Provozní řád – vydávání osobních certifikátů TCS

K čemu slouží?
Elektronický podpis zaručuje identitu odesílatele. Pro elektronický podpis lze používat osobní certifikát od Trusted Certificate Service (CA) zprostředkovaný přes akademickou síť CESNET. CESNET CA zprostředkuje vydávání osobních eScience (gridových) a serverových certifikátů TCS. Tyto certifikáty vydává certifikační úřad společnosti DigiCert, jehož kořenovým certifikátům důvěřuje většina internetových browserů a mailových klientů v implicitní konfiguraci.

Kde se uplatní?
Certifikáty vydané CESNET CA není možné použít pro zabezpečení komunikace se státní správou. Jsou určeny pro použití v rámci národních i mezinárodních vědecko - výzkumných projektů a pro aplikace provozované členy CESNET, z. s. p. o., pro zvýšení důvěryhodnosti a bezpečnosti elektronické pošty i na VŠE.

Komu je určen?
Tento osobní certifikát je bezplatný a je k dispozici pro všechny zaměstnance a studenty Vysoké školy ekonomické v Praze (VŠE).

Postup při vydání:
1. Ověření identity uživatele
Žadatel se dostaví osobně na Centrum podpory uživatelů (CPU) na 22 SB, kde pověřenému pracovníkovi sdělí žádost o ověření svojí totožnosti pro elektronický podpis. Pro ověření totožnosti bude potřebovat svojí studentskou nebo zaměstnaneckou identifikační kartu a jeden doklad totožnosti (občanský průkaz, řidičský průkaz nebo cestovní pas). Bez uvedených požadovaných dokladů nelze provést ověření totožnosti pověřeným pracovníkem.

2. Vydání certifikátu
Žadatel po ověření totožnosti na CPU může požádat o osobní certifikát podle návodu na stránkách CESNET PKI. Soukromý klíč a žádost (CSR) je automaticky vygenerován www prohlížečem.

3. Instalace certifikátu
Po vydání je certifikát uložen v prohlížeči a odtud ho uživatel společně se soukromým klíčem vyexportuje do souboru – tento soubor poté importuje do e-mailového klienta.

Podrobnější návody jsou na webu CI.

Bezpečnost
Soubor obsahující soukromý klíč žadatele (případně soukromý klíč společně s certifikátem) je třeba zabezpečit, aby se k němu nedostal nikdo cizí (mohl by potom číst šifrované e-maily nebo se jménem kompromitovaného žadatele podepisovat). Zároveň je třeba tyto soubory bezpečně zálohovat – při jejich ztrátě není možné číst případné šifrované e-maily, které v minulosti přišly, a není možné podepisovat e-maily.
Pokud by došlo ke kompromitaci počítače (ukradený notebook, zavirování, útok crackera...) nebo ztrátě média se zálohou soukromého klíče, je třeba podle návodu Odvolání certifikátu revokovat původní (kompromitovaný) certifikát a nechat si vystavit nový. V případě, že bylo důvodem zavirování nebo jiné napadení počítače, je třeba nejprve odstranit příčinu (např. reinstalací operačního systému, použití antiviru, firewallu, bezpečnější chování na Internetu...) a až poté požádat o nový certifikát.

Ukončení studia či pracovního poměru uživatele
Před ukončením studia či pracovního poměru je povinen uživatel svůj certifikát revokovat podle návodu Odvolání certifikátu. Pokud tak neučiní, provede to pracovník správy certifikátů na VŠE.