REMEMBER...

The only person who may use the e. resident card issued to you is you.

Don‘t share your PIN and PUK codes with anyone. Keep them safe (keep separately from the e. resident card, don‘t write them down on the card or items that you keep with the card). You can always check your PIN and PUK codes on your account on www.migracija.lt.

The PUK code of the card is intended to unblock the card in case it has been blocked after failing to enter correct PIN code three times in a row.

Should you lose your e. resident card or its PIN code, connect to MIGRIS at www.migracija.lt and report the loss of e. resident card as soon as possible. After submission of the report, the certificate for e. resident authentication in an online environment and the qualified certificate for electronic signatures will be revoked. You may get a new e. resident card only upon submitting a new application for granting the e. resident status.

WHERE CAN I GET HELP?

Should you have any questions about the preparation of your computer for using the e. resident card, you may look for answers on the website www.nsc.vrm.lt/default_en.htm, write an e-mail to adic@adic.gov.lt or make a telephone call to +370 5 271 6062

Information on migration services:
Phone: +370 707 67000
e-mail: info@migracija.gov.lt

Technical issues and service disruptions:
e-mail: migris@migracija.gov.lt

Call customer service:
Monday-Tuesday 7:30–16:30
Friday 7:30–15:15

ELECTRONIC IDENTIFICATION AND ELECTRONIC SIGNATURE TOOL

An e. resident card

is a tool for electronic identification and electronic signature, enabling you to use administrative, public or commercial electronic (remote) services in the Republic of Lithuania and to create qualified electronic signatures. More information about the card is available on the website www.migracija.lt. Click 'Service Information' ⟶ 'Citizens of Other Countries' or 'EU Citizens' ⟶ 'I want to become an electronic resident'.

E. resident certificates:

qualified certificate for electronic signature of e. resident and certificate for e. resident authentication in an online environment, recorded in contact chips of e. resident electronic authentication and electronic signature means issued to e. residents of the Republic of Lithuania.

Certificate owner:

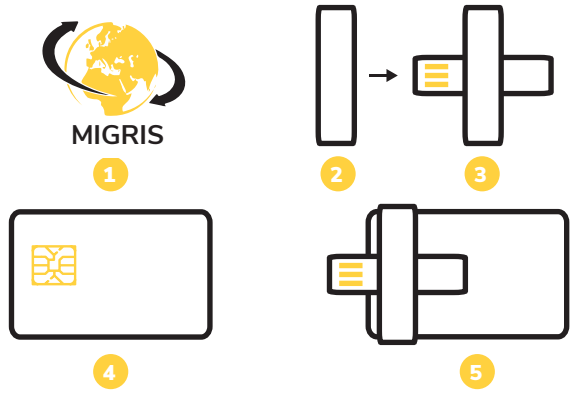
a natural person to whom a certificate has been issued.

Trust service provider:

Identity Documents Personalisation Centre under the Ministry of Interior of the Republic of Lithuania.

YOUR FIRST STEPS

1. Activate your e. resident card by connecting to your account in Lithuanian Migration Information System (hereinafter – MIGRIS) at www.migracija.lt ⟶ Login. On your account, near to your card details you will find the button 'Activate'. After you activate the document, you will be able to see PIN and PUK codes of your card.
2. Take the card reader.
3. Unfold it into the shape of plus sign.
4. Take your e. resident card.
5. Insert the e. resident card into the reader.
6. Download and install the card software from www.nsc.vrm.lt/downloads_en.htm.
7. Plug in the card reader into computer. Ensure that the chip and the reader are in contact.
8. Now you can use electronic services!



OBLIGATIONS OF CERTIFICATE OWNERS

The certificate owner undertakes:

- 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;
- to use signature creation and validation data stored on e. resident electronic identification and electronic signature means and the corresponding certificates solely for e. resident authentication in an online environment and for supporting qualified electronic signatures, observing the restrictions of use specified in particular certificate;
- 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 identification and electronic signature means) issued to him;
- to ensure that other persons do not make use of the signature creation data (e. resident electronic identification and electronic signature means);
- during the certificate validity period having lost control over the signature creation data (e. resident electronic identification and electronic signature means), to immediately revoke the corresponding certificates through his own personal account in the information system MIGRIS;
- 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 identification 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;
- to allow the Trust service provider to use and store personal data as required by the E. Resident Certificate Policy and Certification Practice Statement;
- 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 identification and electronic signature means software which is provided on the internet site www.nsc.vrm.lt.