Hardware key

Hardware keys with support of **FIDO2 security protocol** provide very strong means of **protection against unauthorised access** as they require **physical presence of the user** during login. They are simple to use – you just connect them to your device and confirm access by touch. They significantly increase level of security of CAS user account.

Please get in touch with your **local IT support** with regards to availability of these **hardware keys**.

Hardware keys is **one of the options** for two-factor authentication. It is highly recommended to use it **as secondary to** CU Key **mobile application**.

The activation procedure of hardware key depends on the brand and model of the device itself. Please read thoroughly the instructions for yours as it may require specific activation procedure before use.

Activation process

1. Visit website www.ldap.cuni.cz/mfa and log in to CAS.
   Select **Security key** among the available options.

2. A field for device registration will appear. Click on **Register** and continue.

3. You can **choose a name** for your device or continue with the suggested pre-set.

4. Now the instructions may vary depending on operation system of your PC/laptop. The following instructions apply for Microsoft Windows.

   Select **Security Key**. If you do not see it as the first option, click on **More options**.

5. You will be asked to **insert** the hardware key and set **PIN code**.

Windows Security
Security key setup
Set up your security key so you can sign in to cas.cuni.cz as 70244271.
This request comes from the application "msedge.exe" by "Microsoft Corporation".
OK
Cancel

Windows Security
Continue setup
Insert your security key into the USB port.
Cancel

Windows Security
Continue setup
Please enter the security key PIN.
Security key PIN
OK
Cancel

Windows Security
We're confirming it's you
To sign in to .cas.cuni.cz'.
This request comes from the 'msedge.exe' app from 'Microsoft Corporation'.
Tap your security key
Cancel

6. As soon as your device is successfully registered you will be asked by the system for **verification via the hardware key**.

7. If the registration is **successful**, you will see a **confirmation table** with a picture of your hardware key.

8. Now, visit website that requires CAS login and two-factor authentication, e.g. www.servicedeks.cuni.cz and log in.

9. Click on **Other verification methods** and select **Security key**.

There are more types of security keys that are compatible with CAS two-factor authentication, e.g. **Windows Hello**. Usage of other types of security keys is based on specific workplace requirements. If you are interested in the use of these, **please get in touch with your local IT support**.

It is possible to register only **one security key type per account**.