DITEC - Data Information technology & Expert Consulting

ofil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnos

DITEC je vedúcim integrátorom informačných technológií. Svojim zákazníkom poskytujeme komplexné služby v oblasti nasadzovania a prevádzky informačných systémov.

DITEC
Data Information Technology & Expert Consulting

DITEC je firma s tradíciou. Počas svojej existencie sme sa vypracovali na stabilný subjekt, ktorý je dôveryhodným a dlhodobým partnerom významných organizácií.

DSigner.XML

Ján Dobias
Ditec, a.s.

DITEC
Data Information Technology & Expert Consulting

D.Signer/XML

Obsah

- Podmienky a ciele
- Prečo XML
- Bezpečný podpis XML dokumentu
- D.Signer/XML – charakteristika
- Ukážka vytvorenia podpisu

DITEC Data Information Technology & Expert Consulting

1. Požiadavky, ciele

- Vytvorenie podmienok pre používanie ZEP - okrem HW krypto-zariadenia požiadavka na certifikovanú aplikáciu
- podpisovanie (vytváranie ZEP) na základe vôle osoby
- cieľová aplikácia - web-klient
  - obmedzený rozsah
    - » distribúcia cez Internet
  - obmedzená zložitosť
    - » podpis bez časovej pečiatky

DITEC

D.Signer/XML

2. XML

- XML – formát podpisovaného dokumentu
  - jeden z najrozšírenejších formátov pre e-business a e-government
  - dátovo orientovaný protokol – využitie v automatizovaných procesoch
  - nejednoznačnú vizualizácia - potreba predpisu pre vizualizáciu („podpisujem čo vidím“)
- XML - formát podpisu
  - XML Signature – východiskový štandard (alternatíva k PKCS#7)
  - rozšírenia pre „bezpečné“ podpisovanie XML dokumentu – formát XML ZEP

DITEC Data Information Technology & Expert Consulting

3. Bezpečný podpis

- Nepodpisuje sa len vlastný dokument, ale aj:
  - údaje pre overenie dokumentu (ref. certifikátu pre overenie, ref. podpisovej politiky)
  - referencia na predpis pre zobrazenie – XSLT
  - overenie štruktúry – XML schéma (XSD)
- Overenie podpisu
  - matematické overenie (šifr. algoritmy)
  - PKI overenie (platnosť certifikátu)
  - overenie vyplývajúce z formátu – použité XSD, XSLT, podpisová politika

DITEC Data Information Technology & Expert Consulting

4. D.Signer/XML

- Aplikácia certifikovaná NBÚ
  - súlad s CWA 14170 – Security Requirements for Signature Creation Applications (5/2004)
- Formát podpisu – XML Signature (validná štruktúra) + rozšírenia a obmedzenia
- MS ActiveX
  - použitie – web/desktop aplikácie
  - jednoduchá inštalácia – aj cez Internet
- Ďalšie komponenty
  - MS XML Parser (4)
  - bezpečné zariadenie – CSP (otvorenosť voči certifikovaným zariadeniam)

DITEC
Data Information Technology & Expert Consulting

D.Signer/XML

5. Ukážka

DITEC

Data Information Technology & Expert Consulting

Referencie

dobias@ditec.sk
www.ditec.sk

podpisová politika:
http://repository.dtca.sk/2004/common_sp-v1_0.pdf
formát podpisu:
http://repository.dtca.sk/2004/zepxml-v2_0.pdf
certifikát NBÚ:
http://www.nbusr.sk/NBU_SEP/default.php