

CZ.1.07/2.3.00/20.0148

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



Cíle a aplikace elektronického podpisu

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

Datum: 16.7.2014



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ



Cíle elektronického podpisu

- IDENTIFIKACE - z přijaté zprávy musí jednoznačně vyplývat, od koho pochází, resp. kdo je jejím autorem.
- AUTENTIKACE - údaj o autorovi, který z přijaté zprávy vyplývá (v rámci identifikace), musí být dostatečně věrohodný - v tom smyslu, že je nutné mít možnost jej ověřit
- INTEGRITA - jistota, že zpráva nebyla od svého odeslání (přesněji: od svého podpisu, viz dále) jakkoli změněna. Jde o zajištění tzv. zprávy (ve smyslu: neporušenosti), a to nikoli v tom smyslu, že by ke změně obsahu zprávy nemohlo dojít - zde jde pouze o to, aby příjemce dokázal rozpoznat, zda zpráva byla pozměněna nebo nikoli (pokud byla pozměněna, není cílem zjistit jaká byla původní podoba zprávy, ale pouze varovat příjemce že obsah byl změněn).
- NEPOPIRATELNOST - příjemce zprávy chce mít jistotu, že ten kdo je jejím autorem později nepopře své autorství příslušné zprávy.

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



Aplikace elektronického podpisu

Počítačové

- PDF Signer (Dignita)
- FreePDFSign
- Podepsat PDF

Pro mobilní zařízení

- FormApps Mobile (SW602)



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



The image shows two overlapping software windows. The top window is 'PDF Signer © DIGNITA, s.r.o.' with a yellow background. It displays license information: 'Licence: Licence vyprší: 30.6.2010', 'Certifikát: "DIGNITA, s.r.o."', 'Platnost: 26.6.2010 10:42:49 (vyprší za 29 dní)', 'Druh: Určený k podpisu. Není kvalifikovaný.', 'Důvod: ověření dokumentu', 'Umístění: Praha', and 'Klíč: Vložit registrační Verze: 1.0.1.0'. The bottom window is 'Free PDF Sign 1.0' with a grey background. It has a menu bar (Soubor, Jazyk, Pomoc) and several sections: 'Soukromý klíč' with fields for 'PFX soubor:' and 'Heslo:'; 'PDF' with fields for 'Zdrojový soubor:' and 'Cílový soubor:'; 'Vlastnosti' with fields for 'Důvod podpisu:', 'Místo:', and 'E-mail:'. A 'Podpsat PDF dokument' button is at the bottom. A third window, 'Nastavení programu PodepsatPdf', is partially visible in the center, showing settings for certificate placement, visibility, and position.



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



Vlastnosti aplikací elektronického podpisu

- připojování elektronického podpisu k formulářům
- připojování elektronického podpisu k přílohám ve formátu PDF
- připojování kvalifikovaného časového razítka
- podpora rozsáhlých možností práce s dokumentem (převod do formátu PDF, spojování několika dokumentů do jednoho apod.)
- základní autentizace, autentizace komerčním certifikátem
- šifrovaná komunikace se serverem



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti "in vivo" zobrazovacích technik



Aplikace certifikačních autorit

Hlavní funkcí těchto aplikací je generování žádosti, vytvoření certifikátu a jeho záloha do souboru.

Postsignum:

iSignum

První certifikační autorita (I.CA):

I.CA
NEWCERT

Eidentity:

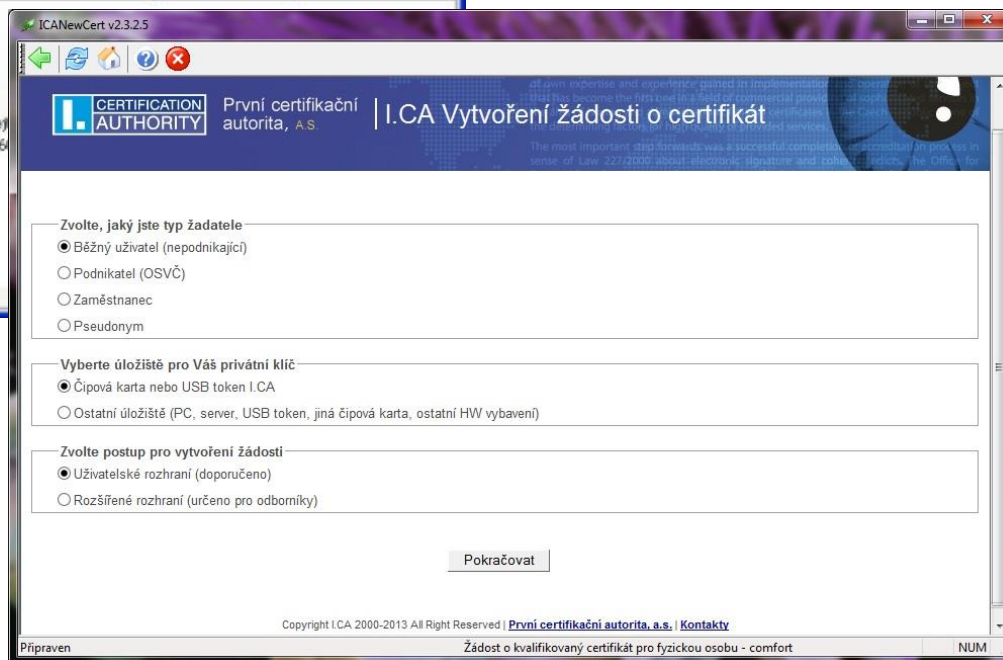
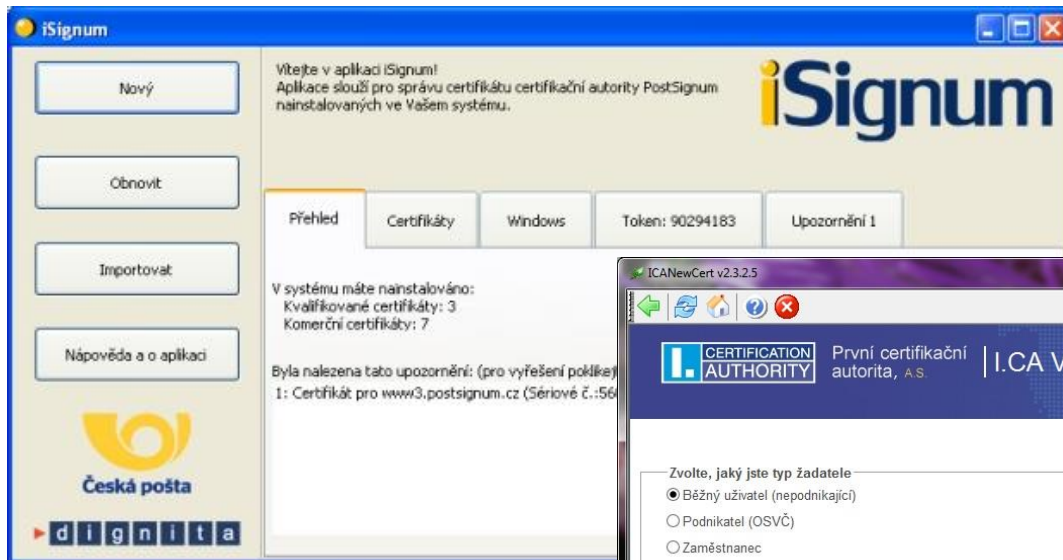
WebApp



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti "in vivo" zobrazovacích technik



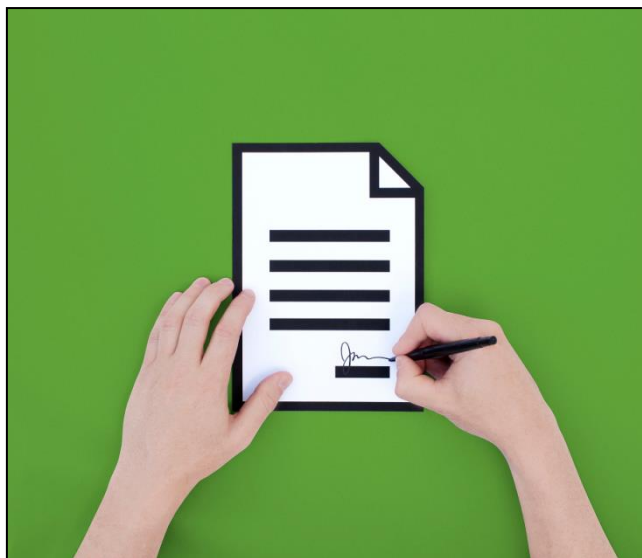
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

CZ.1.07/2.3.00/20.0148

Mezinárodní spolupráce v oblasti „in vivo“ zobrazovacích technik



Děkuji za pozornost



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ