Certifikáty, elektronické podpisy

Certifikát je něco jako Váš elektronický občanský průkaz. Pomáhá Vám bezpečně se přihlašovat do systémů univerzity, podepisovat dokumenty a chránit komunikaci před zneužitím. Na Univerzitě Karlově můžete certifikát získat prostřednictvím certifikačních autorit **TCS** nebo **PostSignum**. Každý systém má jiné využití a způsob vydání.

S čím potřebujete poradit?

Pro koho jsou certifikáty určeny?

- Studenti mohou získat pouze osobní certifikát TCS.
- Zaměstnanci UK mohou využívat všehny typy certifikátů (TCS i PostSignum).

Jaké typy certifikátů univerzita nabízí?

Osobní certifikáty TCS

- Určené pro studenty i zaměstnance Univerzity Karlovy.
- Digitální podpisy e-mailů provedené těmito certifikáty zobrazí většina e-mailových programů jako důvěryhodné, ale **není možné** je použít pro **komunikaci se státní správou**. Jsou ale dobře použitelné pro zabezpečenou komunikaci s kolegy (např. v rámci řešení projektů) a mimo jiné i k nastavení nového ověřeného hesla v CAS bez zadání starého hesla.

Serverové certifikáty TCS

Serverové certifikáty slouží k zajištění bezpečné komunikace. Pomáhají ověřit, že se uživatel připojuje ke správnému serveru a zabezpečují přenášená data.

Osobní certifikáty PostSignum

- Určené pro zaměstnance UK.
- Certifikáty slouží pro **digitální podepisování e-mailů, dokumentů a pro komunikaci se státní správou**.

Podpisové certifikáty PostSignum

- Určené zaměstnancům UK. Certifikáty je možné použít pro digitální **podepisování úředních dokumentů v PDF formátu**.
- **Podpisy jsou uznávané státní správou.**

Jaké jsou podmínky pro získání certifikátu?

Podmínky pro získání TCS certifikátu najdete na https://tcs.cuni.cz

Podmínky pro získání PostSignum certifikátu:

- žadatel musí být zaměstnancem Univerzity Karlovy.
- žadatel musí mít platný účet CAS a v něm ověřenou e-mailovou adresu.
- e-mailová adresa musí být v doméně cuni.cz

Jak získám certifikát?

Postup se liší podle certifikační autority:

TCS certifikáty

- O osobní i serverové certifikáty je možné požádat online na TCS portálu CESNET .

Osobní certifikáty PostSignum

Žádost se podává prostřednictvím Servicedesku a je nutné osobní ověření na poště:

- žadatel podá požadavek na Servicedesk ohledně vydání certifikátu,
- odpovědná osoba na Servicedesku označí zaměstnance a jeho emailovou adresu ve WhoIS ,
- žadatel následně prostřednictvím aplikace iSignum požádá o vydání certifikátu (zde uvede stejný e-mail, který byl označen ve WhoIS),
- po podání žádosti se žadatel osobně dostaví na poštu nebo na Czechpoint s občanským průkazem a vygenerovaným číslem žádosti,
- informaci o vydání certifikátu obdrží na zadanou e-mailovou adresu,
- vydaný certifikát žadatel nainstaluje na svůj počítač.

Podpisové certifikáty PostSignum

Ohledně vydání podpisového certifikátu podá žadatel požadavek na Servicedesk :

- odpovědná osoba na Servicedesku označí zaměstnance a jeho emailovou adresu ve WhoIS, vydá token (s nastaveným PINem) a nainstaluje potřebnou aplikaci,
- žadatel následně prostřednictvím aplikace iSignum požádá o vydání certifikátu (musí uvést stejný e-mail, který byl označen ve WhoIS),

- po podání žádosti se žadatel osobně dostaví na poštu nebo na Czechpoint s občanským průkazem a vygenerovaným číslem žádosti,
- nakonec žadatel na svém počítači v nainstalované aplikaci dokončí proces - stáhne si vydaný certifikát na token.

Jaký je formát certifikátu?

- TCS certifikáty a Osobní certifikát PostSignum mají formu šifrovaného souboru a jsou uloženy na disk uživatelova počítače.
- Podpisový certifikát PostSignum má formu USB tokenu (tento certifikát není možné získat ve formě souboru).

Často kladené dotazy (FAQ)

Osobní certifikát mi přestal platit a vygeneroval jsem si nový. Mohu ten starý smazat?

- Nedělejte to. Staré e-maily, které jsou zašifrované vaším starým certifikátem, novým certifikátem nerozšifrujete. Už byste se k nim nikdy nedostal/a..

Smazal se mi počítač, kde jsem měl certifikát uložený a nainstalovaný. Můžu si ho odněkud znova stáhnout?

- Ne, to nejde. Jakmile získáte certifikát ve formě souboru, musíte si ho dobře zazálohovat. V tomto případě bude nutné podat novou žádost o certifikát.

Smazal se mi počítač, kde jsem měl certifikát nainstalovaný. Mám ho zazálohovaný, ale nepamatuji si heslo. Dá se nějak zjistit?

- Ne, bohužel nedá. V tomto případě bude nutné podat novou žádost o certifikát.

Systém mi odmítá vydat osobní TCS certifikát, co mám dělat?

- Zkontrolujte, jestli v CASu máte e-mailovou adresu ověřenou a jestli ověření není starší než 6 měsíců. Pokud si nejste jisti, tak si radši ověřte e-mailovou adresu v CASu znovu a zkuste pak znovu požádat o osobní certifikát.

Chci osobní TCS certifikát, je nějaké omezení co se týče počítače (Windows, Mac, Linux)?

- Pro získání TCS certifikátu stačí www prohlížeč Firefox nebo Chrome (a klony jako Brave, MS) na Windows, Mac, Linuxu. Používat ho jde na všech platformách.

Chci osobní certifikát PostSignum, je nějaké omezení co se týče počítače (Windows, Mac, Linux)?

- Pro získání certifikátu je nutné vygenerovat žádost v programu, který je pouze ve verzi pro Windows. Vydaný certifikát pak jde na všech platformách.

Chci podpisový certifikát PostSignum, je nějaké omezení co se týče počítače (Windows, Mac, Linux)?

- Pro získání certifikátu je nutné vygenerovat žádost v programu, který je pouze ve verzi pro Windows. Vydaný certifikát je možné používat v systémech, pro které existuje ovladač pro token - ve Windows a na Mac.

Chci podpisový certifikát PostSignum, který se vydává jen do tokenu. Mám vlastní token typu Yubikey, mohu ho použít?

- Ne, certifikát lze vydat jen do tokenu od PostSignum, který univerzita poskytuje.

Podpora, Helpdesk

- TCS - s dotazy a žádostmi o podporu se obracejte na správce TCS za Univerzitu Karlovu. Pište na adresu tcs@cuni.cz
- PostSignum - v prvním kroku doporučujeme obrátit se **vždy** na IT podporu fakulty (kontakty najdete na webu své fakulty nebo součásti). Teprve poté, pokud se nepodaří problém vyřešit, obraťte se na Servicedesk

Důležité odkazy

- Jak požádat o serverový certifikát TCS
- Užitečné příkazy OpenSSL
- CAA DNS záznamy
- Acrobat Reader a certifikáty