encrypted communications.

6.2 Events and Evidences

As stated in article 3.36 of eIDAS regulation, the electronic registered delivery service is <<*a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;*>> therefore, Evicertia Service allows to collect evidence ensuring that the sender's electronic messages are delivered to its receiver, thus guaranteeing the accuracy and completeness of the evidence.

The person in charge of guaranteeing such accuracy and completeness is the CSP, through a series of cryptographic processes such as implementing electronic signatures and qualified time stamps. Both the signature process and the time stamps are provided by CSP in accordance with the eIDAS Regulation.

Evicertia's evidences are referred to as *affidavits* and they are documents that collect all expert information evidencing that an event has occurred, and it has not been subsequently modified. *Affidavits* may include:

- Sender and Receiver's data of electronic messages.
- The contents sent, along with the processed documents attached, that also include cryptographic summaries of the same.
- *Affidavits* may also include information about the following events:
    - Issuance and delivery to the receiver's mail server.
    - Delivery to the receiver's mail server or delivery failure if the message could not been sent.
    - Opening of message.
    - Or any subsequent actions taken by the receiver (if any).
    - The time zone will be UTC (Coordinated Universal Time).

In order to guarantee the integrity of the document and that it has not been subsequently modified, each *affidavit* is electronically signed by the service, and a qualified time stamp is included.

The sender will have access to all his *affidavits* in the qualified delivery service, during the relevant safekeeping period and for a minimum period of two years. The receiver will be able to access the *affidavits* by means of the support service or the sender's information. Once the term of the contract has ended, neither party will have access to the *affidavits*.

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

7 Physical, management and operations security controls

Review this section in Evicertia's CPS.

8 Technical security controls

Evicertia uses reliable systems and products, protected against any alteration and that guarantee the technical and cryptographic security of the certification processes they support.

8.1 Generation and installation of the key pair

8.1.1 Key pair generation

The qualified electronic certificates of the QERDS will be generated by eIDAS Qualified Service Providers, UANATACA (www.uanataca.com) and Firma Profesional (www.firmaprofesional.com), in accordance with their Certification Practices Statement and their Disclosure Statement, being available on their website.

Likewise, the Evicertia key ceremony procedures have been followed, within the high security perimeter assigned to this task. The activities carried out during the key generation ceremony have been registered, dated and signed by all the individuals participating in it, with the presence of an Auditor. Such records are kept for audit and follow-up purposes for an appropriate period determined by Evicertia.

Devices with FIPS 140-2 level 3 or Common Criteria EAL4+ certification are used to generate keys for qualified electronic certificates of the QERDS.

The keys are generated using the RSA public key algorithm, with a minimum length of 2048 bits.

QERDS certificates	2.048 bits	Up to 5 years

8.1.2 Sending the Public Key to the Certificate Issuer

The methods for sending the public key to the Trusted Electronic Service Provider is PKCS#10, another equivalent cryptographic proof or any other method approved by Evicertia.

8.1.3 Distribution of the certification service provider's public key

Evicertia's public keys are communicated to third parties relying on certificates, ensuring the integrity of the key and authenticating its origin, by publishing it in the Repository.

Users can access the Repository to obtain the public keys, and additionally, in S/MIME applications, the data message may contain a chain of certificates, which are then distributed to users.

The certificate of the root and subordinate certification authorities will be available to users on the Evicertia website.

8.1.4 Key Sizes

The length of the keys of the certificates used for signing *affidavits* shall be at least 2048 bits.

8.1.5 Generation of public key parameters

The public key of the certificates used for signing *affidavits* is preferably encrypted according to RFC 5280.

8.1.6 Checking the quality of public key parameters

The quality of the public key parameters shall be at least:

- Module length = 4096 bits
- Key generation algorithm: rsagen1
- Summary cryptographic functions: SHA256.

8.1.7 Generation of keys in computer applications or in hardware

All keys are generated in hardware, as described in the section "Key pair generation".

8.2 Private key protection

Review this section in Evicertia's CPS.

8.3 IT security controls

Review this section in Evicertia's CPS.

8.4 Technical life cycle controls

Review this section in Evicertia's CPS.

8.5 Network security controls

Review this section in Evicertia's CPS.

8.6 Engineering controls of cryptographic modules

Review this section in Evicertia's CPS.

8.7 Sources of Time

Review this section in Evicertia's CPS.

9 Compliance audit

Review this section in Evicertia's CPS.

10 Legal and commercial requirements

Review this section in Evicertia's CPS.

11 Annex I - Acronyms

The acronyms used in this Certification Practices Statement are shown below.

- CA: Certification Authority
- CN: Common Name
- CP: Certificate Policy
- CPS: Certification Practice Statement.
- CRL: Certificate Revocation List.
- CSP: Electronic Certification Services Provider/ Trust Service Provider
- CSR: Certificate Signing Request.
- DES: Data Encryption Standard.
- DN: Distinguished Name.
- DPC: Data Processing Center
- DSA: Digital Signature Algorithm.
- ETSI: European Telecommunications Standards Institute
- FIPS: Federal Information Processing Standard Publication.
- ISO: International Organization for Standardization.
- LDAP: Lightweight Directory Access Protocol.
- NTP: Network Time Protocol
- OCSP: On-line Certificate Status Protocol. OID: Object Identifier.
- PA: Policy Authority.
- PDS: Practice Disclosure Statement.
- PIN: Personal Identification Number.
- PKCS: Public-Key Cryptography Standards
- PKI: Public Key Infrastructure.
- PPSQERDS: Policy and Practice Statement of Qualified Electronic Registered Delivery Service
- QERDS: Qualified Electronic Registered Delivery Services)
- QSCD: Qualified Signature Creation Device.
- RA: Registry Authority
- RSA: Rivest-Shimar-Adleman. Type of encryption algorithm
- SHA: Secure Hash Algorithm. Algoritmo seguro de Hash
- SSL: Secure Sockets Layer
- TCP/IP: Transmission Control. Protocol/Internet Protocol
- TSA: Time Stamping Authority
- TSU: Time Stamping Unity