FAQ

How to proceed after CU Key mobile application update or re-installation on a new device?

In the event of a bigger update or if you are re-installing the CU Key application on a new device you will need to use **other active method of verification**, e.g. Text message code , as your CAS account considers the CU Key application still valid, however, it is not currently active.

1. Open the CU Key mobile application on your phone and log in.
2. Select Other method of verification and use either Security key (if active) or Verification via SMS message.


3.

4. Once you fill in the code and confirm login the application will ask you if you wish to activate biometrics verification, see CU Key Activation process .

How to proceed if you lose your mobile phone or it is stolen?

1. Ask your mobile service provider to **block your SIM card** as soon as possible.
2. Request **new SIM card with the same phone number**.

3. Visit website www.ldap.cuni.cz/mfa and log into CAS. Select **Other method of verification** and use **Text message code** for verification.
4. **Remove CU Key mobile application from active methods** of two-factor authentication to **prevent unauthorized access** to your user account from the lost mobile phone.
   - Click on the arrow next to the SMS message verification method:
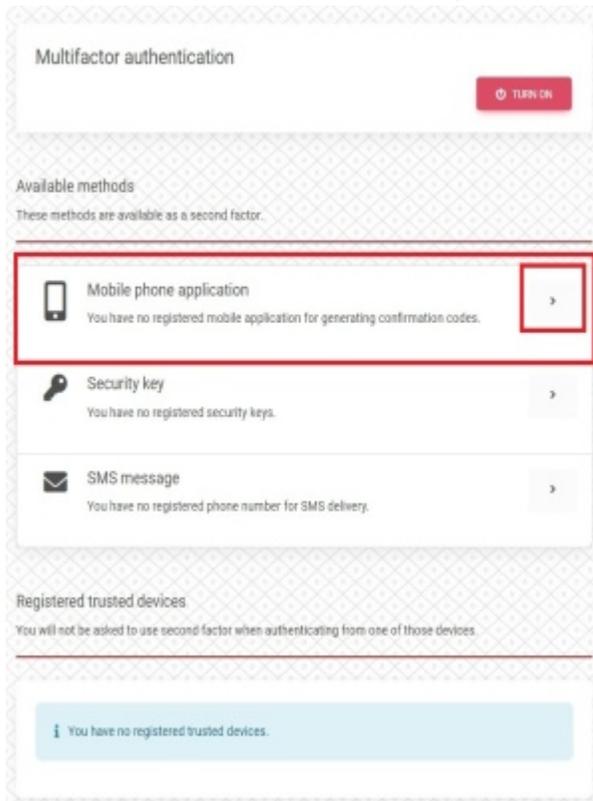
   - Click on Remove all next to the CU Key application

5. Install the CU Key mobile application on your new device and continue with CU Key activation process .

If it is not possible to retrieve your previous phone number from the service provider, you will need to use other means of verification to log into CAS user account. Those are SvipeiD or NIA .

How to proceed if you lose your hardware key or it is stolen?

1. Inform your **local IT support about the loss** of your hardware key as soon as possible.
2. Visit website www.ldap.cuni.cz/mfa and log into CAS. Select any **other active method** of two-factor authentication (CU Key mobile application or Text message code).
3. Remove the hardware key from active means of two- factor authentication, so your lost device cannot be used for unauthorized access.
   - Click on the arrow next to the Security key verification method:
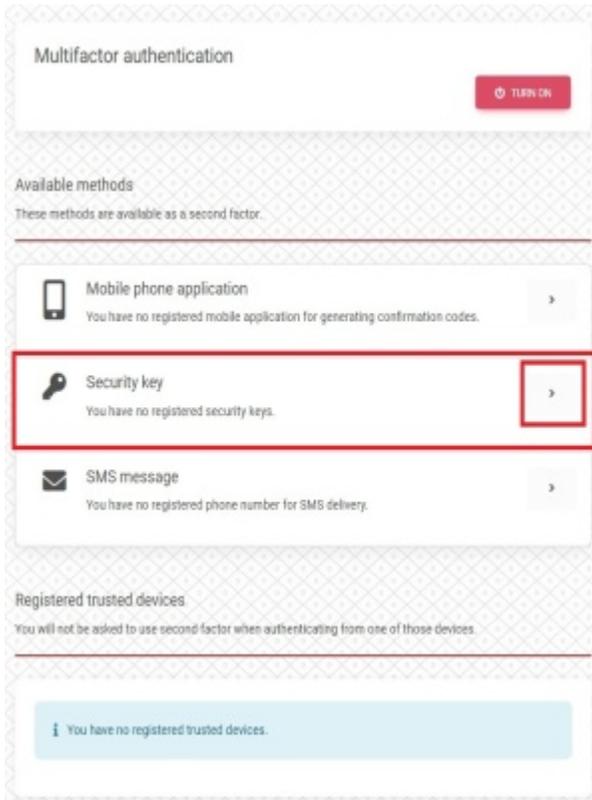
- Click on Remove all at the bottom-right corner: