

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



WORKSHOP – Elektronický podpis



**Radomil Trtílek, Petr Čapek, prof. Ing. René Kizek, Ph.D., RNDr.
Josef Růžička, Mgr. Michal Horák, Mgr. Ondřej Zítka, Ph.D.**



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



Obsah WORKSHOPU – 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



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ



Práce s programem iSignum

- Generování žádosti
- Záloha klíče
- Instalace certifikátu (obnova ze zálohy)

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



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



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



workshop_postsignum

Uspořádat Otevřít Sdílet s Nová složka

Název položky	Datum změny	Typ	Velikost
certifikat.crt	2.9.2014 14:48	Certifikát zabezpečení	2 kB
demopsqualifiedca2.crt	2.9.2014 14:48	Certifikát zabezpečení	2 kB
demopsrootqca2.crt	2.9.2014 14:48	Certifikát zabezpečení	2 kB

Informace o certifikátu

Certifikát kořenové autority není důvěryhodný. Má-li být považován za důvěryhodný, nainstalujte tento certifikát do úložště důvěryhodných kořenových certificačních autorit.

Vystaveno pro: DEMO PostSignum Root QCA 2

Vystavitel: DEMO PostSignum Root QCA 2

Platnost od 11. 12. 2009 do 11. 12. 2024

Nainstalovat certifikát... Prohlášení vystavitele

Vítej vás Průvodce importem certifikátu.

Průvodce vám pomůže kopírovat certifikáty, seznamy důvěryhodných certifikátů a seznamy odvolaných certifikátů z disku do úložště certifikátů.

Certifikát vydaný certificační autoritou potvrzuje vaši totožnost a obsahuje informace nezbytné k ochraně dat nebo k vytvoření zabezpečených síťových připojení. Úložště certifikátů je systémová oblast, v níž jsou certifikáty uloženy.

Pokračujte kliknutím na tlačítko Další.

Úložště certifikátů

Úložště certifikátů jsou oblasti systému, kde jsou uloženy certifikáty.

Systém Windows může automaticky vybrat úložště certifikátů, nebo můžete zadat umístění certifikátů.

Automaticky vybrat úložště certifikátů na základě typu certifikátu

Všechny certifikáty umístit v následujícím úložště certifikátů:

Další informace o úložštích certifikátů

Dokončení Průvodce importem certifikátu

Certifikát bude nainportován po kliknutí na tlačítko Dokončit.

Zadali jste následující nastavení:

Vybrané úložště certifikátů	Automaticky určeno průvodce
Obsah	Certifikát

Import proběhl úspěšně.

OK



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



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



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti "in vivo" zobrazovacích technik



- Podpis emailu – konfigurace poštovního klienta**

Centrum zabezpečení

Důvěryhodní vydavatelé

3 Možnosti ochrany osobních údajů

Zabezpečení e-mailů

Zpracování příloh

Automatické stahování

Nastavení maker

Programový přístup

Síťovaný e-mail

Zašifrovat obsah a přílohy odeslaných zpráv

Přidat digitální podpis do odeslaných zpráv

Při odeslání podepsané zprávy odeslat podepsanou zprávu bez nutnosti ověření

Požadovat oznámení S/MIME pro všechny zprávy s podpisem S/MIME

Výchozí nastavení: [vypádná menu] [Nastavení...]

Změnit nastavení zabezpečení

Předvolby pro nastavení zabezpečení

Název nastavení zabezpečení:

Kryptografický formát: S/MIME

Výchozí nastavení zabezpečení pro tento formát kryptografických zpráv

Výchozí nastavení zabezpečení všech kryptografických zpráv

Názvy zabezpečení... [Nové] [Odstranit] [Heslo...]

Certifikáty a algoritmy

Podpisový certifikát: [vybrat] [Vybrat...]

Algoritmus hash: [vypádná menu]

Šifrovací certifikát: [vybrat] [Vybrat...]

Šifrovací algoritmus: [vypádná menu]

S podepsanými zprávami odesílat tyto certifikáty

[OK] [Storno]

Zabezpečení systému Windows

Vybrat certifikát

Workshop

Vystavitel: DEMO PostSignum Quali...

Platný od: 2.9.2014 do 2.10.2014

Kliknutím zobrazíte vlastnosti certifikátu

[OK] [Storno]



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti "in vivo" zobrazovacích technik



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

The screenshot displays the Microsoft PowerPoint 2010 interface. The main window shows the 'Informace o dokumentu' (Document Information) pane for 'WORKSHOP_Postsignum_NLABSYS.pptx'. The 'Oprávnění' (Permissions) section is expanded, showing options like 'Zamknout prezentaci' (Lock presentation), 'Označit jako konečný' (Mark as final), 'Zašifrovat pomocí hesla' (Encrypt with password), 'Omezit oprávnění podle uživatelů' (Restrict permissions by user), and 'Přidat digitální podpis' (Add digital signature). The 'Přidat digitální podpis' option is highlighted. A 'Potvrzení podpisu' (Signature Confirmation) dialog box is open, displaying a message: 'Podpis byl úspěšně uložen s dokumentem. V případě změny dokumentu přestane být podpis platný.' (Signature was successfully saved with the document. In case of document change, the signature will no longer be valid.) with an 'OK' button. Another 'Podepsat' (Sign) dialog box is open, showing fields for 'Účel podepsání tohoto dokumentu:' (Purpose of signing this document), 'Podepisující uživatel: Workshop' (Signer: Workshop), and 'Vystavitel: DEMO PostSignum Qualified CA 2' (Issuer: DEMO PostSignum Qualified CA 2). It includes 'Podepsat' (Sign) and 'Storno' (Cancel) buttons.



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti "in vivo" zobrazovacích technik



- Podpis dokumentů PDF**

Postsignum_WORKSHOP_TEST.pdf - Adobe Reader

Soubor Úpravy Zobrazení Ořna Nápověda

Nástroje **Podpsat** Poznámka

Nejméně jeden podpis má problémy.

Laboratoř Metalomiky a Nanotechnologií

ELEKTRONICKÝ PODPIS

Workshop

Digitálně podepsal Workshop
DN: c=CZ, o=Název Organizace, a.s.
[IČ 12345678], ou=1, cn=Workshop,
serialNumber=P123456 - DEMO
certifikát
Datum: 2014.09.02 19:23:00 +02'00'

Podpsat jako: Workshop (DEMO PostSignum Qualified CA 2) 2014. ✓

Vydavatel certifikátu: DEMO PostSignum Qualified CA 2 [Informace...]

Vzhled: Standardní text

Workshop
p

Digitálně podepsal Workshop
DN: c=CZ, o=Název Organizace, a.s.
[IČ 12345678], ou=1, cn=Workshop,
serialNumber=P123456 - DEMO
certifikát
Datum: 2014.09.02 19:22:23 +02'00'

Zamknout dokument po podepsání ✓

Klepněte na Zkontrolovat, abyste viděli, zda obsah dokumentu může ovlivnit podepsávání [Recenze...]

Podpsat Zrušit



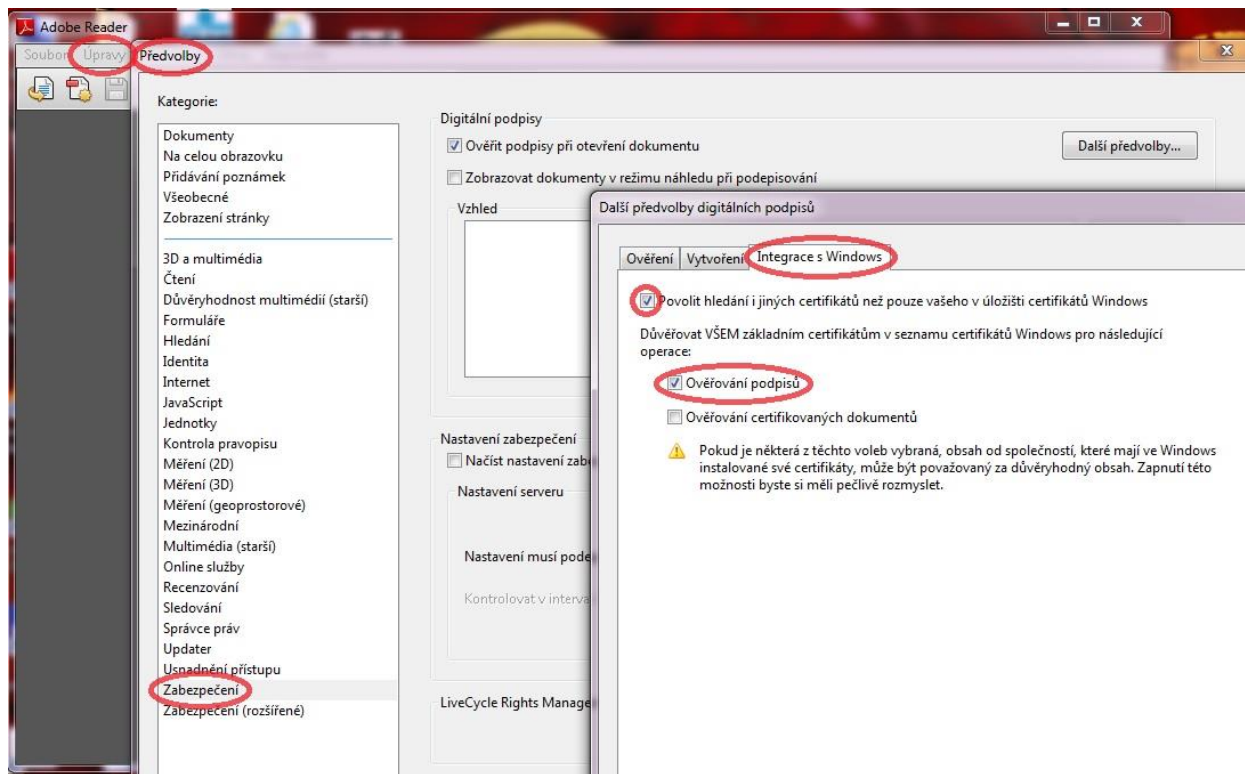
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti "in vivo" zobrazovacích technik



- **Nastavení ověření podpisu v Acrobat Readeru**



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti "in vivo" zobrazovacích technik



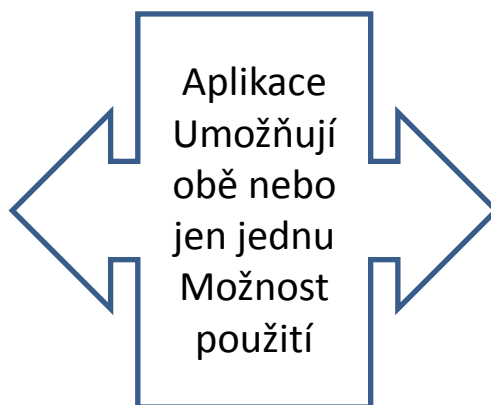
Forma použití certifikátu

Z úložiště

- Systémové (IE, Chrome, Office...)
- Aplikací (Mozilla)



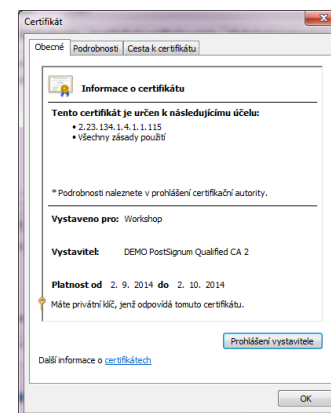
Import ze zálohy certifikátu
(soubor *.pfx)



Ze souboru (*.pfx)

pro podpis

autorizace přístupu



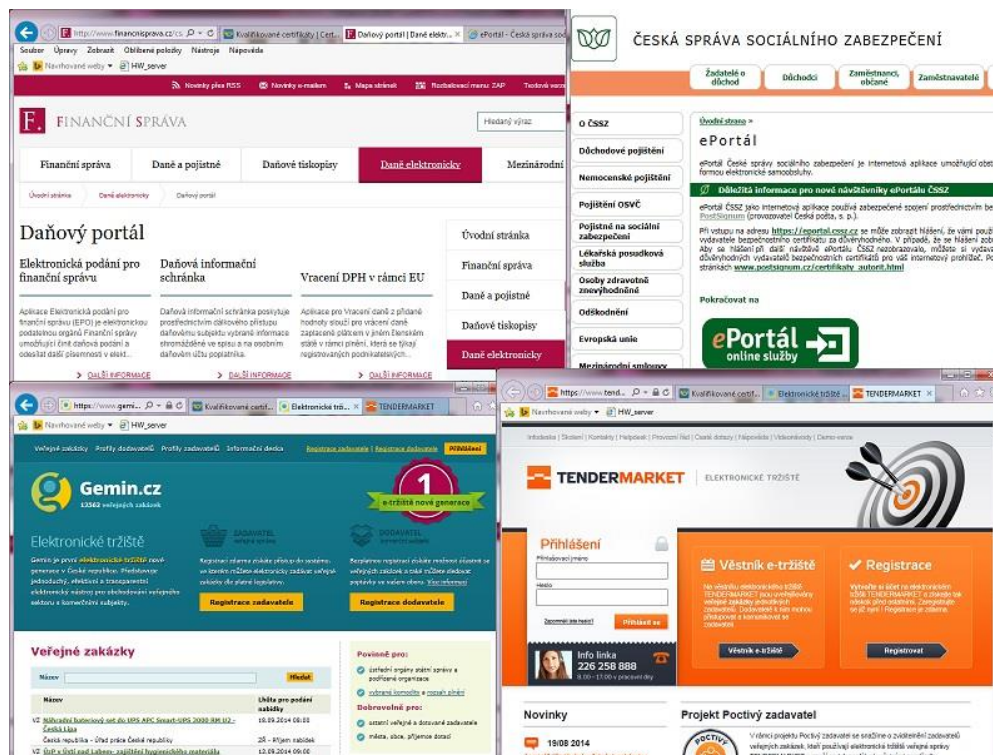
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti "in vivo" zobrazovacích technik



- **Autorizace přístupu, např. portály veřejných zakázek, portály státní správy**



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „*in vivo*“ zobrazovacích technik



Děkuji za pozornost



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ