Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service

Velika Gorica, December 2023

Document information

Document name	Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service
Document version	1.3
Document status	Valid
Date of adoption	15.12.2023.
OID	**1.3.6.1.4.1.54777.1.1.2**
Document type	CPS
Document classification	Public
Owner	HP-Hrvatska pošta d.d., Poštanska 9, 10410 Velika Gorica, PIN: 87311810356, MBS: 080266264 (Commercial Court in Zagreb)
Contact	Optimization Office, Poštanska 9, 10410 Velika Gorica ePreporuka@posta.hr
Document placement	https://www.eposta.hr/info
Related CP	Qualified Electronic Registered Delivery Service Provision Policy OID: 1.3.6.1.4.1.54777.1.1.1

Revision history

Version	Date	Prepared by	Description of Change
1.0	01.10.2021.	Igor Ivaštanin	Initial version
1.1	01.01.2022.	Igor Ivaštanin	Additional clarifications made to the terms of providing the service
1.2	20.03.2023.	Marina Zečević	Additional clarifications made in relation to time synchronization
1.3.	15.12.2023.	Marina Zečević	Change of the organization in charge of administration of the Rules of Procedure

1. Introduction

The document "Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service" (hereinafter: Rules of Procedure) prescribes the rules of procedure which HP – Hrvatska pošta d.d., with its registered office in Velika Gorica, Poštanska 9, PIN: 87311810356, registered with the Commercial Court in Zagreb, MBS: 080266264, (hereinafter: HP d.d.) applies in the provision of a qualified electronic registered delivery service, pursuant to the 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 ("electronic IDentification, Authentication and trust Services", hereinafter: the eIDAS Regulation), the Act on Implementation of eIDAS Regulation, and the by-laws and standardisation documents ETSI EN 319 401, ETSI EN 319 521 and ETSI EN 319 522.

HP d.d. has implemented the infrastructure for the provision of a qualified electronic registered delivery service (hereinafter: QERDS) for its customers.

Qualified electronic timestamp used by HP d.d. when providing the service is outsourced from another qualified trust service provider which is on the EU Trusted List and it indicates the date and time of sending, receiving messages and possible changes of data.

HP d.d. uses an advanced or qualified electronic seal for sealing electronic registered delivery messages when sending and receiving messages, based on an electronic certificate (at least according to the NCP policy) issued by a qualified trust service provider and excludes the possibility of undetectable change of data.

Qualified electronic timestamp and at least an advanced electronic seal will ensure the integrity of the data and the authenticity of the data source.

Qualified trust services are regulated by the Act on Implementation of the eIDAS Regulation and the eIDAS Regulation, and these Rules of Procedure comply with the aforementioned regulation.

This Rules of Procedure refer to the entire HP d.d. infrastructure used to provide the qualified electronic registered delivery service.

The Rules of Procedure will be published on the website https://www.eposta.hr/info.

1.1. Reference documentation

Basic regulations

- 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
- Act on Implementation of the 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 (OG 62/2017)

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Act on Implementation of the General Data Protection Regulation (OG 42/18)

Subordinate Regulations

- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22 (5) 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
- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) 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
- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27 (5) and 37 (5) 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
- Regulation on the Provision and Use of Trust Services (OG 60/2019)

Standardisation documents

- ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management
- ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security management
- ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management
- ETSI EN 319 102-1 V1.1.1. (2016-05) – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI EN 319 401 V2.2.1. (2021-05) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.2.2. (2021-05) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.2.2. (2021-05) – 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
- ETSI EN 319 521 V1.1.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 522-1 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture

1.2. Identification data and OID code

Document name: Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service
OID: 1.3.6.1.4.1.54777.1.1.2
Version 1.3
Date: 15-12-2023
Document link: https://www.eposta.hr/info

1.3. Administration of Rules

1.3.1. Organisation in charge of the administration of the Rules of Procedure

Organisation competent for administration of the Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service:

HP – Hrvatska pošta d.d.
Optimization Office
Poštanska 9
10410 Velika Gorica
Republic of Croatia
email: ePreporuka@posta.hr

1.3.2. Procedure for the Adoption of Rules of Procedure

Each version of the Rules of Procedure shall remain in force until the new version of the Rules of Procedure enters into force.

The initiative for adoption and the initiative for amendments to the Rules of Procedure is given by the Office for Strategy and Development, whereas the announcement of the amendments and the amended Rules of Procedure will be available in the public repository of HP d.d.

The responsible persons of HP d.d. are competent for the adoption of the Rules of Procedure and amendments to the said Rules.

HP d.d. conducts a regular review of these Rules of Procedure once a year.

1.4. Definitions and abbreviations

1.4.1. Definitions

Electronic Registered Delivery Service App	A system consisting of hardware and/or software, which allows the sender and recipient to participate in data exchange with the electronic registered delivery service provider

Evidence of electronic registered delivery service	Data generated within the electronic registered delivery system, proving that a specific event in the system occurred at a specific time
Consignment	The electronic registered delivery service provider has delivered user content within the recipient's eBox QERDS defined by the General Terms of Use of the ePost Service.
Public key	A cryptographic key of a user which is publicly available, and which together with a private key enables digital signature verification or data encryption
Coordinated Universal Time (UTC)	Second-based time scale as defined by ITU-R Recommendation TF.460-5. For most practical applications, UTC is equivalent to the mean solar time at the zero meridian (0°). More accurately, UTC is a trade-off between very stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular rotation of the Earth (relative to the agreed Greenwich Mean Sidereal Time - GMST).
User Content	Original data produced by the sender, to be delivered to the recipient.
User	A natural or legal person that uses trust services.
Qualified Electronic Signature Certificate	A certificate for electronic signatures issued by a qualified trust service provider that meets the requirements set out in Annex I of the eIDAS Regulation.
Qualified Electronic Time Stamp	An electronic time stamp that meets the following requirements: (a) it connects the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; (b) it is based on an accurate time source linked to coordinated universal time; and (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by an equivalent method.
Qualified Trust Service Provider	A trust service provider that provides one or more qualified trust services and has granted the qualified status by the supervisory body.
Qualified Electronic Registered Delivery Service Provider	Trust service provider providing qualified electronic registered delivery service.
Qualified Electronic Registered Delivery Service Provider	Electronic registered delivery service that meets the requirements set out in Article 44 of the eIDAS Regulation
Cryptographic module	An element of the certification system that has the function of generating and/or storing keys during cryptographic operations (*Hardware Security Module*).

List of qualified service providers	Trusted List of certification service providers supervised/accredited by EU Member States
List of revoked certificates	List of revoked or suspended certificates, whose availability must be ensured to relying parties or other persons or systems (*Certificate Revocation List*).
Advanced Electronic Signature	Electronic signature which reliably guarantees the identity of the user and which: ▪ is uniquely linked to the user; ▪ unequivocally identifies the user; ▪ is created using data that the user can solely control and that is exclusively under the supervision of the user; ▪ contains a direct link to the data to which it relates in a way that unequivocally allows review of any modification of the original data.
Certificate revocation	Procedure for suspending the validity of certificates before their regular expiration.
Relying Party	A natural or legal person relying on electronic identification or a trust service.
Trusted roles	Roles that are assigned to employees and on which the safety of certification service provider's work depends. Trusted roles and related responsibilities must be clearly defined and described in the employee's job description
Shipment	Structured data in electronic form prepared by the sender and intended for electronic registered delivery, consisting of user content and metadata (name of the recipient, address of the recipient, etc.).
Sender	A natural or legal person which sends the user content.
Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service	Rules of procedure for the provision of electronic registered delivery services in accordance with the requirements of the eIDAS Regulation.
Recipient	The natural or legal person to whom the user content is addressed.
Private key	A cryptographic key of a user that is known only to the user, and together with the public key enables the creation of a digital signature or decryption of data.
Electronic Registered Delivery Service Provider	Trust service provider that provides electronic registered delivery service.
Conformity assessment body	A body competent to carry out the conformity assessment of a qualified trust service provider and the qualified trust services provided by such provider.
Handover	After the trusted authentication of the recipient, the user content is downloaded or rejected by the recipient through the QERDS

	application, or the scheduled deadline for delivery has expired regardless of the authentication of the recipient.
Signature validation	The process of verification and confirmation that the electronic signature is valid.
Signature verification	The process of verifying the cryptographic value of a signature using signature verification data.
Electronic Registered Delivery Service	An electronic service, which allows the transmission of data/shipment between the sender and the recipient, while securing evidence of sending and receiving of data and protection measures to reduce the risk of loss, theft, destruction or unauthorized change of data.

1.4.2. Abbreviations

ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
NCP	Normalized Certificate Policy
OID.	Object Identifier
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QERDSP	Qualified Electronic Registered Delivery Service Provider
QTSP	Qualified Trust Service Provider
QSCD	Qualified Signature Creation Device
TLS	Transport Layer Security
Tsp	Trust Service Provider

2. Policies and procedures

2.1. Trust Services Policy

The policy for trust services is the Qualified Electronic Registered Delivery Service Provision Policy of HP d.d.

2.2. Rules of Procedure for Trust Services

The rules are publicly available on the HP d.d. website and are regularly updated.
This Rules of Procedure address:

a) the method of authentication of the sender and the recipient;
b) safety measures to reduce the risk of loss, theft, destruction or unauthorized change of data;
c) limitations of the use of a qualified electronic registered delivery service (e.g. limitations on the availability of evidence);

d) obligations of the sender and the recipient;
e) obligations of the relying parties;
f) information on events in the electronic registered delivery service for which evidence will be created;
g) list of qualified trust service providers involved in the provision of this service (found in Schedule I hereof)

Key customer information can be found in the Terms of Qualified Electronic Registered Delivery Service.

2.3. Terms of Service

Users and HP d.d. shall enter into a contractual relationship for a qualified electronic registered delivery service (hereinafter: the Contract) in the manner specified in the General Terms and Conditions of Use of the ePost Service. The Agreement includes the Request for the use of a qualified electronic registered delivery service, the Notice of Acceptance, the Terms of Provision of a qualified electronic registered delivery service (hereinafter: Terms of Service), with all key terms regarding the provision of the service and all other components listed in the General Terms of Use of the ePost Service.

In the process of entering into the Contract, the user is getting familiar with all restrictions on the use of QERDS and the obligations of all parties involved in the provision of the service.

HP d.d. will retain signed Contracts and Terms of Service, which may also be in electronic form.

2.4. Information Security Policy

The principles of information security are described in the internal act Regulation on the Security of Information Systems.

2.5. Obligations of the QERDS provider

HP d.d., as a qualified trust service provider, is responsible for:

- correct identification of users when contracting the service,
- trusted authentication of senders and recipients,
- providing the service in a secure manner while ensuring the authenticity, confidentiality and integrity of the data,
- proper protection of personal data,
- conducting internal and external compliance reviews,
- compliance with all prescribed obligations.

In addition, HP d.d. provides QERDS in accordance with the eIDAS Regulation, the Act on the Implementation of the eIDAS Regulation, and standardisation documents. HP d.d. is responsible for the use of a reliable and credible information infrastructure which is used for the implementation of the qualified electronic registered delivery service.

2.5.1. Obligations of the user

Users will:

- provide accurate and complete information in the request for contracting the service,
- accept the Terms of Service and other related documents,
- keep authentication elements safe from loss, theft, damage or unauthorized use,
- report to HP d.d. any event that has compromised the security of authentication elements or a suspicion that such an event has occurred,
- refrain from taking advantage of any security failures or irregularities in the operation of the HP d.d. system, and notify HP d.d. immediately upon determination of such failures, as well as
- refrain from transferring its responsibilities in dealing with the qualified electronic registered delivery service to third parties.
- use the service in a lawful manner, in accordance with its permitted purpose and in compliance with applicable regulations.

2.5.2. Obligations of the relying party

Reasonable confidence in a qualified electronic registered delivery service for the relying party is achieved if, at the time of use:

- takes the necessary preventive safety measures,
- verifies advanced/qualified electronic seal and qualified electronic time stamp of HP d.d. by using trustworthy systems,
- uses reliable applications in a secure IT environment.

The relying party not acting in accordance with these Rules of Procedure and the obligations arising therefrom is solely responsible for the risks of trusting the advanced/qualified electronic seal and qualified electronic time stamp of HP d.d.

2.6. Limitation of Liability

Apart for what HP d.d. is expressly responsible for pursuant to the Clause 9. of the "Qualified Electronic Registered Delivery Service Provision Policy" and Clause 2.5. of these Rules, HP d.d. as a provider of qualified trust services is not liable for any other obligation or liability, especially not in the event that liability of HP d.d. under the given obligations would result from a breach of obligations and liability caused by other participants listed in the Clause 9 of the said Policy and Clause 2.5. of these Rules.

HP d.d. is not liable for damages, including indirect damages or loss of revenue, loss of data or other damages related to qualified trust services, caused by the use of electronic registered delivery of other service providers or the use of QERDS of HP d.d. in other way than as permitted in this Rules.

3. BASIC CONCEPT

3.1. Integrity and confidentiality of user content

HP d.d., as a qualified trust service provider, provides the service in accordance with the eIDAS Regulation, the Act on the Implementation of the eIDAS Regulation, and standardisation documents, ensures the availability, integrity and confidentiality of user content and metadata, during transmission and storage.

Electronic documents are protected by an electronic signature/seal, supported certificate issued pursuant at least ETSI 319 411-1 NCP policy by a qualified trust service provider (QTSP), generated in such a way as to prevent undetectable change of data.

HP d.d. must check the correctness of the electronic seal and time stamp and the qualification of the QTSP (EU Trust List) by periodically reviewing whether the service provider of qualified certification and issuance of time stamps is on the EU Trust List. This qualification check is carried out by inquiry on the EU Trust List. Reviews of the electronic signature and seal as well as of the qualified electronic time stamp are carried out in accordance with ETSI EN 319 102.

QERDS supports the signing of shipments in two ways:

- delegated scenario – signature is executed by the service provider,
- additional security scenario – signature executed by the sender.

3.2. User identification and authentication

Identification of a natural person when contracting QERDS is performed in the following ways:

1) personally, with the operator at the post office by presenting the identity card or passport.
2) by remote electronic registration with digital signature supported by a personal certificate accepted by HP, issued pursuant to the policies ETSI 319 411-1 NCP, ETSI 319 411-2 QCP-n or QCP-n-qscd.

Identification of a legal person or a natural person who is the registered business operator when contracting QERDS is performed in the following ways:

1) Personally by the authorized representative of the legal person or by the natural person who is the registered business operator, with the sales representative, by presenting the identity card and by collecting and verifying data on the legal person or the registered business (full name and legal status, proof of existence and proof of the authorized representative, e.g. from the competent register (by bringing an extract or printout of an electronic record from the register and/or online inquiry into the register). In case an attorney contracts a service for a legal person or for a registered business operator, it is also necessary to obtain power of attorney, which is enclosed to the contract itself and on which the signature of the authorized representative of the legal person must be notarized.
2) By remote electronic registration, using digital signature supported by a business certificate issued pursuant to the policies ETSI 319 411-1 NCP, ETSI 319 411-2 QCP-l or QCP-l-qscd.

For the purpose of determination of the identity of natural persons, the following information and documents are collected:

a) Basic information on the person subject to certification and/or the authorized representative, which include:

- full name and surname,
- type and number of the document proving the identity
- PIN or in case the user does not have a PIN then another national identification number from the identification document,
- permanent residence address,
- date of birth.

b) Relevant documents are required to verify the name, identity and grounds for issuing the certificate.

c) Documents that are considered acceptable proof of identity for issuing certificates to natural persons are:

- personal ID card,
- passport.

After successful identification, the collected data is used to register users for QERDS. By registering, the user of the system is assigned with a secure electronic mailbox address (eBox QERDS). Upon completion of the registration, the user can also use QERDS.

The authentication of a natural person and/or a legal entity when logging into the system for the qualified service is carried out by two-factor authentication (username, password and OTP one-time password submitted via the mPost application or via SMS).

Trusted authentication must be used when using the mobile application to access the qualified electronic registered delivery service. The users log into it with their PIN numbers, which in addition to possessing a mobile device, which is proven by the ePost mobile application that is securely connected to the mobile device, constitutes a 2-factor authentication.

The mobile application checks the PIN entered and:
a) in case of three incorrect entries, it is blocked for 5 minutes;
b) in case of three subsequent incorrect entries after unblocking, it is blocked for an additional 5 minutes;
c) in case of three subsequent incorrect entries after the second unblocking, it is deactivated and its reactivation is required.

OTP is generated on the side of the server (random number of 6 digits), at the request of the user from the ePost mobile application, it is linked to the user and is valid for a certain predefined time. If the user does not have the ePost mobile application, the user can request OTP delivery via SMS when logging in to the qualified service system.

A detailed overview of the use of the ePost mobile application and the entry of the OTP generated in the mobile application are shown in the document "eBox eDelivery, Performance Documentation".

3.3. Time reference

The date and time of sending, receiving and any modification of the user content are marked with a qualified electronic time stamp. HP d.d. in this implementation uses an outsourced service provider of a qualified electronic time stamp who is on the EU Trusted List (European Trust List). The EU Trusted List is regularly checked for this service provider. In addition to user content, all evidence in the QERDS system (hereinafter: QERDS evidence) is marked with a qualified electronic time stamp.

3.4. Events and Evidence

The system provides QERDS evidence of the submission of the shipment, and of the consignment and/or handover of the shipment. QERDS evidence is protected by an advanced/qualified electronic seal, supported by a certificate issued under at least ETSI 319 411-1 NCP policy and a qualified electronic time stamp (PAdES Baseline level LT or LTA) generated by a qualified trust service provider (QTSP).

The evidence provided to the sender is identical in internal delivery (blackbox model) and external delivery (4-corner model). They are delivered to the sender by its ERDS provider (S-ERDS), and in external delivery, the source of evidence is mainly the recipient's ERDS provider (R-ERDS). The following table describes the events in which evidence is provided to the sender.

Table 1. Sender Evidence

Event	Event Type	Source of evidence	Provision of evidence
Submission	Accepted submission Rejected submission	S-ERDS	It is mandatory to save the evidence and make it available to the sender through sender's mailbox.
Consignment	Successful consignment Failed consignment	S-ERDS (BB) R-ERDS (4C)	It is mandatory to save the evidence and make it available to the sender through sender's mailbox.
Handover	Successful handover Declined handover Handover time expired	S-ERDS (BB) R-ERDS (4C)	It is mandatory to save evidence for all shipments, and evidence is available to the sender through sender's mailbox only for shipments with a return receipt. A notification with the evidence is sent to the sender's mailbox

Event	Event Type	Source of evidence	Provision of evidence
			and to sender's e-mail address, only for shipments with a return receipt. For shipments without a return receipt, evidence of delivery may be available to the sender upon request.

Except the evidence for the sender, there is evidence for QERDS providers in external delivery (4-corner model), and the events in which they are provided are described in the following table.

Table 2. Evidence for ERDS Provider

Event	Event Type	Source of evidence	Provision of evidence
Relay	Accepted Declined Failed	portable ERDS	Mandatory
Transmission of non-ERDS	Successful Failed Received from non-ERDS	portable ERDS	Optional

The semantics of QERDS evidence are in accordance with clause 8 of standard EN 319 522-2.

QERDS evidence is kept for 10 (ten) years.

Records from the system are stored in a secure manner to ensure confidentiality, integrity and availability of data. It is not allowed to alter the data in records/archive.
Records shall note:

- User identification data and log and archive all events related to the verification of the initial and further identification of the sender and recipient
- User authentication data
- Proof that the sender's identity was initially verified
- Records of the operation of the ERDS system, Verification of identity and activities of the sender, recipient and communication
- Proof of identity verification of the recipient before submission or handover of the shipment
- A means of proving that the user content has not been changed during transmission
- Hash of all user content
- Time stamps corresponding to the date and time of submission, consignment and handover of the shipment.

In addition, system records are noted:

- Employee activities with trusted roles in the trust services system
- All security events, security policy changes, system boot, shutdown and crash, hardware issues, changes to firewalls and routers.

Records and archives are kept for 10 (ten) years, and additionally noted system records for 2 (two) years and are not available after that.

3.5. Interoperability

For the purpose of harmonizing the electronic registered delivery service with the eDelivery standard, AP (Access point) and SML (Service Metadata Locator) components have been added to the system. The SML component is a cloud service, implemented and maintained by the IT department of the EU Commission.

The eDelivery concept is based on the so-called four-corner model. Nodes one and four represent background systems that do not exchange messages directly but through the service provider's AP components represented by nodes two and three. The back-end system exchanges messages through the public network in an interoperable way through AP components.

The sender's service provider dials the AP component, which ensures the sealing of the shipment using an advanced/qualified electronic seal (in accordance with ETSI EN 319 102), a qualified time stamp and encryption with the public key of the recipient's service provider.

When receiving the shipment, the recipient's service provider decrypts the shipment with its private key, checks the advanced/qualified electronic seal with the public key of the sender's service provider and the time stamp in accordance with ETSI standards EN 319 102 and EN 319 421.

The recipient's service provider sends a signed ERDS evidence of submission to the sender's service provider, which is then available to the sender.

When sending and receiving a shipment, reliable authentication of the sender and recipient is performed with the establishment of the TLS protocol in transmission (encryption of data in transmission).

4. Risk assessment

The risk assessment for the provision of QERDS is performed and documented within a separate document "Risk Assessment in the Provision of a Qualified Electronic Registered Delivery Service".

5. QERDS management and operations

5.1. Internal organization

With regards to risk of liability for damages pursuant to the Article 13 of the eIDAS Regulation, HP d.d. has sufficient financial resources and appropriate liability insurance. HP d.d. has sufficient resources

and financial stability to provide qualified trust services. HP d.d. has valid contracts with all external companies, which are involved in the implementation and maintenance of the system for the provision of a qualified electronic registered delivery service. Critical functions are carried out based on the principle of "two pairs of eyes" and reliable authentication.

5.2. Supervision of employees' work

Trusted roles represent the basis of trust for the provision of a qualified trust service, they are assigned to authorized and competent employees of HP d.d. Each trusted role has clearly defined tasks, obligations and responsibilities.

Trusted roles include roles:

- Security Officer – trusted role responsible for:
  - implementation of security rules in the system for the provision of qualified trust services
  - configuration of rules for creating log and audit records
  - drafting and maintaining these Rules, the Certification Policy and other publicly available documents
  - cryptographic key management
- System Administrator - trusted role responsible for configuration and maintenance of all hardware and software components of the QERDS system
- System Operator - trusted role responsible for conducting backup and recovery procedures, managing user accounts in the system and supervising the operation of QERDS components
- System Auditor - trusted role responsible for reviewing audit records, reports on system operation and conducting internal audits in the system according to these Rules and the QERDS Policy
- Identity Verification Officer – ensures that the user identity verification process complies with the definition in this Rules and
- Registration officer – a trusted role responsible for conducting and supervising the user registration process.

Trusted roles were assigned to HP d.d. employees by a separate Decision.
Employees assigned with the role of Security Officer may be assigned with the trusted role of Identity Verification Officer and no other.
Employees assigned with the role of System Administrator may be assigned with the trusted role of System Operator and no other.
Employees assigned with the role of System Operator may be assigned with the trusted role of System Administrator and no other.
Employees assigned with the role of System Auditor may only be assigned with that trusted role.
Employees assigned with the role of Identity Verification Officer may be assigned with the trusted role of Security Officer and no other.
Employees assigned with the role of Registration Officer may only be assigned with that trusted role.

The tasks related to the provision of QERDS are carried out exclusively by authorized employees, in sufficient numbers, knowledge, experience and qualifications. The job description of trusted roles

defines the mandatory expertise of candidates for working with cryptographic technologies as well as expertise regarding the protection of computer and information systems. Employees with trusted roles in HP d.d. may not be employed or engage in other business relationship with other qualified trust service providers.

Before the commencement of work position of trusted roles, HP d.d. conducts appropriate candidate checks to assess their ability and reliability in accordance with the needs of trusted roles. Employees performing trusted roles in HP d.d. are continuously educated and trained in accordance with the needs of their trusted roles and they possess the documentation necessary to perform the activities in accordance with the authorizations of the assigned trusted role. Unauthorized actions by HP d.d. employees with trusted roles constitute a breach of employment obligations in accordance with the provisions of applicable regulations and internal regulations.

External partners, i.e. persons from other business entities who perform tasks on the basis of a business cooperation agreement, perform their functions with the same obligations as employees of HP d.d. who perform functions in the system and appropriate internal acts. Renewal of training of trusted roles performers from the system is carried out in accordance with the training plans of HP d.d.

5.3. Asset Management

All components of the QERDS delivery system are clearly identified, listed and classified in accordance with safety and business importance. Media containing archival and backup data of the system in electronic form is stored in a separate protected location with appropriate technical and physical protection systems. Media are adequately protected against damage, theft and unauthorized access. Data from discarded media is destroyed in a safe manner, by electronic deletion or physical destruction of the media.

5.4. Access control

Each access authorization is granted through a controlled process. The principles of minimum necessary rights and segregation of duties are respected. The assigned authorizations are reviewed periodically. The layered protection systems associated with physical and logical access control ensure secure operation of electronic time stamp service.
The protection measures applied are:

- physical security of the environment,
- segregation of duties,
- network segmentation using firewalls,
- monitoring of events in the information system,
- reinforcement of the configuration of the information system components.

The system for the provision of QERDS is logically separated from the rest of IT infrastructure in HP d.d., it uses at least logically separated network (switches and firewalls) and server (physical and virtual) systems and interface consoles.

5.5. Cryptographic controls

The certificate for the qualified electronic seal of shipments and QERDS evidence is in a high-security system according to ETSI 319 411-2 QCP-l-qscd policy, which is stored on a secure cryptographic device (HSM). HP d.d. uses cryptographic devices in accordance with the FIPS PUB 140-2, level 3 and/or CC EAL 4+ standard.

A pair of keys for the qualified electronic seal of shipments and QERDS evidence is generated in the protected zone on the cryptographic device, with at least double control by authorized persons.

Private key backups are generated in a protected area where only authorized persons have access. Private key backups are also generated by authorized persons outside the cryptographic module (HSM) are exclusively in encrypted form and are stored in protected zones in physically separate locations. The minimum required number of key backups is made only to ensure the continuity of service.

After the expiration of private signature keys, all copies of the keys are destroyed and cannot be used. The qualified electronic time stamp service has been outsourced by HP d.d. from qualified trust service provider and its status on the EU Trusted List is regularly checked.

5.6. Physical protection of equipment and premises

Access to the protected area where the components of the system for the provision of QERDS are located is allowed only to authorized persons. In case access to this area must be provided to persons employed by external service providers, the stay of persons employed by external service providers in the protected area must be constantly monitored by HP d.d. employees. Every entry and exit from the protected area is recorded.
Technical and physical protection includes:

- physical protection – security guards and firefighters,
- video surveillance system,
- entry control,
- anti-theft and
- fire protection system.

Access and entry into the protected area is monitored 24 hours a day, 7 days a week.

5.7. Protection of operations

HP d.d. has implemented an information security system with appropriate security controls that ensures that operational and security risks are within the acceptable limit. These controls are:

- Management of operational and security risks, with the aim of identifying and assessing risks and identifying security controls to mitigate them;
- Incident management, a formal procedure with described steps to respond to incidents, with the aim of reducing damage and returning to normal operations;

- Business continuity management, in response to crisis situations and disasters, with regular testing and updating of Business Continuity Plans;
- Vulnerability and threat management process – identify vulnerabilities and threats, and take action to resolve them;
- Change management process, a formal process that ensures the maintenance of the level of security during changes in the system;
- Security information and event management (SIEM) – early detection of unauthorized access to the HP d.d. information system

5.8. Network security

The security of the computer network of the system for the provision of QERDS is based on the concept of dividing the network into network zones of different levels with the positioning of servers and other devices in different network zones separated by a firewall and access control. Network zones are separated by firewalls that only allow the necessary network traffic.
Network equipment configuration procedures ensure:

- change management,
- limiting access to the required minimum and
- prevention of unauthorized access.

Security controls at the network level are based on the firewall and the establishment of a secure communication protocol TLS (Transport Layer Security). All network traffic has been identified and approved. Additional security controls implemented in the system enable the analysis of network traffic and the prevention of network intrusion and the spread of malware.

Periodically and after each significant change in the system, a penetration test of the network infrastructure is performed.

5.9. Incident management

Preventive safety measures based on the results of the risk assessment can reduce the number of incidents, but they cannot be completely eliminated. The ability to react to an incident in a timely and appropriate manner is key to detecting incidents, mitigating impacts, and restoring the full functionality of the services.
The key elements of incident management are:

- evaluation of events, incidents and crisis situations,
- defining the escalation level,
- roles in escalation,
- incident response procedures.

Information on security events and incidents is classified.

5.10. Collection of records for QERDS internal service

All components of the system for the provision of QERDS are configured in such a way that all events relevant for the security of system operation and transactions performed on the system are automatically recorded in the audit record. The servers for collecting audit records are located in the protected zone of HP d.d.
The following types of events related to the provision of a qualified electronic time stamp service are recorded in the audit record:

- all safety events,
- changes in security policy,
- booting,
- stopping and crash of the system,
- hardware problems,
- changes to firewalls and routers.

The time on all servers within the system for the provision of QERDS is synchronized pursuant to the UTC (Coordinated Universal Time) via the central service for time synchronization. Time synchronization performance is checked at least once a day. The audit records of the system for the provision of QERDS are kept for a minimum of 24 (twenty-four) months and may be used as evidence in court proceedings and in the event of termination of the QERDS service provision. Audit records for QERDS provision are reviewed regularly on a daily basis.

5.11. Business Continuity Management

Data and key software in the system of the provision of QERDS are backed up regularly. Backups of data and key software are stored within the protected zone of HP d.d. Recovery of data and key software from backups is regularly tested.

The Business Continuity Management Plan for the system for the provision of QERDS is a procedure for dealing with crises and critical incidents, and is regularly tested and updated. Critical business processes and their recovery parameters are regularly updated.

The Business Continuity Management Plan also includes a scenario for the loss, damage or suspected compromise of HP d.d. private keys for advanced/qualified electronic seal and cryptographic devices where these keys are stored.

5.12. Termination of QERDSP

On the planned termination of the provision of the qualified trust service HP d.d. will:

- notify all users of the service, relying parties and the national competent authority at least three (3) months before the planned termination of the provision of qualified trust services;
- make an effort to analyse the possibility of providing qualified trust services with another qualified trust service provider.

Detailed procedure for termination of the provision of trust service is prescribed in the internal document "Plan for Termination of the Provision of Trust Services".

In the event that HP d.d. cannot secure the provision of QERDS with another qualified trust service provider, HP d.d. will revoke the advanced/qualified electronic seal certificates and destroy the associated private keys.

In the event of termination of the provision of a qualified trust service, HP d.d. will continue to maintain the user data collected in the registration process and the data generated in the operation of the system, which are necessary for the provision of evidence in court, administrative and other proceedings, in accordance with applicable regulations or will contract their maintenance with another business entity.

5.13. Compliance

Supervision of the provision of qualified trust services within the scope of these Rules of Procedure is carried out by the competent national authority (Ministry of Economy and Sustainable Development) in accordance with the provisions of Regulation (EU) No. 910/2014 (eIDAS), implementing acts adopted thereof and the Act on Implementation of Regulation (EU) No. 910/2014.

External compliance reviews shall be carried out at least every 2 (two) years in accordance with eIDAS Regulation and ETSI EN 319 403.

Regular monitoring of the information security management system to verify compliance with ISO/IEC 27001 shall be carried out at least every 12 (twelve) months.

Internal compliance reviews are carried out periodically at least once a year, before the provision of new qualified trust services, and after significant changes in the system for the provision of QERDS. The compliance assessment includes evaluation of the following areas of providing qualified trust services:

- completeness and accuracy of documentation;
- implementation of requirements for qualified trust services;
- organizational processes and procedures;
- technical processes and procedures;
- implemented information security measures;
- trustworthy systems;
- physical security of the sites in question.

The description of the said evaluation of the compliance is defined in the compliance evaluation plan.

HP d.d., in accordance with the objective and reasonable possibilities of software support and the properties and functionalities of the QERDS service, has taken appropriate measures to enable the highest possible level of observation, operability, comprehensibility and stability of the QERDS service, all in order to make this service equally available to all users. It is important to note that HP d.d., in addition to the digital QERDS service, enables the provision of an equivalent substitute service of registered delivery that is not in digital form.

6. Entry into force; date of application of these terms;

These Rules enter into force on the date of their adoption and apply from 15 December 2023, whereby the Rules of Procedure for the Provision of a Qualified Electronic Registered Delivery Service of 20 March 2023 shall expire.

Number: HP-19/1-038964/23

HP-Hrvatska pošta d.d.
President of the Management Board

Ivan Čulo

Schedule I List of qualified trust service providers

HP d.d. uses the services of the following qualified trust service providers:

Qualified electronic time stamp

- Name

AKD d.o.o.

- Trade name

AKD d.o.o.

- Postal address

Savska cesta 31
10000 - HR

- Electronic address

helpdesk-kid@akd.hr

- Information URL

https://www.id.hr/hr

- Trusted List URL

https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/HR/2

- ID

OID: 1.3.6.1.4.1.43999