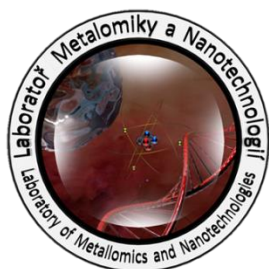




Laboratoř Metalomiky a Nanotechnologií



Elektronické podpisy certifikované autoritou informačního systému

Abstrakt

Pokud si chceme pořídit klíč a certifikát, záleží k čemu jej chceme používat. Vnitrofiremní komunikaci lze podepisovat certifikáty vydanými vedením firmy. Banky často vydávají certifikáty svým klientům, aby s nimi mohly bezpečně komunikovat. Pokud však chceme mít



certifikát pro běžné používání, musíme si najít nějakou obecně uznávanou autoritu. Pro komunikaci s úřady potřebujeme dokonce kvalifikovaný certifikát, které u nás vydávají tyto autority: První certifikační autorita (ICA), PostSignum (Česká pošta) a Eldentity. znak FNC1 (funkční znak 1).



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



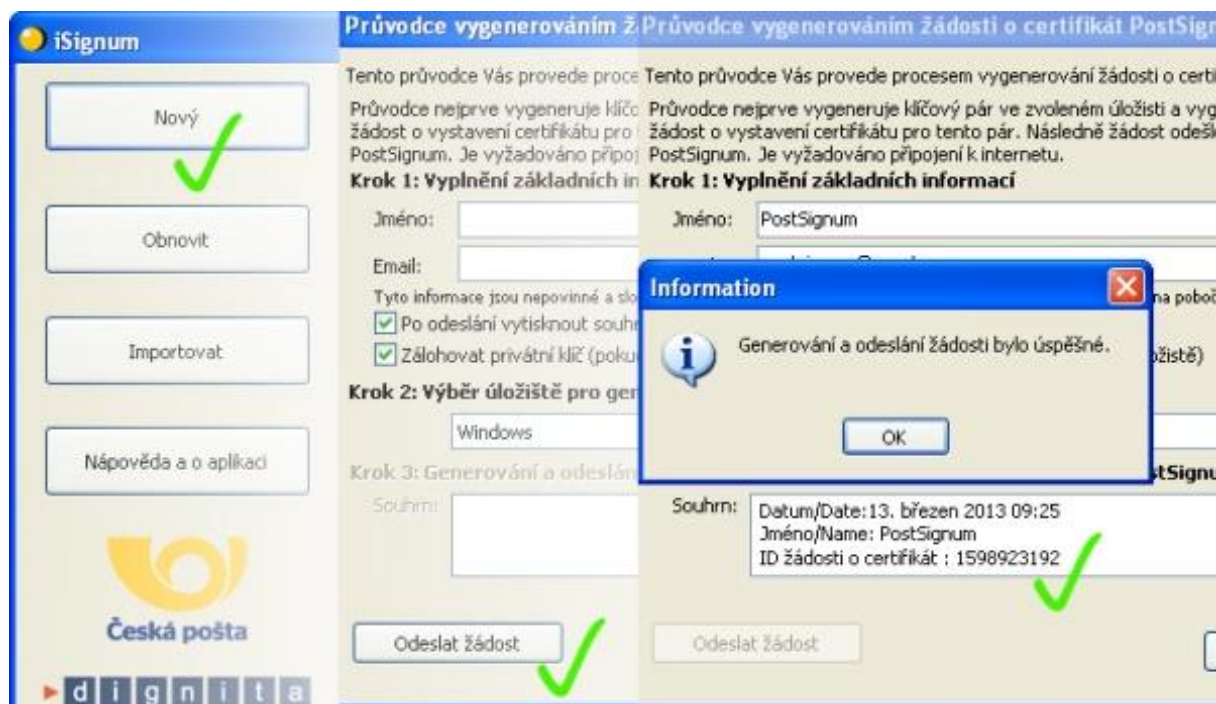
OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Elektronický podpis POSTSIGNUM

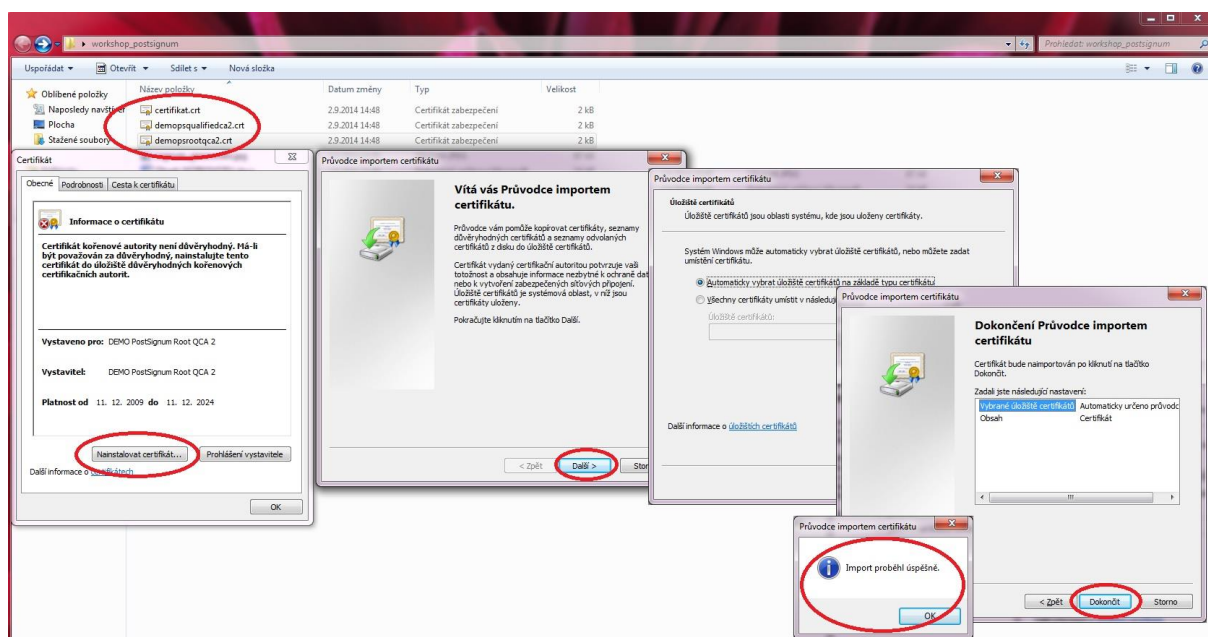
- Web Postsignum - <http://www.postsignum.cz/>
- Program iSignum - <http://www.postsignum.cz/isignum.html>
- Generujeme žádost a záloha soukromého klíče
- Vydání testovacího certifikátu
- Instalace do systému
- Způsoby a formy použití certifikátu
- Praktické použití v programech
- Dotazy a diskuze

Práce s programem iSignum



Cvičení: Testovací certifikát

- Generování žádosti v Internet Exploreru
https://www.postsignum.cz/testovaci_certifikat.html
- Instalace root a qualified authority
- Instalace osobního kvalifikovaného cert. – QCA



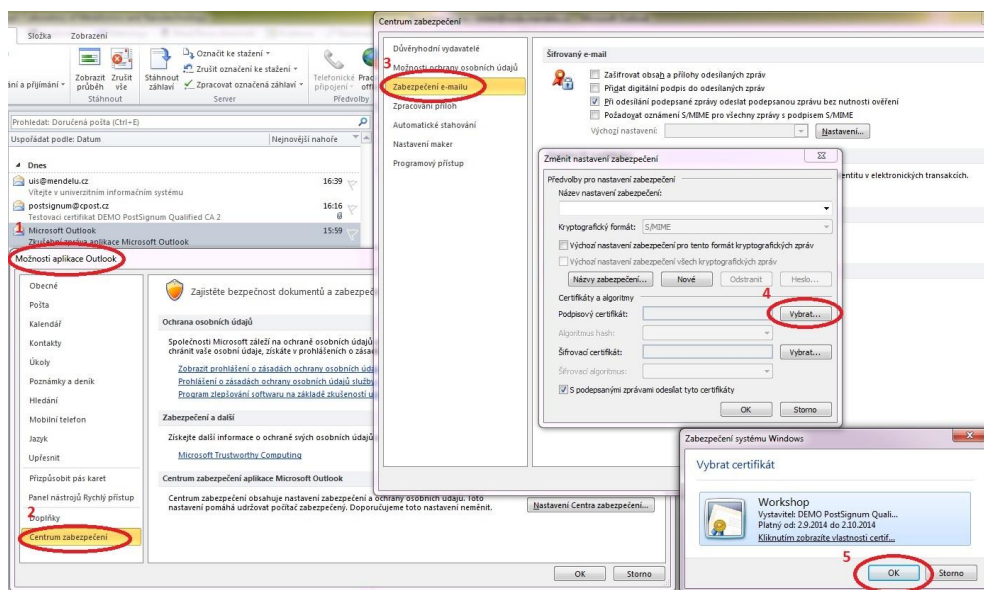
Možnosti použití certifikátů dle jeho druhu:

- Kvalifikované (osobní, systémové – tzv. elektronická značka)
- Komerční (osobní, serverové)
- Komerční doménové (pro jednu doménu, SAN - Subject Alternative Name nebo tzv. Wildcard tj. např. *.mendelu.cz)

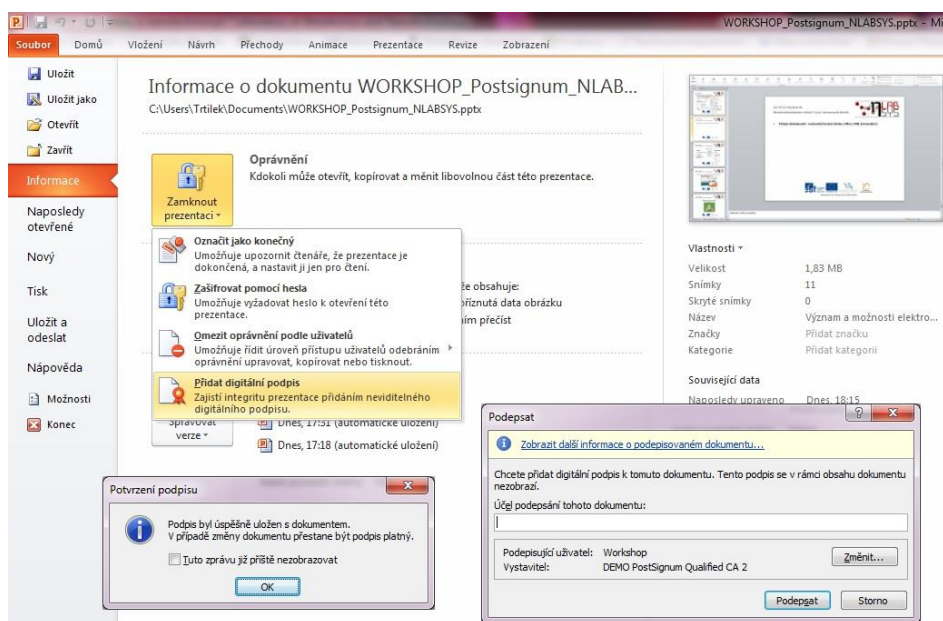
http://www.postsignum.cz/vyuziti_certifikatu.html

Pro podrobnější seznámení s problematikou doporučuji následující dokument:
http://www.postsignum.cz/files/politiky/CA_Zprava_pro_uzivatele_v2_4.pdf

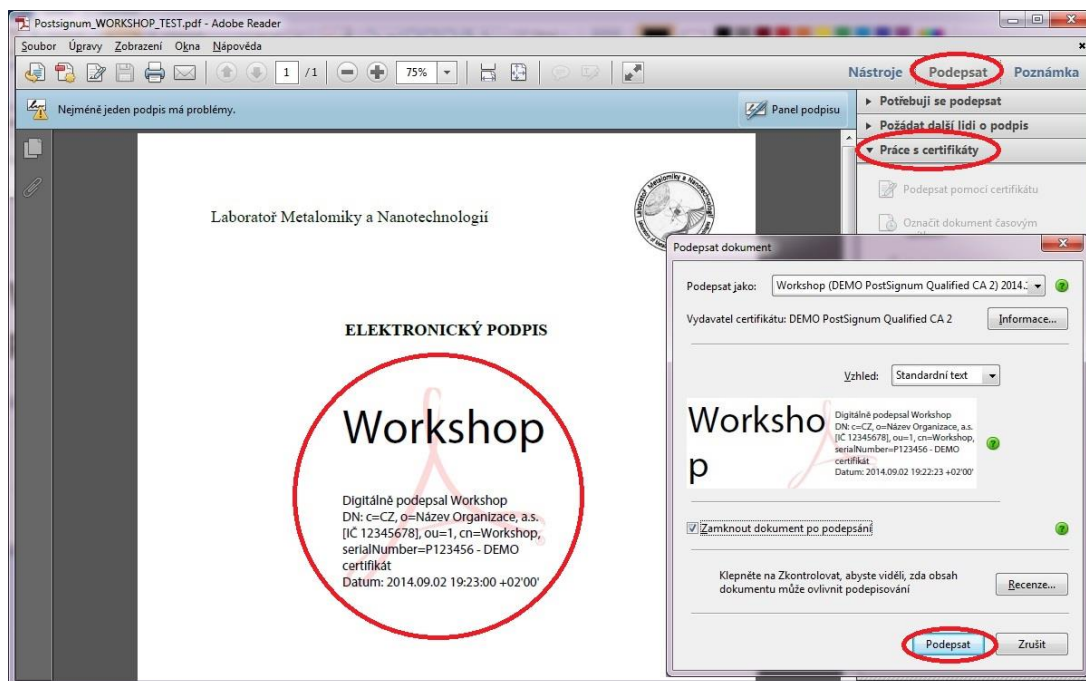
• **Podpis emailu – konfigurace poštovního klienta**



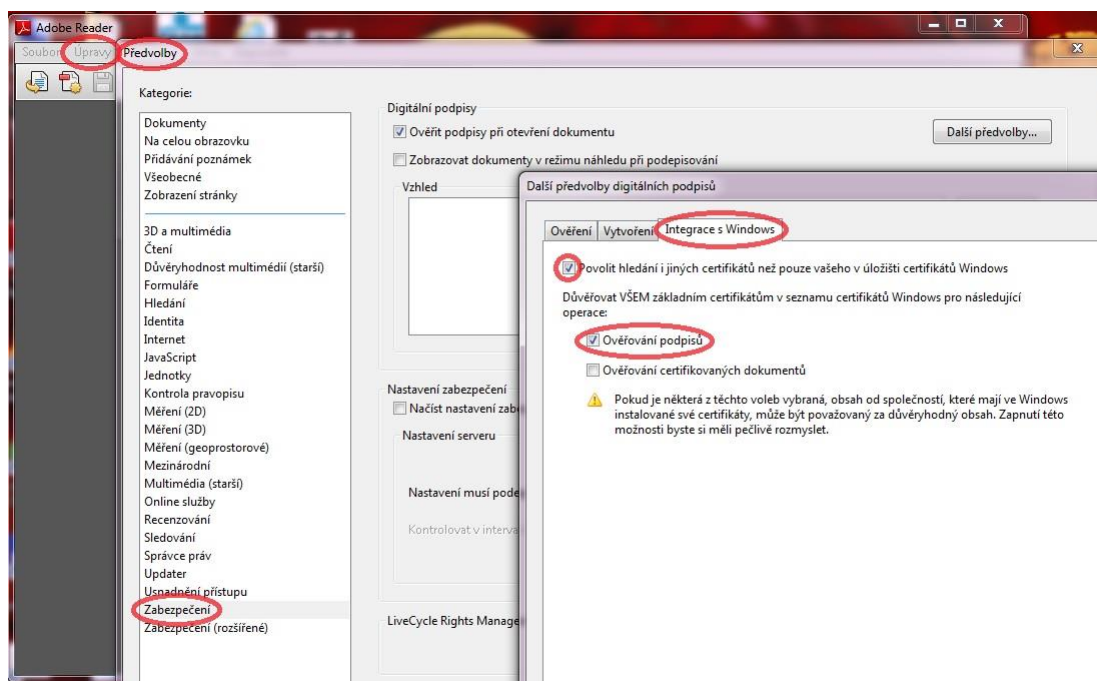
• **Podpis dokumentů – nejčastěji formát Adobe, Office, XML (formuláře)**



- **Podpis dokumentů PDF**



- **Nastavení ověření podpisu v Acrobat Readeru**





Forma použití certifikátu

