APPROVED
by Directive No. 1.1-2/16-090 of 2 June 2016
of the Director General of the Information System Authority

The Requirements for the Trust Services of the Data Exchange Layer of Information Systems

The Information System Authority has developed requirements, which shall be followed in provision of trust services of the data exchange later of information systems (hereinafter X-Road) in the event of using the Estonian X-Road supporting version 4 of the X-Road message protocol. There are requirements established for the timestamping service, the security server authentication certificate, the X-Road member eSeal certificate, and the OCSP response services.

Following these terms and conditions is important in order to ensure the processability, integrity, and confidentiality of the data in transporting the data through X-Road.

1. The requirements for the timestamping service

1.1. The timestamping service used by an X-Road member shall issue qualified e-timestamps for the purposes of 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.

1.2. The timestamping service used by an X-Road member:
- 1.2.1. shall support the timestamp protocol described in the IETF standard RFC 3161;
- 1.2.2. shall support HTTP as the transport protocol and the POST inquiry;
- 1.2.3. shall support SHA-256 or stronger hash algorithms in requests;
- 1.2.4. shall use a certificate for signing timestamps, which is equipped with the *key usage* field *id-kp-timeStamping* (1.3.6.1.5.5.7.3.8);
- 1.2.5. shall not require usage of the timestamp policy field (*reqPolicy*) in timestamp requests;
- 1.2.6. shall use at least a 2048-bit RSA-key signature algorithm and SHA-256 or a stronger hash algorithm for signing responses;
- 1.2.7. may depart from the UTC time by up to 1 second;
- 1.2.8. must not suffer continuous (scheduled or unscheduled) interruptions of more than four hours.
- 1.2.9. The period of validity of the certificate used for timestamping may not exceed five years.

2. The requirements for the authentication certificate of security server

2.1. An authentication certificate of security server – a certificate connected to a security server issued by a qualified provider of a trust service, which certifies the authenticity of the security server and is used in creation of connection between security servers for authentication of security servers.
2.2. The certificate shall meet the IETF standard RFC 5280.
2.3. It shall be possible to check the validity of the certificate pursuant to the requirements described in clause 4.

2.4. The provider of the certification service shall:
   2.4.1. receive the PKCS#10 certification requests (in *.p10* or *pem* format);
   2.4.2. support issuing of the certificates to at least 2048-bit public RSA keys;
   2.4.3. use at least 2048-bit RSA-key signature algorithms and SHA-256 or a stronger hash algorithm for signing the certificates.
2.5. Upon issuing authentication certificates, at least one of the following list shall be specified as the area of application: *digitalSignature, keyEncipherment* or *dataEncipherment*. Alternatively, the value of the extension *extended key usage* may include the values *ClientAuthentication* or *ServerAuthentication.* The area of application of *nonRepudiation* shall not be used upon issuing authentication certificates.
2.6. A security server authentication certificate may be used until the expiry of the certificate or until declaration of the certificate invalid. In the event of suspension of the validity of a certificate, the certificate must not be used until termination of the suspension of the certificate.

3. The requirements for the eSeal certificate of an X-Road member

3.1. A member's eSeal certificate – a qualified certificate issued by a qualified certification service provider for creation of the eSeal, which is connected to the member's eSeal and is used to verify the integrity of the messages relayed and to verify the connection of the member with the message.
3.2. eSeal certificates shall comply with the requirements for qualified certificates for the purposes of 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. The certificate shall be in conformity with the IETF standard RFC 5280.
3.3. It shall be possible to check the validity of the certificate pursuant to the requirements described in clause 4.
3.4. The policy for provision of the certification service shall:
   3.4.1. enable to receive PKCS#10 certification inquiries (in *.p10* or *pem* format);
   3.4.2. support issuing of certificates to at least 2048-bit public RSA keys;
   3.4.3. specify the value of the key usage of the certificate as *nonRepudiation*.
   3.4.4. use at least 2048-bit RSA-key signature algorithms and SHA-256 or a stronger hash algorithm for signing the certificates.
   3.4.5. in the case of a certificate used to create a qualified eSeal, ensure location of the private key on a secure, hardware-based *Qualified Signature Creation Device* for the purposes of 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;
   3.4.6. ensure secure handling of the private key in the case of a certificate used for creation of an advanced eSeal;
3.5. in the event of using the security server software provided by the Centre, the qualified signature creation device shall be connectable to the security server by using the PKCS#11 protocol.
3.6. An eSeal certificate may be used until the expiry of the certificate or until declaration of the certificate invalid. In the event of suspension of the validity of a certificate, the certificate must not be used until termination of the suspension of the certificate.

4. The requirements for the certificate OCSP response service

4.1. The certificate OCSP response service shall:
   4.1.1. correspond to the IETF standard RFC 6960 or RFC 2560;
   4.1.2. use at least 2048-bit RSA-key signature algorithms and SHA-256 or a stronger hash algorithm.
4.2. The maximum permitted duration of a contentious downtime of the certificate OCSP response service shall be 4 hours and the duration of the total downtime per day may not exceed 12 hours.

5. Transitional provisions

5.1. The security server authentication certificates or eSeal certificates issued up to 30 June 2016 may be used until the expiry of the certificate or declaration of the certificate invalid.
5.2. Up to 30 June 2016, the timestamping service used on X-Road may issue qualified timestamps for the purposes of the Digital Signatures Act.