

Pursuant to Article 55 paragraph 7 of the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions (*Official Gazette of the Republic of Serbia* Nos. 94/17 and 52/21),

the Minister of Trade, Tourism and Telecommunications passes this

RULEBOOK

on the Conditions for the Provision of Qualified Electronic Delivery Service and Content of Electronic Receipt and Transmission Delivery Confirmation

Official Gazette of the Republic of Serbia No. 99 of 15 July 2020 and No. 74 of 23 July 2021

Scope

Article 1

This Rulebook shall govern in detail the conditions for the provision of qualified electronic delivery services and the content of electronic delivery and transmission confirmation issued by providers of qualified electronic delivery services.

Performance of Qualified Electronic Delivery Services in accordance with the Regulations, Standards and Recommendations

Article 2

The provider of qualified electronic delivery services (hereinafter referred to as the “service provider”) shall provide such service in accordance with the requirements of the following standards:

- 1) ETSI EN 319 401 – General Policy requirements for Trust Service Providers;
- 2) ETSI EN 319 521 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers (hereinafter referred to as “EN 319 521”);
- 3) ETSI EN 319 522 – Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services (hereinafter referred to as “EN 319 522”), including:
 - (1) Part 1: Framework and Architecture,
 - (2) Part 2: Semantic Contents,
 - (3) Part 3: Formats,
 - (4) Part 4: Bindings:
 - 319 522-4-1: message delivery binding,
 - 319 522-4-2: evidence and identification binding,
 - 319 522-4-3: capability/requirements binding;
- 4) ETSI EN 119 524-1 – Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 1: Testing conformance;

5) ETSI EN 119 524-2 – Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 2: Test suites for interoperability testing of Electronic Registered Delivery Service Providers;

6) The requirements contained in other standards to which the standards set out in items 1)–5) directly or indirectly refer, as well as other standards, documents and recommendations pertaining to the provision of qualified trust services set forth in this Rulebook and other regulations passed pursuant to the Law on Electronic Documents, Electronic Identification and Trust Services in Electronic Transactions (hereinafter referred to as the “Law”).

Application of General Provisions governing the Provision of Qualified Trust Services

Article 3

The qualified electronic delivery service provider shall, in compliance with the regulations governing the conditions for the provision of qualified trust services, apply the general provisions applicable to the provision of qualified trust services that pertain to:

- 1) The performance of qualified trust services in accordance with the regulations, standards and recommendations;
- 2) The contract for qualified trust service provision;
- 3) The content of the service provider’s bylaws;
- 4) The general terms and conditions of service;
- 5) The service provision policy and practical rules for service provision;
- 6) Information security;
- 7) Human resources;
- 8) Liability insurance for damage caused through the provision of qualified trust services;
- 9) The use of secure devices and products;
- 10) Keeping of relevant information;
- 11) The service provider’s closing-down plan.

Policy and Practical Rules for the Provision of Qualified Electronic Delivery Services

Article 4

The qualified electronic delivery service provision policy shall set out the detailed rules a qualified electronic delivery service should meet, while the practical rules for the provision of qualified electronic delivery services shall set out detailed operational procedures designed to meet those requirements, i.e. the way in which the service provider is to meet the technical, organisational and procedural business requirements set out in the qualified electronic delivery service provision policy, in compliance with the Law and the regulations governing the conditions for the provision of qualified trust services.

The qualified electronic delivery service provision policy shall be defined regardless of the service provider's specific operating environment, while the practical rules for the provision of qualified electronic delivery services shall set out a detailed description of the service provider's organisational structure, operating procedures and physical and computer environment, in compliance with the Law and the regulations governing the conditions for the provision of qualified trust services.

Conditions to be met by the Policy and the Practical Rules

Article 5

The qualified electronic delivery service provision policy and the practical rules for the provision of qualified electronic delivery services must be compliant with the provisions of the Law, the provisions of the regulations passed pursuant to the Law and the requirements of the standards applicable under those regulations.

The qualified electronic delivery service provision policy and the practical rules for the provision of qualified electronic delivery services should comply with the requirements of the standard EN 319 521, including the requirements of any other standards to which that standard directly or indirectly refers, as they pertain to the policy and the practical rules for the provision of qualified electronic delivery services.

Conditions for the Provision of Qualified Electronic Delivery Services

Article 6

The service provider shall meet the following conditions for service provision:

- 1) Enter into a contract for qualified electronic delivery service provision with the user;
- 2) Verify the user's identity at registration;
- 3) Verify the user's identity, i.e. perform authentication and authorisation, whenever a qualified electronic delivery service is accessed, based on an identification scheme with a medium or high confidence level in accordance with the Law;
- 4) Verify the sender's identity before performing a qualified electronic delivery;
- 5) Verify the recipients identity before performing a qualified electronic delivery;
- 6) Hold data confirming the receipt, forwarding and downloading of the content of an electronic message;
- 7) Ensure that an electronic message contains all required elements;
- 8) Ensure that no changes in the data content occur during the qualified electronic delivery;
- 9) Notify the recipient and the sender if the data content changes during the provision of qualified electronic delivery services;
- 10) Ensure that the time of sending, receipt, forwarding or downloading of an electronic message is confirmed by a qualified electronic timestamp;

11) Ensure electronic keeping of data on completed qualified electronic delivery and/or of individual deliveries in accordance with the standard ETSI TS 119 511 – Policy & security requirements for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques, and the standard ETSI TS 119 512 – Protocols for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques;

12) Ensure the keeping of relevant information;

13) Provide an updated list of service users and a service for other service providers to verify users' addresses;

14) Ensure their service supports message receipt and sending also if the sender or the recipient is the user of another qualified electronic delivery service provider;

15) Enable sender notification of the forwarding and downloading of delivered electronic messages on another service provider's platform.

Identity Verification and User Registration

Article 7

Registration of users of qualified electronic delivery services shall be done on the user's request and the service provider shall ensure the following when registering the user:

1) Before entering into a contractual relationship with the user, publicly notify the user using clear and comprehensible language of the relevant terms and conditions of using the qualified electronic delivery services;

2) If the user is identified as a natural person, determine and verify the user's identity, as follows:

(1) In the user's physical presence, based on the identity card, passport, foreign passport, passport for foreigners or identity card for foreigners, or

(2) Via a public document used as a means of remote identification, in accordance with the law, or

(3) Via remote identification in accordance with the law;

3) If the user is identified as a legal entity:

(1) In accordance with item 2) of this paragraph, determine and verify the identity of the user's authorised representative who submits the application for the qualified electronic delivery service on behalf of the user;

(2) Verify the power of attorney based on the user's bylaw by which the authorised person is authorised to apply for the qualified electronic delivery service on behalf of the user;

(3) Verify the data of the user as a legal entity by accessing data maintained by the Business Registers Agency or on the basis of a registration document for the legal entity issued by the competent authority;

4) Obtain from the user accurate and reliable information on the physical address or other attributed describing how the user may be contacted;

5) Enter into an agreement with the user.

When registering a user, the service provider shall also comply with the other requirements set out in the regulation governing the conditions for the provision of qualified trust services.

Electronic Message Transmission

Article 8

Electronic message transmission using qualified electronic delivery services is done by the sender transmitting an electronic message to the service provider with which the sender has a contract in order to transmit it to the recipient.

When providing qualified electronic delivery services, the service provider shall issue two confirmations to the sender, namely:

1) A confirmation of receipt of the sender's electronic message and its forwarding to the recipient;

2) A confirmation that the recipient has downloaded the delivered electronic message.

If the sender and the recipient have contracts with the same service provider, the electronic message shall be forwarded directly to the recipient.

If the sender and the recipient do not have contracts with the same service provider, the electronic message shall be forwarded to the service provider with which the recipient has a contract.

Content of Confirmation of Electronic Message Receipt by the Service Provider

Article 9

The confirmation of receipt of electronic message referred to in Article 8 paragraph 2 item 1) of this Rulebook shall include:

1) The identification mark of the electronic message assigned by the service provider;

2) Information on the sender and the recipient:

(1) In case of a natural person: name and surname,

(2) In case of a legal entity: business name, registration number or unique identification mark in accordance with the legislation of its country of establishment,

(3) Address for electronic delivery;

- 3) Data linking the confirmation to the content of the electronic message;
- 4) Date and time when the service provider received the sender's electronic message;
- 5) Date and time when the electronic message was forwarded to the recipient or the recipient's service provider.

Content of Confirmation of Electronic Message to the Recipient

Article 10

The service provider shall enable the recipient to confirm delivery of the electronic message using the electronic delivery software, at which point the electronic message shall be deemed to have been delivered.

Upon obtaining confirmation of receipt of the electronic message from the recipient, the service provider shall notify the sender thereof without delay.

The confirmation referred to in paragraph 2 of this Article must contain as a minimum:

- 1) The identification mark of the electronic message assigned by the service provider;
- 2) Information on the sender and the recipient:
 - (1) In case of a natural person: name and surname,
 - (2) In case of a legal entity: business name, registration number or unique identification mark in accordance with the legislation of its country of establishment,
 - (3) Address for electronic delivery;
- 3) Data linking the confirmation to the content of the electronic message;
- 4) Date and time when the forwarded electronic message was delivered, i.e. when it was downloaded by the recipient.

Use of Advanced Electronic Seal

Article 11

The service provider shall send the confirmations referred to in Articles 9 and 10 automatically in an electronic form, signed by an advanced electronic seal, and may also issue them electronically or in print on request.

The advanced electronic seal referred to in paragraph 1 of this Article must comply with the requirements set out in the law governing qualified trust services.

Keeping of Relevant Information

Article 12

The service provider shall keep the confirmations referred to in Article 8 paragraph 2 of this Rulebook and shall make them accessible to the user.

In addition to the confirmations referred to in paragraph 1 of this Article, the service provider shall also keep:

- 1) Data on determination and confirmation of the user's identity;
- 2) Data on determination of the sender's identity before qualified electronic delivery;
- 3) Data on determination of the recipient's identity before qualified electronic delivery;
- 4) Data showing the content of the electronic message was received and forwarded;
- 5) Data showing the content of the electronic message was downloaded;
- 6) Proof that the content of the data was not modified during qualified electronic delivery;
- 7) Data on the time of sending, receipt, forwarding and downloading of the electronic message, verified by a qualified electronic time seal.

The service provider shall ensure confidentiality, integrity and accessibility of the data referred to in paragraphs 1 and 2 of this Article.

The data referred to in paragraphs 1 and 2 of this Article shall be kept permanently.

Human Resources employed by the Service Provider

Article 13

The service provider shall ensure the necessary human resources, i.e. employees, who must have the expertise, the experience and the required qualifications for the service provided, specifically:

1) Minimum two employees with qualifications in information and communication technologies obtained in undergraduate academic or undergraduate vocational studies and with minimum three years of relevant work experience in the field of information system maintenance and security, who have passed at least one of the following examinations: CompTIA Security+, ISC2 CISSP or SANS GSEC; these employees are also required to regularly, at least once a year, attend trainings and seminars to update their knowledge on new security threats and current security procedures;

2) Minimum two employees with qualifications in information systems and with five years of relevant work experience in the field of information systems, who have passed at least one of the following examinations: ISC2 CISSP or SANS GSEC; these employees are also required to regularly, at least once a year, attend trainings and seminars to update their knowledge on new security threats and current security procedures.

Exchange of Electronic Messages between Providers of Qualified Electronic Delivery Services

Article 14

Exchange of electronic messages between providers of qualified electronic delivery services enables providers to verify the addresses of users of other service providers, which

enables them to receive and send messages also when the sender or the recipient of a message is a user of another provider of qualified electronic delivery services.

The service provider shall provide all other service providers with parameters for accessing the service used for verifying the data on the addresses of its users, which shall, upon inquiry, provide information on the existence of a particular address on the list of users of that service provider.

Access to such service must be based on the principle of authorised inquiry for verification of users' address data.

Each service provider shall grant another service provider access to its service used for verifying the data on the addresses of its users based on authorised inquiry.

Final Provision

Article 15

This Rulebook shall come into force on the eighth day of its publishing in the *Official Gazette of the Republic of Serbia*.

Number 110-00-74/2020-12

Done in Belgrade, on 30 June 2020

Minister,

Rasim Ljajić, PhD., own signature