Certificate Policy for Qualified Electronic Registered Delivery Service

Velika Gorica, November 2026.

Document info:

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

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	15.12.2023.	Marina Zečević	Change of organization responsible for policy administration
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
1.4	17.11.2026.	Marina Zečević	Updating timeline for obligation to report significant changes in the provision of the service and competent national authority

1. Introduction

This "Certificate Policy for Qualified Electronic Registered Delivery Service" (hereinafter referred to as the Policy) sets forth the requirements implemented by HP – Hrvatska pošta d.d. (hereinafter referred to as HP d.d.), having its registered office at Poštanska 9, Velika Gorica, VAT No.: 87311810356, registered in the Registry of the Commercial Court in Zagreb under Reg. No. (MBS): 080266264 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 at least advanced electronic seal shall ensure data integrity and authenticity of the source of information.

This Policy applies to the entire infrastructure of HP d.d. used to provide the QERDS. This Policy shall apply to all participants in the QERDS provision system, including but not limited to HP d.d. as a service provider, users and relying parties.

The structure of this document is in compliance with normative document ETSI EN 319 411-1 V1.4.1. (2023-10) to the extent it applies to the provision of the QERDS.

The provisions of this Policy and the procedures relevant to their implementation are defined in greater detail in the "Practice Statement for Qualified Electronic Registered Delivery Service" (hereinafter referred to as the Practice Statement).

This Policy shall be published on HP d.d.'s website at: 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: Certificate Policy for Qualified Electronic Registered Delivery Service
OID: 1.3.6.1.4.1.54777.1.1.1
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 **1.3.6.1.4.1.54777.1.1.1** to this Certificate Policy
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. Participants and scope of service

Provider of the qualified electronic registered delivery service

HP d.d. provides the QERDS and uses in the process a qualified time stamp and an advanced or qualified electronic seal to protect the integrity of user content and QERDS proof and to match them with exact times.

Users

Users of the QERDS are natural and legal persons who have, at the time of arranging the QERDS, accepted the Terms and Conditions of Providing the Qualified Electronic Registered Delivery Service and other related documents relevant to the performance of the service. QERDS users may be senders and recipients of user content.

Relying parties

In the context of the QERDS, the relying parties are external service providers, being business entities that maintain business relationships with HP d.d. and accept QERDS proof, and not being users. Such relying parties must verify the advanced or qualified electronic seal, the qualified electronic time stamp and certificates, as well as the relevant certificate revocation list or use an OCSP facility to verify certificates used by HP d.d. before accepting information contained in QERDS proof.

Other participants

The other participants in the QERDS system are legal person that do not provide or use qualified trust services but do participate in certain parts of the process relating to the provision of qualified trust services. This group of participants includes the manufacturers and distributors of hardware and software used within the system to provide the QERDS, manufacturers and distributors of HSMs and other cryptographic devices, independent reviewers, etc.

1.4. Administration of the Policy

1.4.1. Organization responsible for administering this Policy

The organization responsible for administering the Certificate Policy for Qualified Electronic Registered Delivery Service:
HP - Hrvatska pošta d.d.
Product Management
Poštanska 9
10410 Velika Gorica
Republic of Croatia
email: ePreporuka@posta.hr

1.4.2. Policy issuance procedure

Each version of the Policy remains effective until such time a new version of the Policy enters into effect.
Strategy and Development Office may propose initiatives to amend the Policy. Such amendments must be notified in advance and such amended Policy shall be available in HP d.d.'s public repository. HP d.d.'s qualified persons shall be responsible for the adoption of this Policy and any amendments thereto.

1.5. Definitions and acronyms

1.5.1. 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 user, as defined in the General Terms and Conditions of Using the ePost Service, 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: (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; (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 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: ▪ uniquely linked to the user; ▪ capable of unambiguously identifying the user; ▪ created using electronic signature creation data that the user can, with a high level of confidence, use under his sole control; and ▪ 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 user 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	HP d.d. or another 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.

1.6.2. 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
OCSP	Online Certificate Status Protocol
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. Responsibility for publishing information and repositories

As a qualified trust service provider, HP d.d. maintains the repository of the QERDS provision system and is responsible for the documents and information contained therein. Such repository is publicly available and contains:

- the public key and certificate used by HP d.d. for its advanced or qualified electronic seal for user content and QERDS proof; and
- QERDS documents.

Such repository is also available at: https://www.eposta.hr/info

3. Identification and confirmation of identity

3.1. Identification and authentication of users

At the time of arranging QERDS delivery, 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.

Citizens of Republic of Croatia are identified by their personal ID card while foreigners are identified by their passport.
At the time of arranging QERDS delivery, 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.

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 (eBox QERDS). On completion of registration and fulfillment of other conditions precedent to arranging the service, the user may use the qualified electronic registered delivery service.

Registered user can´t open additional user account based on his personal data and will be warned about it by system or a registration officer.

The user shall also be identified as described above in case of any loss or corruption or suspicion of compromise of any of the authentication elements.

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 mPost app which is securely connected to such mobile device, two-factor authentication.

4. Operation of the service

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 Trusted List) by periodically checking that the qualified certification and time stamp service provider is on the EU Trusted List. Such qualified status is verified by making a query to the EU Trusted 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.

The system secures QERDS proof of submission, consignment and handover of an item. Such QERDS proof is protected using an advanced or qualified electronic 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), and is retained for 10 (ten) years.

5. Equipment and site security measures, organizational security measures and supervision of employees' work

The security measures implemented by HP d.d. are:

- definition and assignment of trusted roles for the QERDS;
- supervision of employees' work;
- asset management;
- access control;
- cryptographic control;
- physical protection of equipment and sites;
- operational security;
- network security;

- incident management;
- collection of audit trails;
- business continuity management; and
- defined action to be taken in case of service interruption.

The equipment and site security measures, organizational security measures and supervision of employees' work are detailed in the Rules of Conduct.

6. Technical security measures for the QERDS provision system

The pair of keys for the electronic seal is generated in a secure zone using a cryptographic device, subject to at least double check by qualified persons.
Key lengths and algorithms used in the QERDS provision system:

- HP QERDS – key length = 2048 bits, algorithm=sha256WithRSA

The validity period of HP QERDS certificates for the advanced or qualified electronic seal and the key pair is 2 years.

Cryptographic devices defined in FIPS PUB 140-2, level 3 and/or CC EAL 4+, are used to store private keys.

The private keys for the advanced or qualified electronic seal stored on a cryptographic module are enabled after the ePost system is started on HP d.d.'s servers. Reliable authentication is required to enable a cryptographic module. The private keys for the advanced or qualified electronic seal are disabled by turning off the ePost system.

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 (appearing on the EU Trusted List).

The other technical security measures for the QERDS provision system are detailed in the Practice Statement.

7. Certificate profiles and Certificate Revocation Lists

The qualified electronic seal used by HP d.d. to provide the QERDS is supported by a qualified certificate compliant with the ETSI 319 411-2 QCP-I-qscd policy, issued by a qualified trust service provider (QTSP), and makes it impossible to alter data undetectably.
The *Subject* field within the certificate contains the full name of the QERDS provider - HP d.d.
The path to such Certificate Revocation List and the OCSP facilities to verify the status of the qualified trust service provider that issued the certificate for HP d.d. is contained within the certificate, in the *CRL Distribution Points* and *Authority Information Access* fields.

8. Conformity audits and other checks

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 the eIDAS Regulation, its implementing regulations and the eIDAS Regulation

Implementing Act. 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.

9. Other financial and legal matters

9.1. Service fee

The use of the QERDS is subject to the rates defined in HP d.d.'s applicable pricelist.

9.2. Liability insurance

As regards the risk of liability for damage, HP d.d. carries appropriate liability insurance. HP d.d. has sufficient funds available and financial stability needed to provide qualified trust services.

9.3. Confidentiality of information

All employees of HP d.d. involved in the operation of the QERDS provision system are required to maintain all information/data defined in this Section in confidence. Such duty to protect the confidentiality of information/data also applies to employees of external service providers, who must be defined by a business cooperation agreement between HP d.d. and such external service provider. Any information/data within the QERDS provision system not designated as public shall be treated as confidential information/data, including all information/data necessary to provide qualified trust services, classified information, as well as information/data which, if disclosed, may cause damage to participants in the process.

9.4. Personal data protection

HP d.d. has adopted personal data protection measures in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th of 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). HP d.d. is responsible for protecting personal data processed in the course of providing qualified trust services.

During and after the user registration process, HP d.d. may collect personal data necessary to validly identify a user and other data necessary for valid provision of qualified trust services. Personal data which are collected by HP d.d. and which do not appear in any public records and/or registries that must be duly maintained for the purposes of providing qualified trust services shall be treated as confidential personal data duly protected by HP d.d.

Other than for the purposes of performing its obligations under law or contract, HP d.d. may use and disclose personal data subject to user's written consent, which may be given as part of the service request or subsequently.

Such personal data may be presented to third parties subject to the applicable legal requirements.

9.5. Protection of intellectual property

All data and documents published in the public repository of the QERDS provision system are intellectual property of HP d.d.
The Object Identifiers used are property of HP d.d., registered with the competent authority.
HP d.d. does not claim any intellectual property rights in the software used as part of the QERDS provision system, which is property of third parties.

9.6. Obligations and responsibilities

9.6.1. Service 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.

9.6.2. 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, damage 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.

9.6.3. Relying parties' 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 Rules of Conduct 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.

All changes that may affect provision of QERDS service, relying party is obliged to inform HP d.d.

9.7. Limitation of liability

As a qualified trust service provider, HP d.d. assumes no liability for any damage that may be incurred if:

- the user is registered based on inaccurate or unauthentic information provided by the requestor;
- the QERDS is used improperly or maliciously;
- the requestor encounters any inconvenience or incurs any loss between the time of submitting their registration request and the time of delivering the authentication elements to such requestor;
- the user or relying party acts in violation of this Policy and Rules of Conduct;
- user's or relying party's computer has been abused or security-compromised;

- the user has allowed unauthorized persons to use the QERDS;
- the user's or relying party's computer malfunctions;
- the infrastructure not under the responsibility or control of the QERDS provision system is interrupted or malfunctions; or
- any circumstances attributable to force majeure occur.

Other than HP d.d.'s liabilities specifically defined in Section 9.6 of this Policy, 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 that same Section of this Policy.

HP d.d. shall not be liable for any damage, including indirect damages, 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 this Policy and the Rules of Conduct.

9.8. Compensation for damage

Each participant in the QERDS provision system shall be liable to each party that incurs damage as a result of such participant's failure to comply with this Policy, the Rules of Conduct or any applicable regulations.

9.9. Resolution of complaints and disputes

Each user may submit to HP d.d. a complaint about the provision of the qualified trust service and HP d.d. shall respond to such complaint. Such complaints are submitted and the relevant procedure is conducted as defined in the General Terms and Conditions of Using the ePost Service. Any disputes between HP d.d. and a user that may arise in the course of using the QERDS shall be resolved amicably. Otherwise, such dispute shall be brought before the competent court in Zagreb and shall be governed by Croatian law. As an exception, if applicable, a natural person eligible to be treated as a consumer under the Alternative Resolution of Consumer Disputes Act may pursuant to such Act bring a consumer dispute before the relevant alternative dispute resolution body at: https://ec.europa.eu/consumers/odr.

9.10. Applicable regulations

HP d.d. provides the qualified trust service in accordance with the regulations specified in Section 1.1 of this Policy.

9.11. Effective date

This Policy shall enter into force on the day of its adoption and shall apply as of 17th of November 2026., whereby the Policy of providing qualified electronic registered delivery service from the 31th of December 2025. cease to be valid.

Class: 025-02/26-06/44
No.: HP-03-02-26-3

HP-Hrvatska pošta d.d. (Croatian Post Inc)
Member of the Management Board — President of the Management Board

Siniša Šukunda — Ivana Mrkonjić, PhD



