The terms of creation and management of certificate for e. resident authentication in an online environment and of qualified certificate for electronic signature of the e. resident

1. General provisions

1.1. The terms of creation and management of certificate for e. resident authentication in an online environment and of qualified certificate for electronic signature of e. resident (hereinafter collectively referred to as certificates) (hereinafter – the terms of creation and management of certificates) are aimed at informing the e. residents of the Republic of Lithuania about the purpose of certificates and restrictions on their use, the main obligations and liability of the Trust service provider that has issued these certificates and of e. residents as certificate owners, also the key aspects of the operation of the Trust service provider.
1.2. By submitting the application for e. resident status in the information system MIGRIS and having confirmed there that he has read and agrees with the terms of creation and management of certificates, the e. resident assumes all obligations and liability set out therein.
1.3. The terms of creation and management of certificates stipulate, that the e. resident shall familiarise oneself with E. resident Certificate Policy and Certification Practice Statement that are published on the Trust service provider's website www.nsc.vrm.lt.

2. Contact data

2.1. Trust service provider:
Identity Documents Personalisation Centre
Žirmūnų g. 1D, LT-09239 Vilnius
E-mail: adic@adic.gov.lt;
Website: www.nsc.vrm.lt

Inquiries are answered by Identity Documents Personalisation Centre, Certification Division. Tel. +370 271 6062.
Business hours (EET): Mon-Thu 7:30–16:30, Fri 7:30–15:15.

3. Content, purpose and restrictions on use of certificates

3.1. The Trust service provider shall create and manage for e. residents:
3.1.1. certificates for e. resident authentication in an online environment intended for authenticating the e. resident in an online environment;
3.1.2. qualified certificates for electronic signatures intended for supporting qualified electronic signatures according to 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 (hereinafter – Regulation (EU) No. 910/2014).
3.2. Certificates issued to e. residents may contain solely such signature validation data, which along with corresponding signature creation data are generated in the contact chip of e. resident electronic authentication and electronic signature means, which is a qualified electronic signature creation device.
3.3. Certificates issued to e. residents shall be valid for 3 years from the moment of their creation.
3.4. The structure of certificates created for e. residents shall meet requirements of ETSI EN 319 412-2 "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons". The personal data contained in e. resident certificates is specified by the Form of the E. Resident Electronic Authentication and Electronic Signature Means approved by the Minister of Interior of the Republic of Lithuania. Currently they include: e. resident's name, surname, and identity code.

4. Obligations of certificate owners

4.1. The certificate owner undertakes:
4.1.1. as required by Certification Practice Statement, to provide to the Trust service provider (or its representatives) accurate and complete information necessary for authenticating a person and creating certificates;
4.1.2. to use signature creation and validation data stored on e. resident electronic authentication and electronic signature means and the corresponding certificates solely for the purposes specified in subparagraph 3.1 hereof, observing the restrictions of use specified in the certificate;
4.1.3. to use certificates during their validity period only. During the certificate validity period having received a notification or otherwise becoming aware that certificates issued to him have been revoked or that a certification authority which has created certificates has been compromised, to immediately and permanently stop using the signature creation data corresponding to certificates (e. resident electronic authentication and electronic signature means) issued to him;
4.1.4. to ensure that other persons do not make use of the signature creation data (e. resident electronic authentication and electronic signature means);
4.1.5. during the certificate validity period having lost control over the signature creation data (e. resident electronic authentication and electronic signature means), to immediately revoke the corresponding certificates through his own personal account in the information system MIGRIS;
4.1.6. during the certificate validity period, upon the change of data recorded in certificates or after becoming aware that certificates contain incorrect data, also after becoming aware that activation data (password) of the contact chip of the e. resident electronic authentication and electronic signature means could have become or became known to other persons, to immediately and permanently stop using the signature creation data and to revoke the corresponding certificates through his own personal account in the information system MIGRIS;
4.1.7. to allow the Trust service provider to use and store personal data as required by the E. Resident Certificate Policy and Certification Practice Statement;
4.1.8. for the purpose of signature creation, to use computers with an installed operating system which is supported by the system manufacturer, is receiving automatic updates issued by the system manufacturer, and the latest version of the e. resident electronic authentication and electronic signature means software which is provided on the internet site www.nsc.vrm.lt

5. Obligations of the Trust service provider

5.1. The Trust service provider undertakes to provide its services complying with requirements of Regulation (EU) No. 910/2014, the Law on Electronic Identification and Trust Services for Electronic Transactions of the Republic of Lithuania and their implementing acts, including but not limited to the following requirements:
5.1.1. to provide at any time of day the information necessary to verify the revocation status of certificates;
5.1.2. having received a request in proper form without undue delay to temporarily suspend or revoke the certificate;
5.1.3. without undue delay to lift the temporary suspension of certificate having received a proper request of the certificate owner or law enforcement authority, at the request of which the certificate has been temporarily suspended;
5.1.4. to preserve applications of e. residents for the issuance of certificates, the data of certificates issued to e. residents and the management data of these certificates and store them for at least 7 years from the date of certificate expiry.

6. Liability of the Trust service provider

6.1. The Trust service provider shall be liable for violations of requirements of Regulation (EU) No. 910/2014, the Law on Electronic Identification and Trust Services for Electronic Transactions of the Republic of Lithuania and their implementing acts in accordance with the Code of Administrative Offenses of the Republic of Lithuania.
6.2. The Trust service provider shall pay damages done by its actions or omission in accordance with the procedure and conditions established by the Civil Code and other laws of the Republic of Lithuania.
6.3. The Trust service provider shall not assume liability where damages have been caused by:
6.3.1. unauthorized use of certificates (for example, when expired or revoked certificate is used for signing, or the certificate is used for other than its intended purpose, or restrictions on the use of the certificate are otherwise breached);
6.3.2. superior force (force majeure);
6.4. The Trust service provider shall insure its civil liability to secure obligations of the Trust service provider in accordance with the paragraph 10 of the Law on Electronic Identification and Trust Services for Electronic Transactions of the Republic of Lithuania.

7. Duties of relying parties

7.1. The parties relying on certificates must have read the E. Resident Certificate Policy and Certification Practice Statement.
7.2. Before relying on certificates, the relying parties shall verify certificate validity, validity of certificates forming a certificate trust chain to the certificate in question, also that the certificate is used for the purpose indicated therein.
7.3. Certificate validity shall be verified using an inquiry system, which provides certificate revocation status information at the time of verification. Detailed information on certificate validity verification is available in Certification Practice Statement which is published on the website of the Trust service provider.

8. Certificate revocation

8.1. Certificates may be revoked in the following cases:
8.1.1. at the choice of the certificate owner;
8.1.2. when the certificate owner losses control over the signature creation data corresponding to the certificate;
8.1.3. as it turns out that the Trust service provider has been provided with inaccurate data for issuing a certificate or they have changed;
8.1.4. having received a notification that the certificate owner has been declared mentally incapable or has died;
8.1.5. at the decision of the Trust service provider, when it becomes aware that the certificate owner does not comply with the Terms of certificate creation and management;
8.1.6. when the Trust service provider terminates its activities, and no other trust service provider takes over certification activities;
8.1.7. when security of the Trust service provider systems has been breached posing danger to reliability of the issued certificates, or security requirements imposed to ensure the trust in certificates change due to circumstances beyond the Trust service provider's control;
8.1.8. in other cases provided for by laws and the CPS.
8.2. The e. resident may revoke certificate himself through his personal account in the information system MIGRIS.
8.3. Where certificate is revoked in cases listed in subparagraphs 8.1.2, 8.1.3 or 8.1.5-8.1.8 hereof, a certificate owner shall be informed thereof indicating the reason for revocation.
8.4. The revoked certificate may not be unrevoked.
8.5. Retroactive certificate revocation shall not be allowed.
8.6. In all cases where the e. resident electronic authentication and electronic signature means becomes invalid, certificates recorded therein shall be revoked automatically.

9. Temporary certificate suspension

9.1. Certificates may be temporarily suspended:
9.1.1. at the choice of the certificate owner for the chosen period of time;
9.1.2. at a reasoned request of law enforcement authorities in order to prevent criminal acts, for the specified period of time;
9.1.3. having received information that certificate data are possibly incorrect;
9.1.4. having received information that the certificate owner possibly lost control over the signature creation data corresponding to the certificate;
9.1.5. at the time of production of the e. resident electronic authentication and electronic signature means, until the means is handed over to its owner.
9.2. The e. resident may suspend certificate himself through his personal account in the information system MIGRIS.
9.3. Where certificate is temporarily suspended in cases listed in subparagraphs 9.1.2-9.1.4 hereof, a certificate owner shall be informed thereof indicating the reason for suspension.

10. Lifting the temporary certificate suspension

10.1. The e. resident may lift the temporary certificate suspension himself, however only if certificate has been temporarily suspended for the reasons indicated in subparagraphs 9.1.1 and 9.1.5 hereof.
10.2. Where the certificate has been temporarily suspended for the reason indicated in subparagraph 9.1.2 hereof, the temporary certificate suspension shall be lifted upon the request of the law enforcement authority, at the request of which the certificate has been suspended.
10.3. Where the certificate has been temporarily suspended for the reasons indicated in subparagraphs 9.1.3-9.1.4 hereof, the certificate owner shall submit a written request and an explanation denying information on the basis whereof the certificate has been temporarily suspended. Having failed to submit the request and the explanation within 30 days from the day of certificate suspension, the certificate shall be revoked.

11. Certificate renewal

11.1. Certificates for e. residents are renewed (new certificates issued) only in conjunction with the issuance of the new e. resident electronic authentication and electronic signature means.

12. Protection of the signature creation data stored on the e. resident electronic authentication and electronic signature means

12.1. In order to protect the signature creation data stored on the e. resident electronic authentication and electronic signature means from unauthorised use, activation data (password) of the contact chip of the means shall be used and the number of failed attempts to enter the correct password shall be limited, i.e. having entered an incorrect password three consecutive times, the use of signature creation data shall be blocked.
12.2. The blocking shall be cancelled only by using a dedicated software and an unlock data of the contact chip (PUK code).

13. Fees

13.1. No additional fees shall be charged for certificates issued in conjunction with the e. resident electronic authentication and electronic signature means.
13.2. The Trust service provider may establish fees for certain services, except for a fee for the provision of information necessary to determine the reliability and to verify the revocation status of certificates issued by it.

14. Applicable law, personal data protection, complaints and dispute resolution procedures

14.1. All legal relations resulting from provision of trust services shall be governed by the law of the Republic of Lithuania.
14.2. The Trust service provider shall process data collected for the creation of certificates in accordance with the 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.
14.3. All disputes related to the creation and management of certificates shall be resolved in accordance with laws of the Republic of Lithuania.

15. Evidence of reliability of certification activities

15.1. The Trust service provider is a certification service provider issuing qualified certificates registered in 2015 with the supervisory body, namely, Communication Regulatory Authority of the Republic of Lithuania. Based on conformity assessment report issued by conformity assessment body Elektrotechnický zkušební ústav, s. p. in March 2019 and decision of the supervisory body, the Trust service provider is a qualified trust service provider authorised to issue qualified certificates for electronic signatures.
15.2. The Trust service provider shall publish conclusions of external inspections of operations on the website of the Trust service provider.