# Practice Statement for Qualified Electronic Registered Delivery Service

Velika Gorica, November 2026.

.

| | |
|---|---|
| **Title:** | Practice Statement for Qualified Electronic Registered Delivery Service |
| **Document version:** | 1.4 |
| **Document status:** | Valid |
| **Issued on:** | 17.11.2026. |
| **OID:** | **1.3.6.1.4.1.54777.1.1.2** |
| **Type of document:** | CPS |
| **Classification of document:** | Public |
| **Owner:** | HP-Hrvatska pošta d.d., Poštanska 9, 10410 Velika Gorica<br>VAT No.: 87311810356, MBS: 080266264 |
| **Contact:** | Product Management, Poštanska 9, 10410 Velika Gorica<br>ePreporuka@posta.hr |
| **Document repository:** | https://www.eposta.hr/info |
| **Linked CP** | Certificate Policy for Qualified Electronic Registered Delivery Service OID: **1.3.6.1.4.1.54777.1.1.1** |

**Change history:**

| Version | Date | Made by | Change description: |
|---|---|---|---|
| 1.0 | 01.10.2021. | Igor Ivaštanin | Initial version |
| 1.1 | 01.01.2022. | Igor Ivaštanin | Added additional clarifications on service provision |
| 1.2 | 08.03.2023. | Marina Zečević | Added additional clarifications regarding time synchronization |
| 1.3 | 11.11.2025. | Marina Zečević | Updating the competent organizational unit and reference documentation, defining the obligation to report significant changes in the provision of the service and assigning responsibilities for network and information security |
| 1.4 | 12.11.2026. | Marina Zečević | Updating timeline for obligation to report significant changes in the provision of the service and competent national authority |

.

## 1. Introduction

These "Practice Statement for Qualified Electronic Registered Delivery Service" (hereinafter referred to as Practice Statement) set forth the rules of conduct implemented by HP – Hrvatska pošta d.d. (hereinafter referred to as HP d.d.) in the provision of its qualified electronic registered delivery service in accordance with 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 and Regulation (EU) No 1183/2024 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework ("**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices", hereinafter referred to as the eIDAS Regulation), the eIDAS Regulation Implementing Act, the relevant subordinate legislation, and normative documents ETSI EN 319 401, ETSI EN 319 521 and ETSI EN 319 522.

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

The qualified electronic time stamp used by HP d.d. in the provision of this service has been outsourced to another qualified trust service provider being on the EU Trusted List and it is used to indicate date and time of sending, receiving messages and possible change of data.

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

Such qualified electronic time stamp and advanced electronic seal shall ensure data integrity and authenticity of the source of information.

The qualified trust services are defined in the eIDAS Regulation Implementing Act and the eIDAS Regulation and these Rules are aligned with such legislation.

These Practice Statement apply to the entire infrastructure of HP d.d. used to provide the qualified electronic registered delivery service.

These Practice Statement shall be published on HP d.d.'s website: https://www.eposta.hr/info

### 1.1. References

**Primary legislation**

- 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 1183/2024 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
- Act Implementing 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 (Official Gazette No 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)
- General Data Protection Regulation Implementing Act (Official Gazette No 42/18)

**Secondary legislation**

- 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
- Ordinance for the Provision and Use of Trust Services (Official Gazette No 60/2019)

**Normative documents**

- ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- ETSI EN 319 102-1 V1.4.1. (2024-06) – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI EN 319 401 V3.1.1. (2024-06) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.4.1. (2023-10) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

.

- ETSI EN 319 411-2 V2.3.1. (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 V1.2.1 (2024-01) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture

### 1.2. Identifying particulars and OID

Title: Practice Statement for Qualified Electronic Registered Delivery Service
OID: 1.3.6.1.4.1.54777.1.1.2
Version: 1.4
Date: 17.11.2026.
Link: https://www.eposta.hr/info

Unique OID (Object Identifier) **1.3.6.1.4.54777** is assigned to HP d.d. Based on that, HP d.d. assigned OID **1.3.6.1.4.1.54777.1.1.2** to this Practice Statement
Method of OID allocation, explanation of digits after unique OID:

- first digit: 1 – documentation
- second digit: 1 – main documentation
- third digit: 1-CP, 2-CPS

### 1.3. Administration of the Practice

#### 1.3.1. Organization responsible for administering these Practice Statement

The organization responsible for administering the Practice Statement:
HP - Hrvatska pošta d.d.
Product Management
Poštanska 9
10410 Velika Gorica
Republic of Croatia
email: ePreporuka@posta.hr

#### 1.3.2. Practice Statement issuance procedure

Each version of the Practice Statement remains effective until such time a new version of the Practice Statement enters into effect.
Strategy and Development Office may propose initiatives to amend the Practice Statement. Such amendments must be notified in advance and such amended Practice Statement shall be available in

.

HP d.d.'s public repository. HP d.d.'s qualified persons shall be responsible for the adoption of these Practice Statement and any amendments thereto.
At least once a year HP d.d. shall conduct a revision of these Practice Statement.

### 1.4. Definitions and acronyms

#### 1.4.1. Definitions

| | |
|---|---|
| **Electronic registered delivery service app** | A system comprising hardware and/or software, which allows the sender and recipient to participate in the exchange of data with the electronic registered delivery service provider |
| **Proof of electronic registered delivery service** | Data generated within the electronic registered delivery system, which prove that a specific event occurred within the system at a specific time |
| **Consignment** | The electronic registered delivery service provider has delivered user content within the recipient's QERDS eBox as defined in the General Terms and Conditions of Using the ePost Service. |
| **Public key** | A user's cryptographic key which is publicly available and which enables in combination with a private key verification of a digital signature or data encryption |
| **Coordinated Universal Time (UTC)** | A second-based time scale as defined in ITU-R Recommendation TF.460-5. For most practical purposes, UTC is equivalent to the mean solar time at 0° longitude. Specifically, UTC is a compromise between the very stable atomic time (Temps Atomique International - TAI) and the solar time derived from the Earth's irregular rotation (in relation to the agreed Greenwich Mean Sidereal Time - GMST). |
| **User content** | Original data created by a sender, which need to be delivered to a recipient. |
| **User** | A natural or legal person using trust services. |
| **Qualified electronic signature certificate** | An electronic signature certificate issued by a qualified trust service provider and satisfying the requirements defined in Annex I to the eIDAS Regulation. |
| **Qualified electronic time stamp** | An electronic time stamp satisfying the following requirements:<br>(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;<br>(b) it is based on an accurate time source linked to Coordinated Universal Time; and<br>(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method. |

.

| | |
|---|---|
| **Qualified trust service provider** | A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body. |
| **Qualified electronic registered delivery service provider** | A trust service provider providing the electronic registered delivery service. |
| **Qualified electronic registered delivery service** | An electronic registered delivery service which meets the requirements laid down in Article 44 of the eIDAS Regulation. |
| **Hardware Security Module** | An element of the certification system which generates and/or stores keys in the course of cryptographic operations. |
| **Trusted List** | A reliable list of certification service providers supervised/accredited by EU Member States. |
| **Certificate Revocation List** | A list of revoked or suspended certificates, which must be made available to relying parties or other persons or systems. |
| **Advanced electronic signature** | An electronic signature which reliably guarantees the user's identity and is:<br>▪ uniquely linked to the user;<br>▪ capable of unambiguously identifying the user;<br>▪ created using electronic signature creation data that the user can, with a high level of confidence, use under his sole control; and<br>▪ linked to the data signed therewith in such a way that any subsequent change in the data is detectable. |
| **Certificate revocation** | A process to end the validity of a certificate prior to its scheduled expiry date. |
| **Relying party** | A natural or legal person that relies upon an electronic identification or a trust service. |
| **Trusted roles** | Roles assigned to employees, which ensure the security of certification service provider's operation. Such trusted roles and the associated responsibilities must be clearly defined and described within such employee's job description. |
| **Item** | Structured data in electronic form, prepared by the sender and intended for electronic registered delivery, comprising user content and metadata (recipient's name, recipient's address, etc.). |
| **Sender** | A natural or legal person that sends user content. |
| **Practice Statement for Qualified Electronic Registered Delivery Service** | Practice Statement for Qualified Electronic Registered Delivery Service in accordance with the requirements laid down in the eIDAS Regulation. |
| **Recipient** | A natural or legal person to whom user content is addressed. |

.

| | |
|---|---|
| **Private key** | A user's cryptographic key known only to that user, which enables in combination with a public key creation of a digital signature or data decryption. |
| **Electronic registered delivery service provider** | A trust service provider that provides the electronic registered delivery service. |
| **Conformity assessment body** | A body accredited in accordance with the applicable regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides. |
| **Handover** | After the recipient is reliably authenticated, the user content has been accepted or rejected by the recipient via the QERDS app or the handover time limit has expired with or without recipient identification. |
| **Signature validation** | A process to verify and confirm that an electronic signature is valid. |
| **Signature verification** | A process to verify the cryptographic value of a signature by using signature verification data. |
| **Electronic registered delivery service** | An electronic service that makes it possible to transmit data/items between a sender and a recipient and provides proof of sending and receiving the data and measures to reduce the risk of loss, theft, destruction or unauthorized alteration of data. |

### 1.4.2. Acronyms

| | |
|---|---|
| **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. Policy applicable to trust services

.

The policy applicable to trust services is the Certificate Policy for Qualified Electronic Registered Delivery of HP d.d.

**2.2. Practice Statement for trust services**

These Practices are publicly available on HP d.d.'s website and are regularly updated.
These Practice Statement address:

a) the method of authenticating the sender and the recipient;
b) the protective measures to reduce the risk of loss, theft, destruction or unauthorized alteration of data;
c) the restrictions in the use of the qualified electronic registered delivery service (e.g. restrictions in availability of proof);
d) sender's and recipient's obligations;
e) relying parties' obligations;
f) the events for which proof will be generated in the electronic registered delivery system; and
g) the list of qualified trust service providers involved in the provision of this service (Appendix I to these Practices).

The crucial elements for users are provided in the Terms and Conditions of Providing the Qualified Electronic Registered Delivery Service.

**2.3. Terms and conditions of providing the service**

Users and HP d.d. establish a contractual relationship for the qualified electronic registered delivery service (hereinafter referred to as the Contract) as defined in the General Terms and Conditions of Using the ePost Service. Such Contract includes a request to use qualified electronic registered delivery, a Notice of Admission, the Terms and Conditions of Providing the Qualified Electronic Registered Delivery Service (hereinafter referred to as the Terms and Conditions of Service Provision) including all principal elements of service provision, as well as other integral parts thereof as specified in the General Terms and Conditions of Using the ePost Service.

In the process of entering into such Contract, the user is made aware of all restrictions in the use of the QERDS and the obligations of all parties involved in the provision of the service.

HP d.d. shall retain all signed Contracts and Terms and Conditions of Service Provision, including in electronic format.

**2.4. Information security policy**

The principles of information security are described in the internal corporate document titled "Information System Security Rulebook".

.

### 2.5. QERDS provider's obligations

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

- proper identification of the user at the time of arranging the service;
- reliable authentication of the sender and the recipient;
- providing the service in a secure way, by ensuring data authenticity, confidentiality and integrity;
- informing interested parties, users, relying parties and the national competent authority in the event of significant changes in the provision of the service one month before implementation, and in the case of the cessation of the service three months before planned cessation;
- appropriate personal data protection;
- conducting internal and external conformity audits; and
- complying with all prescribed obligations.

In addition, HP d.d. provides the QERDS in accordance with the eIDAS Regulation, the eIDAS Regulation Implementing Act and the relevant normative documents. HP d.d. is responsible for using reliable and authentic information infrastructure to implement the qualified electronic registered delivery service.

#### 2.5.1. User's obligations

Each user is required to:

- provide accurate and complete particulars in the service request;
- accept the Terms and Conditions of Providing the Service and other related documents;
- protect the authentication elements against loss, theft, corruption or unauthorized use;
- report to HP d.d. any event that compromises the security of authentication elements or any suspicion of such event;
- refrain from taking advantage of any security defects or irregularities in the operation of HP d.d.'s system and report them to HP d.d. immediately upon becoming aware of them; and
- refrain from delegating its qualified electronic registered delivery service responsibilities 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. Relying party's obligations

Reasonable reliance on the qualified electronic registered delivery service for a relying party shall be deemed achieved if such relying party, at the time of its use:

- takes the necessary preventive security measures;
- verifies HP d.d.'s advanced or qualified electronic seal and qualified electronic time stamp by using authentic systems; and
- uses reliable applications in a secure IT environment.

.

Where a relying party acts in violation of these Practice Statement and the relevant obligations defined herein, such relying party shall bear the risk of relying on HP d.d.'s advanced or qualified electronic seal and qualified electronic time stamp.

### 2.6. Limitation of liability

Other than HP d.d.'s liabilities specifically defined in Section 9 "Certificate Policy for Qualified Electronic Registered Delivery Service" and Section 2.5 of these Practices, HP d.d. shall, as a qualified trust service provider, not be liable for any other obligations or responsibilities, in particular where such liability of HP d.d. results from a breach of obligations or responsibilities of other participants specified in Section 9 of that Certificate Policy and Section 2.5 of these Practices.

HP d.d. shall not be liable for any damage, including indirect damage, loss of revenue, loss of data or any other damages associated with qualified trust services, resulting from the use of electronic registered delivery provided by other service providers or the use of HP d.d.'s QERDS in violation of these Practices.

## 3. Basic concept

### 3.1. Integrity and confidentiality of user content

As a qualified trust service provider, HP d.d. provides the service in accordance with the eIDAS Regulation, the eIDAS Regulation Implementing Act and the applicable normative documents, and also ensures the availability, integrity and confidentiality of user content and metadata while transmitted and stored.

Electronic documents are protected using an electronic signature/seal, supported by a certificate issued at least under the ETSI 319 411-1 NCP policy by a qualified trust service provider (QTSP) and generated in a way that makes it impossible to alter data undetectably.

HP d.d. verifies the correctness of the electronic seal and time stamp and the qualified status of the QTSP (EU Trust List) by periodically checking that the qualified certification and time stamp service provider is on the EU Trust List. Such qualified status is verified by making a query to the EU Trust List. Electronic signatures and seals and qualified electronic time stamps are verified in accordance with ETSI EN 319 102.

The QERDS supports signing for items in two ways:

a) delegated scenario, the service provider implements the signature; and
b) additional security scenario – the sender implements the signature.

.

### 3.2. User identification and authentication

At the time of arranging the QERDS, an *Individual* shall be identified as follows:

1) personally by the operator at a post office, subject to presenting an ID card or passport;
2) by remote electronic registration, using a digital signature supported by a personal certificate accepted by HP d.d., issued under ETSI 319 411-1 NCP, ETSI 319 411-2 QCP-n or QCP-n-qscd.

At the time of arranging the QERDS, a *Legal Entity* or a registered activity undertaken by a natural person shall be identified as follows:

1) personally by an authorized representative of the legal person or the natural person performing such registered activity, or by a sales representative subject to presenting an ID card or any other identity document and collection and verification of the particulars of the legal person or such registered activity (full name and legal status, evidence of existence and evidence of the authorized representative, e.g. from the relevant registry (by providing a physical extract or printout of an electronic record from and/or by making an online query to such registry)). Where an empowered person is arranging the service for a legal person or an individual performing a registered activity, it is also necessary to collect evidence of the power of attorney, which should be attached to the contract and whereupon the authorized representative's signature must be notarized.
2) by remote electronic registration, using a digital signature supported by a business certificate issued under ETSI 319 411-1 NCP, ETSI 319 411-2 QCP-l or QCP-l-qscd.

The following information and documents shall be collected for the purpose of identifying natural persons:

a) General particulars of the certification subject and/or such person's authorized representative, including:

- full name;
- type and number of the identity document;
- PIN or, in case the user does not have a PIN, another national identifier appearing in the identity document;
- address; and
- date of birth.

b) Appropriate documents must be provided to verify the name, identity and basis for certificate issuance.

c) The following are considered proof of identity acceptable for issuing certificates to natural persons:

- identity card; and
- passport.

After successful identification, the data collected shall be used to register the user for the QERDS. The user shall thereby be assigned a secure electronic mailbox address. On completion of registration and fulfillment of other conditions precedent to arranging the service, the user may use the QERDS.

.

When logging into the qualified service system, each Individual and/or Legal Entity shall be authenticated using two-factor authentication (username, password and OTP-one-time password delivered via the ePost mobile app or as a text message).

Reliable authentication shall be used when using the mobile app to access the qualified electronic registered delivery service. The user shall report it by his/her PIN, which constitutes, in combination with a mobile device demonstrated to exist via the ePost mobile app which is securely connected to such mobile device, two-factor authentication.

Rules of validation entered PIN validation:
a) app will be blocked for 5 minutes if user three times enter wrong PIN;
b) after unblocking, app will be blocked for another 5 minutes if user three times enter wrong PIN;
c) after second unblocking, app will be deactivated if user three times enter wrong PIN and reactivation will be required.

OTP is generated on server side (random 6-digit number) based on user request from ePošta mobile app, linked to user and valid for predefined period. If user doesn`t have ePošta mobile app, he can request OTP via SMS.

Detailed view of ePošta mobile app use and OTP entry can be found in “eBox eDelivery Izvedbena dokumentacija” document.

**3.3. Time reference**

The date and time of sending, receiving or any modification to any user content are identified by a qualified electronic time stamp. HP d.d. has outsourced the implementation thereof to a qualified electronic time stamp service provider appearing on the EU Trusted List. This service provider is regularly checked against the EU Trusted List. In addition to user content, such qualified electronic time stamp is also used to identify proof in the QERDS system (hereinafter referred to as QERDS proof).

**3.4. Events and proof**

The system secures QERDS proof of submission, consignment and handover of an item. Such QERDS proof is protected using an advanced or qualified electronic signature/seal, supported by a certificate issued at least under the 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 proof provided to the sender is identical to that used in internal delivery (*blackbox model*) and external delivery (*4-corner model*). It is provided to the sender by his/her ERDS provider (S-ERDS), whereas the source of such proof in external delivery is normally the recipient’s ERDS provider (R-ERDS). The table below describes the events where proof is provided to the sender.

.

***Table 1. Proof for the sender***

| Event | Type of event | Source of proof | Provision of proof |
|---|---|---|---|
| Submission | Submission accepted<br>Submission rejected | S-ERDS | The proof must be retained and available to the sender via his/her mailbox. |
| Consignment | Consignment successful<br>Consignment failed | S-ERDS (COMPONENT)<br>R-ERDS (4C) | The proof must be retained and available to the sender via his/her mailbox. |
| Handover | Handover successful<br>Handover rejected<br>Handover time expired | S-ERDS (COMPONENT)<br>R-ERDS (4C) | The proof must be retained for all items and is only available to the sender via his/her mailbox for items with a return receipt. A notice containing such proof is sent to the sender's mailbox and to his/her e-mail address, for items with a return receipt only.<br>In case of items without a return receipt, the proof may be made available to the sender on request. |

In addition to such proof for the sender, there is also proof for QERDS providers in external delivery (4-corner model) and the events where such proof is provided are described below.

***Table 2. Proof for the ERDS provider***

| Event | Type of event | Source of proof | Provision of proof |
|---|---|---|---|
| Relay | Submitted<br>Rejected<br>Failed | Relay ERDS | Required |
| Non-ERDS relay | Successful<br>Failed<br>Received by non-ERDS | Relay ERDS | Optional |

The semantics of QERDS proof are in compliance with Section 8 of EN 319 522-2.

QERDS proof is retained for 10 (ten) years.

System logs are stored in a secure way so as to ensure data confidentiality, integrity and availability. It is not permitted to alter any data in such logs/records.

.

The logs record:

- user's identifying particulars, including logging and archiving of all events relating to the verification of the initial and any further identification of the sender and the recipient;
- user's authentication data;
- proof that the sender's identity has been initially verified;
- ERDS system operation logs, verification of sender's and recipient's identities and activities, and communication;
- proof that the sender's identity has been verified before submission or handover;
- means of proving that the user content was not altered during transmission;
- a hash for the entire user content; and
- time stamps consistent with the date and time of submission, consignment and handover of an item.

System logs are also recorded:

- activities of employees with trusted roles within the trust service system;
- all security events, changes to the security policy, system interruption and failure, hardware issues, and changes to firewalls and routers.

Such logs and records are retained for 10 (ten) years and additionally recorded system logs are retained for 2 (two) years.

### 3.5. Interoperability

For the purpose of aligning 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 EU Commission's IT Department.

The eDelivery concept is based on a so-called four-corner model. Corners one and four represent background systems which do not exchange messages directly but via service provider's AP components representing corners two and three. The background system uses such AP component to exchange messages via a public network in an interoperable way.

The sender's service provider calls the AP component which ensures that the item is sealed using an advanced or qualified electronic seal (in accordance with ETSI EN 319 102), a qualified time stamp and encryption using the public key of the sender's service provider.

When receiving an item, the recipient's service provider decrypts the item using its own private key and verifies the advanced or qualified electronic seal using the public key of the sender's service provider, as well as the time stamp in accordance with EN 319 102 and EN 319 421.

The recipient's service provider sends signed ERDS proof of submission to the sender's service provider and such proof then becomes available to the sender.

.

At the time of sending and receiving an item, the sender and recipient are reliably authenticated by establishing a TLS protocol (encryption of data being transmitted).

**4. Risk assessment**

Risk assessments for QERDS purposes are carried out and documented in a separate document titled "Qualified Electronic Registered Delivery Service Risk Assessment".

**5. QERDS management and operations**

**5.1. Internal organization**

As regards the risk of liability for damage under Article 13 of the eIDAS Regulation, HP d.d. has sufficient funds available and carries appropriate liability insurance. HP d.d. has sufficient funds available and financial stability needed to provide qualified trust services. HP d.d. has effective contracts in place with all external entities involved in the implementation and maintenance of the qualified electronic registered delivery service system. Critical functions are performed on a 4-eyes basis and based on reliable authentication.

**5.2. Supervision of employees' work**

Trusted roles constitute the basis of trust for the provision of the qualified trust service and are assigned to HP d.d.'s authorized and competent employees. Each trusted role is matched with clearly defined, tasks, duties and responsibilities.
Such trusted roles include:

- *Security Officer* – a trusted role responsible for:
  - implementing security rules in the qualified electronic registered delivery service system;
  - configuring the rules for creating log files and audit trails;
  - formulating and making these Practices, the Certification Policy and other documents publicly available;
  - managing cryptographic keys; and
  - network and information security management;
- *System Administrator* – a trusted role responsible for configuring and maintaining all hardware and software components of the QERDS system;
- *System Operator* – a trusted role responsible for implementing backup and recovery procedures, managing user accounts within the system and monitoring the operation of QERDS system components;
- *System Auditor* – a trusted role responsible for reviewing audit trails and system operation reports and for conducting internal audits within the system in accordance with these Rules and the QERDS Provision Policy.
- *Identity Verification Officer* – ensures that the user identity verification process is conducted as defined in these Rules; and

.

- *Registration Officer* – a trusted role responsible for conducting and supervision the user registration process.

Such trusted roles are assigned to HP d.d.'s employees by a specific Decision.

Employees appointed with trusted role Security Officer can only be appointed to trusted role Identity Verification Officer and no other.
Employees appointed with trusted role System Administrator can only be appointed to trusted role System Operator and no other.
Employees appointed with trusted role System Operator can only be appointed to trusted role System Administrator and no other.
Employees appointed with trusted role System Auditor can only be appointed to that trusted role.
Employees appointed with trusted role Identity Verification Officer can only be appointed to trusted role Security Officer and no other.
Employees appointed with trusted role Registration Officer can only be appointed to that trusted role.

Tasks relating to the provision of the QERDS are only performed by a sufficient number of authorized employees having sufficient knowledge, experience and qualifications. The job description for each trusted role defines the professional skills each candidate is required to have regarding the use of cryptographic technologies and professional skills regarding computing system and information system security. An employee who is assigned a trusted role in HP d.d. may not be employed by or have any other business relationship with other qualified trust service providers.

Before a trusted role is assumed, HP d.d. screens its candidates to evaluate their ability and reliability as necessary for such trusted roles. Employees who are assigned trusted roles in HP d.d. are educated and trained on an ongoing basis as necessary for their trusted roles and are provided with documents needed to perform their activities according to the privileges attached to each trusted role. Any unauthorized action taken by an employee of HP d.d. who is assigned a trusted role shall be treated as a breach of employment duty under the applicable legislation and internal rulebooks.

External partners, i.e. persons employed by other entities who perform their services under business cooperation agreements, are imposed the same obligations as HP d.d.'s employees performing system functions in accordance with the relevant internal corporate documents. Holders of system trusted roles are trained in accordance with the relevant employee training plans of HP d.d.

**5.3. Asset management**

All components of the QERDS provision system are clearly identified, listed and classified based on security and business relevance. Media containing archival and backup copies in electronic format are stored at a separate secured site using appropriate technical and physical security systems. Such media are adequately protected against damage, theft and unauthorized access. Data contained in discarded media are securely destroyed by electronic erasure or physical destruction of the medium.

.

### 5.4. Access control

Each access authorization is given through a controlled process. Least privilege and segregation of duties principles are adhered to. Assigned privileges are periodically reviewed. Layered security systems connected with physical and logical access controls ensure that the electronic time stamp service process runs securely.
The following security measures are implemented:

- physical security of the environment;
- segregation of duties;
- network segmentation via firewalls;
- monitoring of events in the information system; and
- enhancing of information system component configurations.

The QERDS provision system is logically separated from the rest of HP d.d.'s IT infrastructure and uses at least logically separated network (switches and firewalls) and (physical and virtual) server system, as well as management consoles.

### 5.5. Cryptographic controls

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

The pair of keys used for qualified electronic seal for items and QERDS proof is generated within a protected zone, using a cryptographic device and no less than dual control by authorized persons.

Backup copies of private keys are generated in a protected zone, which may only be accessed by authorized persons. Such backup copies of private keys are created by authorized persons, are only available in encrypted form beyond the Hardware Security Module (HSM) and are stored in protected zones at physically separated locations. At least the number of backup copies of keys necessary to ensure service continuity are created.

On expiry of such private signature keys, all copies of the keys are destroyed and may no longer be used.
HP d.d. has outsourced the qualified electronic time stamp service to a qualified trust service provider and regularly checks its status against the EU Trusted List.

### 5.6. Physical security of equipment and sites

Access to a protected area containing components of the QERDS provision system is only allowed to authorized persons. In case it is necessary to allow access to such areas to persons employed by external service providers, each such person employed by an external service provider must be

.

accompanied by an employee of HP d.d. at all times while being in such areas. Each instance of entering and exiting a secured area is recorded.
Technical and physical security includes:

- physical security – security guards and firemen;
- a video surveillance system;
- transit control;
- an antiburglary system; and
- a fire protection system.

Access to and entry in such secured area are monitored on a 24/7 basis.

### 5.7. Security of operations

HP d.d. has implemented an information security system including appropriate security controls which ensure that operational and security risks remain on acceptable levels. Such controls are:

- Management of operational and security risks for the purpose of identifying and assessing such risks and defining security controls for their mitigation;
- Incident management – a formal procedure including descriptions of steps to be taken in response to incidents for the purpose of minimizing damage and restoring normal operation;
- Business continuity management in response to crises and disasters, including regular testing and updating of Business Continuity Plans;
- The process of managing vulnerabilities and threats designed to identify any vulnerabilities or threats and take action to rectify them;
- The change management process – a formal process ensuring that the required security level is maintained while making changes in the system; and
- Security Information and Event Management (SIEM) – early detection of unauthorized access to HP d.d.'s information system.

### 5.8. Network security

The security of the network system used to provide the QERDS is based on a concept of segmenting the network into network zones of different levels and positioning servers and other devices in different network zones separated by firewalls and access control. Such network zones are separated by firewalls that only allow necessary network traffic.
The procedures used for configuring network equipment ensure:

- change management;
- reduction of access to a minimum; and
- prevention of unauthorized access.

On the network level, security controls are based on firewalls and establishment of a TLS (Transport Layer Security) secure communication protocol. All network traffic is identified and approved. Further

.

security controls implemented in the system allow network traffic analysis and prevent network intrusions and malware dissemination.

The network infrastructure is subjected to penetration tests, both periodically and after each significant change.

### 5.9. Incident management

Preventive security measures based on risk assessment results may reduce the number of incidents but cannot completely eliminate them. The ability to respond to incidents in a timely and adequate manner is crucial for detecting incidents, mitigating their impacts and restoring full functionality of services.
The crucial components of incident management are:

- evaluation of events, incidents and crises;
- defining of escalation levels;
- escalation roles; and
- incident response procedures.

Information on security events and incidents are classified.

### 5.10. Collection of logs for the QERDS internal Service

All components of the QERDS provision system are configured to automatically record all events relevant to the security of the system and transactions conducted therein in audit trails. The servers used to collect audit trails are located in a secured zone within HP d.d.
The following types of events relating to the provision of the qualified electronic time stamp service are recorded in audit trails:

- all security events;
- changes to security policy;
- rebooting;
- system interruption and failure;
- hardware problems; and
- changes to firewalls and routers.

Time on all servers from the QERDS service provision system is synchronized according to UTC (Coordinated Universal Time) through a central time synchronization service. The success of time synchronization is checked at least once a day. Audit trails generated by the QERDS provision system are retained for at least 24 (twenty-four) months and may be used as evidence in judicial proceedings and in case of QERDS interruptions. Such QERDS audit trails are reviewed on a daily basis.

.

### 5.11. Business continuity management

Data and critical software within the QERDS provision system are regularly backed up. Backup copies of data and critical software are stored within HP d.d.'s secured zone. The recoverability of data and software from such backup copies is regularly tested.

The Business Continuity Plan relevant to the QERDS provision system is a procedure that defines the action to be taken in case of crisis or critical incidents and is regularly tested and updated. Critical business processes and their recovery parameters are regularly updated.

The Business Continuity Plan includes scenarios for loss, corruption or suspicion of compromise of HP d.d.'s private keys for the advanced or qualified electronic seal and cryptographic devices storing such keys.

### 5.12. Discontinuation of the QERDS

Where HP d.d. plans to discontinue the provision of the qualified trust service, it shall:

- notify all users of the Service, relying parties and the competent national authority at least three months in advance of such planned discontinuation of qualified trust services;
- use efforts to analyze the possibility of having another qualified trust service provider provide such qualified trust services.

In case HP d.d. is unable to arrange for the QERDS to be provided by another qualified trust service provider, HP d.d. shall:

- revoke the certificates for the advanced or qualified electronic seal and destroy the associated private keys.

In case HP d.d. ceases to perform the qualified trust service, it shall continue to support users' data collected in the process of registration and data resulting from system operation which are necessary to provide evidence in judicial, administrative and other proceedings in accordance with the applicable regulations or arrange for such data to be maintained by another entity.

Detailed procedure of termination of trusted service provision can be found in internal document "Plan prestanka pružanja usluga povjerenja".

### 5.13. Conformity

The competent national authority (Ministry of Justice, Administration and Digital transformation) supervises the provision of the qualified trust services contemplated in these Rules of Conduct in accordance with Regulation (EU) No 910/2014 (eIDAS), legislation implementing Regulation (EU) No 910/2014 and the Act Implementing Regulation (EU) No 910/2014.

External conformity audits are conducted at least every 2 (two) years in accordance with the eIDAS Regulation.

.

Regular audits of the information security management system are conducted at least every 12 (twelve) months for conformity assessment purposes, in accordance with ISO/IEC 27001.

Internal conformity audits are conducted at least once a year, before any new qualified trust services are provided and after any significant changes in the QERDS provision system.
Such conformity audits shall include the following areas of qualified trust service provision:

- integrity and accuracy of documentation;
- implementation of requirements applicable to qualified trust services;
- organizational processes and procedures;
- technical processes and procedures;
- implemented information security measures;
- authentic systems; and
- physical security of the sites concerned.

Such conformity assessment is defined in the Conformity Assessment Plan.

In accordance with objective and reasonable possibilities of software support, properties and functionalities of QERDS service, HP d.d. conducted appropriate measures for providing a higher level of possibilities perception, operability, comprehensibility and stability of QERDS service, and all to make service available to all users. It is important to note that HP d.d., except providing digital QERDS service, offers equivalent registered delivery service that is not in a digital form.

**6. Effective date; Applicability**

This Policy shall enter into force on the day of its adoption and shall apply as of 17th of November 2026., whereby the Rules of Conduct for the Provision of Qualified Electronic Registered Delivery Service from 31th of December 2025. cease to be valid.

Class: 025-02/26-06/44
No.: HP-03-02-26-5

HP-Hrvatska pošta d.d. (Croatian Post Inc)

| Member of the Management Board | President of the Management Board |
|---|---|
| Siniša Šukunda | Ivana Mrkonjić, PhD |
| Siniša Šukunda Digitally signed by Siniša Šukunda Date: 2026.11.17 12:46:14 +01'00' | Ivana Mrkonjić Digitally signed by Ivana Mrkonjić Date: 2026.11.17 13:19:31 +01'00' |

.

**Appendix 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**

**mailto: helpdesk-kid@akd.hr**

- **Information URI**

**http://www.id.hr/en**

- Trusted List URL

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

- Identifikacijska oznaka

OID: 1.3.6.1.4.1.43999