

Hardwarový klíč

Hardwarové klíče s podporou FIDO2 poskytují velmi silnou ochranu proti neoprávněnému přístupu, protože vyžadují fyzickou přítomnost uživatele při přihlášení. Jsou jednoduché na použití – stačí je připojit k zařízení a potvrdit přihlášení dotykem.

Výrazně se tak zvyšuje zabezpečení vašeho účtu CAS.

S dotazy na dostupnost tohoto typu Bezpečnostního klíče se prosím obračejte na lokální IT podporu vaší fakulty nebo součásti.

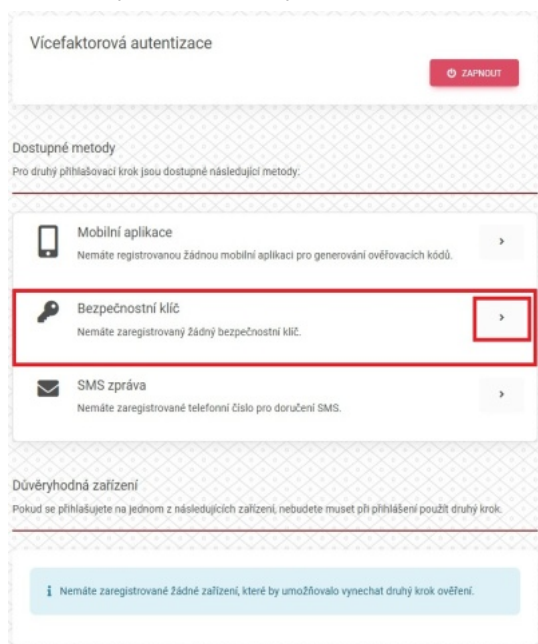
Použití hardwarového klíče je další z možností dvoufaktorového ověření. Doporučujeme tuto metodu využívat jako sekundární k mobilní aplikaci UK Klíč.

Postup aktivace hardwarového klíče závisí na značce a modelu samotného zařízení. Pečlivě si proto prostudujte návod k vašemu hardwarovému klíči a pokud je potřeba zařízení předem aktivovat, postupujte podle návodu.

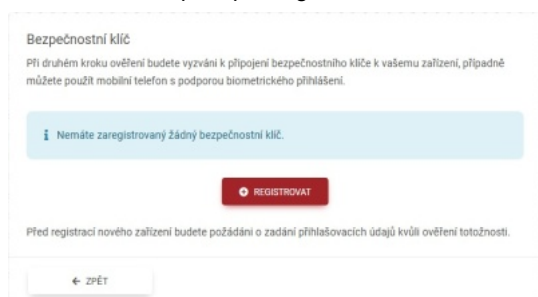
Postup aktivace

1. Přejděte na stránku www.ldap.cuni.cz/mfa a přihlaste se.

V dostupných metodách vyberte možnost **Bezpečnostní klíč**.



2. Zobrazí se vám pole pro registraci nového zařízení.

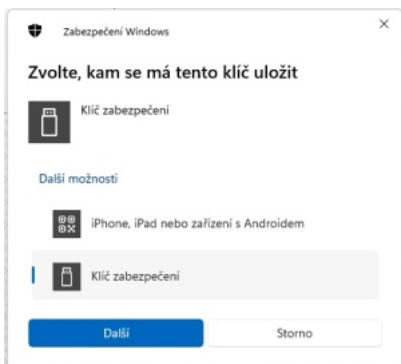


3. Systém vás vyzve k **pojmenování** zařízení. Jakmile vyberete vhodné jméno zařízení, klikněte na **Registrovat**.

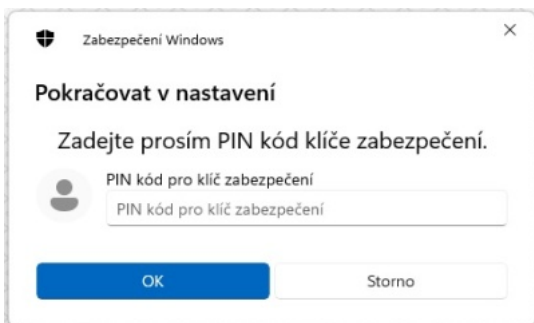
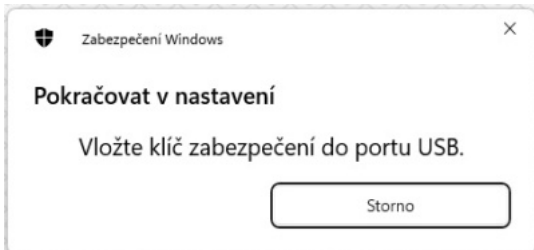


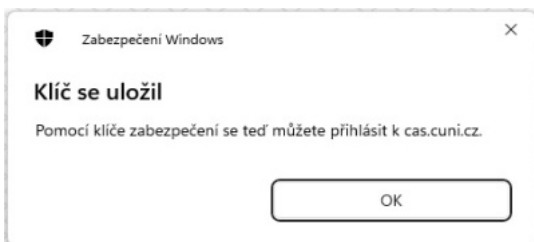
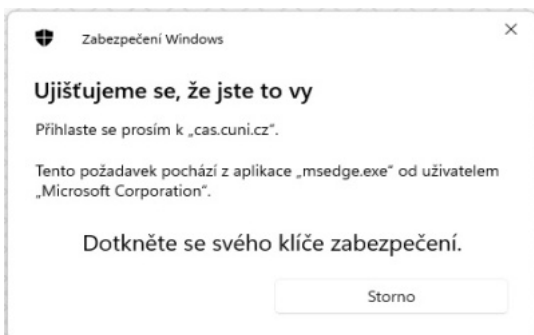
4. Nyní se může návod lišit v závislosti na operačním systému vašeho počítače. Následující pokyny jsou určeny pro systém Windows.

Zvolte **Klíč zabezpečení**. Pokud tuto možnost nevidíte jako první, klikněte na **Další možnosti**.



5. Budete vyzváni k **vložení zařízení** a následně k **nastavení PIN kódu**.

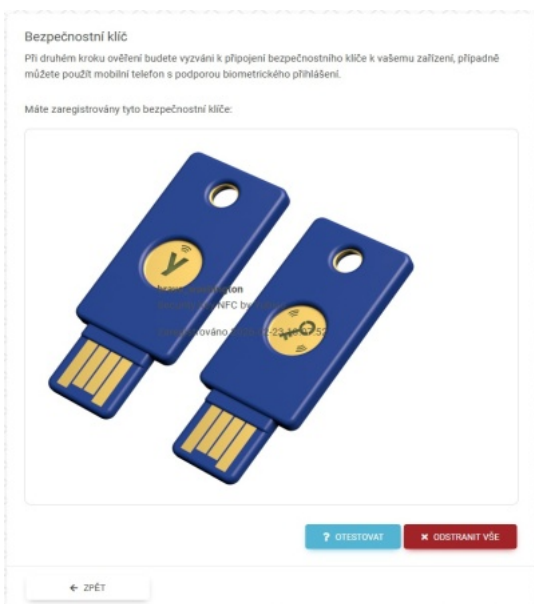




6. Jakmile bude zařízení úspěšně zaregistrováno, systém vás vyzve k **ověření pomocí hardwarového klíče**.



7. Pokud bude zařízení přidáno **úspěšně**, zobrazí se vám **potvrzení o registraci** zařízení.



8. **Přejděte na stránku, která vyžaduje přihlášení přes CAS a zároveň dvoufaktorové ověření, např. www.servicedesk.cuni.cz a přihlaste se.**

Profil uživatele

Jste přihlášení jako **70244271**, nicméně aplikace **Profil uživatele** požaduje nové ověření vaší totožnosti. Prosím zadejte vaše uživatelské jméno a heslo a pokračujte dále.

Uživatelské jméno*

Heslo:*

PŘIHLÁSIT

[Zapomněli jste heslo?](#)
[Nastavení bezpečnostního klíče](#)
[Potřebujete pomoc?](#)

Z bezpečnostních důvodů se po ukončení práce odhlaste a zavřete všechna okna prohlížeče!
 Po pěti neúspěšných pokusech o přihlášení bude váš účet na 20 minut zablokován.

Další možnosti ověření

SVIPEID

IDENTITA OBČANA

EDUID

EDUGAIN

Vaše externí identita musí být zaregistrována, abyste se mohli přihlásit ke svému CAS účtu.

9. Zvolte metodu pro druhý krok ověření:

Vyberte metodu pro druhý krok ověření:

Mobilní aplikace
 Pro ověření identity ve druhém kroku použijete jednorázové heslo vygenerované mobilní aplikací na vašem telefonu.

POUŽÍT

DALEŠÍ METODY OVĚŘENÍ

Vyberte metodu pro druhý krok ověření:

Mobilní aplikace
 Pro ověření identity ve druhém kroku použijete jednorázové heslo vygenerované mobilní aplikací na vašem telefonu.

POUŽÍT

Bezpečnostní klíč
 Při druhém kroku ověření budete vyzváni k připojení bezpečnostního klíče k zařízení s prohlížečem. Můžete použít i mobilní telefon s podporou biometrického přihlášení.

POUŽÍT

Ověření pomocí SMS zprávy
 Na zaregistrované telefonní číslo vám bude odeslána SMS zpráva s ověřovacím kódem, který zadáte ve druhém kroku ověření.

POUŽÍT

ZRUŠIT

Existují i další typy bezpečnostních klíčů, které jsou kompatibilní se systémem dvoufaktorového ověření, např. **Windows Hello**. Využití a podporu těchto prvků si však určují jednotlivá pracoviště sama. Pokud máte zájem o jejich využití, **informujte se u IT podpory vaší fakulty nebo součásti**.

V rámci vašeho účtu navíc může být zaregistrováno **pouze jedno zařízení tohoto typu**.