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.

Zaručený elektronický podpis

Ako ho môžeme naozaj využívať

Obsah

- Legislatívna báza ZEP
- Praktické aspekty používania ZEP
- Implementácia aplikácie pre ZEP
- D.Signer/XML

1. Legislatívna báza

- Zákon č. 215/1002 Zb.
  - §4 odsek 1 – splnenie podmienok pre ZEP
    - » je vyhotovený pomocou súkromného kľúča, ktorý **je určený na vyhotovenie ZEP**,
    - » možno ho vyhotoviť **len s použitím bezpečného zariadenia** na vyhotovovanie EP podľa § 2 písm. h),
    - » na verejný kľúč patriaci k súkromnému kľúču použitému na vyhotovenie ZEP je vydaný **kvalifikovaný certifikát**.
  - §5 odsek 1 – používanie ZEP
    - » ak možno v styku s verejnou mocou používať EP, tento EP **musí byť ZEP**

DITEC
Data Information Technology & Expert Consulting

ITAPA 2004

- §24 odsek 1 - požiadavky na produkty pre ZEP
  - » na uchovávanie súkromných kľúčov a na vyhotovovanie ZEP **sa musia používať** bezpečné zariadenia na vyhotovovanie EP, ktoré .....
- §24 odsek 3 – bezpečné zariadenia musia ... :
  - » spoľahlivo zabezpečiť, že podpisovaný elektronický dokument **pri vyhotovovaní ZEP sa nemení**,
  - » umožniť, aby sa elektronický dokument, ktorý sa bude elektronicky podpisovať, **zobrazil podpisovateľovi** ešte predtým, ako sa spustí procedúra na vyhotovenie ZEP,
  - » . . .

- Vyhláška NBÚ 537/2002 - definícia formátu a spôsobu vyhotovenia ZEP
  - §3 Čl. 2 – definovanie formátov ZEP (bez ČP, ...)
  - §3 – podpisová politika
    - » . . . súbor pravidiel upravujúcich vyhotovovanie a overovanie zaručených elektronických podpisov . . .
    - » subjekt, ktorý prijíma dokumenty podpísané zaručeným elektronickým podpisom, určí podpisovú politiku, ktorú akceptuje.
    - » podpisovateľ a overovateľ zaručeného elektronického podpisu použijú tú istú podpisovú politiku.
  - §6 - Podpisové schémy na vyhotovovanie ZEP a časovej pečiatky

DITEC
Data Information Technology & Expert Consulting

ITAPA 2004

- Vyhláška NBÚ 538/2002 - kvalifikované certifikáty
- Vyhláška NBÚ 539/2002 - požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre EP
  - §3 Odsek 1 - **produkty určené na uchovávanie súkromných kľúčov** a na vyhotovenie ZEP
  - §3 Odsek 2 - požiadavky podľa odseku 1 možno primerane uplatniť aj na **produkty na vyhotovovanie EP**
- Vyhláška NBÚ 540/2002 - akreditované certifikačné služby

DITEC
Data Information Technology & Expert Consulting

ITAPA 2004

- Vyhláška NBÚ 541/2002 - prevádzková dokumentácia CA, bezpečnostné pravidlá a pravidlá pre výkon certifikačných činností
- Vyhláška NBÚ 242/2002 - o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku
  - §3 – použitie ZPE - v administratívnom styku možno na podpisovanie elektronického dokumentu používať len ZEP
  - §6 – elektronická podateľňa
  - §9 – formáty elektronických dokumentov (aj XML)

2. Používanie ZEP

- ZEP je nevyhnutnosťou pre implementáciu elektronických procesov pre štátnu správu (portálu štátnej správy)
- Oblasti využitia ZEP
  - ekvivalent k vlastnoručnému podpisu - papierový dokument vs. elektronický dokument
  - použitie obmedzené ostatnou legislatívou - služby a procesy dané zákonom a vyhláškami (oblasti G2C, G2B), komerčná a občianska komunikácia
  - kde je potrebné dosiahnuť dôveryhodnú identifikáciu, autorizáciu a neodmietnuteľnosť – úzka väzba na pravidlá využitia obsahu dokumentu

Čo môžeme podpisovať ZEP

- Formáty elektronických dokumentov definované NBÚ
  - RTF, PDF, HTML, XML, SHTTP, S/MIME ...
- „office“ formáty
  - neštruktúrované údaje, vhodné pre štandardné administratívne agendy
  - obtiažne automatizované
  - „štandardizované“ vizualizačné prostriedky
- XML
  - dátovo-orientovaný formát, vhodný pre automatické spracovanie
  - vizualizácia problematická

Čo potrebujeme pre ZEP

- kvalifikovaný certifikát podpisovateľa – vydaný ACA
- certifikovaný prostriedok pre generovanie a uchovávanie kľúčov
  - SCDev – Secure Creation Device
- certifikovaná aplikácia pre vytváranie ZEP
  - SCA – Secure Creation Application
  - certifikovaná pre XML a „office“ formáty
- schválený formát vytváraného ZEP
- zverejnená podpisová politika

3. SCA - vytváranie ZEP

- Vytvorenie ZEP:
  - z hľadiska používateľa jednoduchá procedúra
  - nesmie viesť k narušeniu bezpečnosti privátneho kľúča
  - univerzálna – pre viac typov (formátov) dokumentov
- Používateľ musí:
  - vedieť, že vytvára ZEP
  - vidieť, aké údaje podpisuje a rozumieť im
  - explicitne odsúhlasiť použitie privátneho kľúča na vytvorenie ZEP

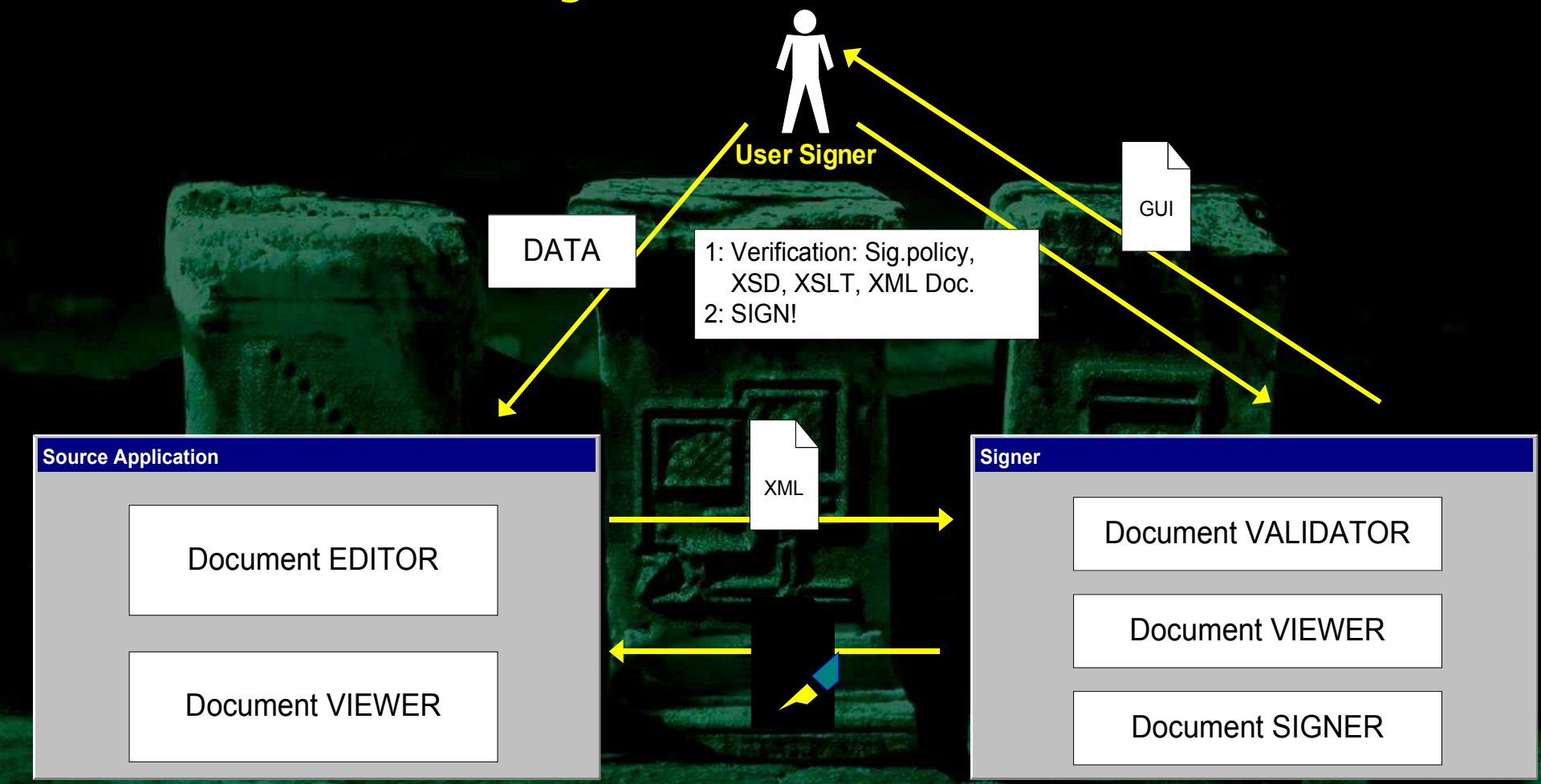
Požiadavky na SCA

- Referenčný popis požiadaviek na SCA
  - CWA 14170
- Základná funkčnosť:
  - prevziať elektronický dokument (údaje) a príslušné parametre podpisu,
  - vizuálne ich prezentovať podpisovateľovi, a to jednoznačným, adekvátnym a zrozumiteľným spôsobom,
  - umožniť podpisovateľovi na základe jeho explicitného súhlasu vytvoriť nad podpisovanými údajmi ZEP
  - garancia nezmenenia údajov po zobrazení pri podpise

Problémy so SCA

- Formát podpisu
  - závislý od typu dokumentu a spôsobu použitia (PKCS #7, XML Signature, XML AdES, ...)
- Spôsob vizualizácie podpisovaného dokumentu
  - závislý od typu dokumentu
- Prevádzka v existujúcich prostrediach
  - čo je potrebné implementovať a čo je možné využiť z operačného prostredia
- Ako vieme, že bol vytvorený certifikovaným zariadením ?
  - iba QC (overenie „kvalifikovanosti“ certifikátu !!)

Procedúra vytvárania ZEP



Procedúra vytvárania ZEP

1. vytvorenie údajov v zdrojovej aplikácii
2. poskytnutie údajov „podpisovacej aplikácii“
3. vizualizácia podpisovaného dokumentu podpisovateľovi
4. podpisovateľ overí:
   - podpisovú politiku, vizuálne správnosť podpisovaných údajov
5. podpisovateľ rozhodne o podpísaní
6. vrátenie podpísaného dokumentu do aplikácie

Podpisová politika

- podporované typy záväzkov (napr. schválenie dokumentu)
- povinnosti podpisovateľa, overovateľa a spoliehajúcej sa strany
- bezpečnostné požiadavky na prevádzkové prostredie
- pravidlá platnosti ZEP (formáty dokumentov, formát ZEP, atribúty ZEP, certifikáty)
- spôsob prevádzky a používania SCA
- Spôsob zverejňovania a zmien podpisovej politiky

4. D.Signer/XML

- Certifikovaná bezpečná aplikácia pre vytváranie ZEP určená pre XML dokumenty
- Prevádzkové prostredie
  - Win32 (2000, XP, 2003) – ActiveX, COM
  - využívané súčasti: MS XML Parser, MS Crypto API)
  - integrácia do aplikácií pre MS IE > 5.0
- Otvorenosť a interoperabilita
  - možnosť použitia kvalifikovaných certifikátov všetkých ACA v SR
  - podpora certifikovaných SCDev integrovaných cez CSP (Cryptographic Service Provider)

DITEC
Data Information Technology & Expert Consulting

ITAPA 2004

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Č. : 3499/2004/EP-011

Bratislava 24. septembra 2004

Príloha: 1/3

Národný bezpečnostný úrad podľa § 10 ods. 2 písm. j) zákona č.215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov vydáva

Certifikát bezpečného produktu pre zaručený elektronický podpis

Názov produktu: D.Signer/XML

Typ, varianty alebo verzia: version 1.0

Hash odtlačok výslednej knižnice (SHA 1):DSig.dll [24e12b085fba236c12919043293b163033ddaf80]

Použitie produktu: pre vyhotovenie zaručeného elektronického podpisu XML dokumentov

Výrobca: Ditec, a.s., Plynárenská 7/C, 82109 Bratislava

Číslo záverečného protokolu: ZP-006 /2004 **č. p.:** 3499/2004/EP

Doba platnosti certifikátu do: 24. septembra 2007

Týmto certifikátom sa osvedčuje spôsobilosť bezpečného produktu pre vyhotovenie zaručeného elektronického podpisu XML dokumentov.

Obmedzenie a podmienky použitia:

Obmedzenia a podmienky použitia sú uvedené v prílohe, ktorá je neoddeliteľnou súčasťou tohto certifikátu.

NBÚ si vyhradzuje právo zrušiť platnosť certifikátu, ak po jeho vydaní nastanú okolnosti, pre ktoré by tento certifikát nevydal.

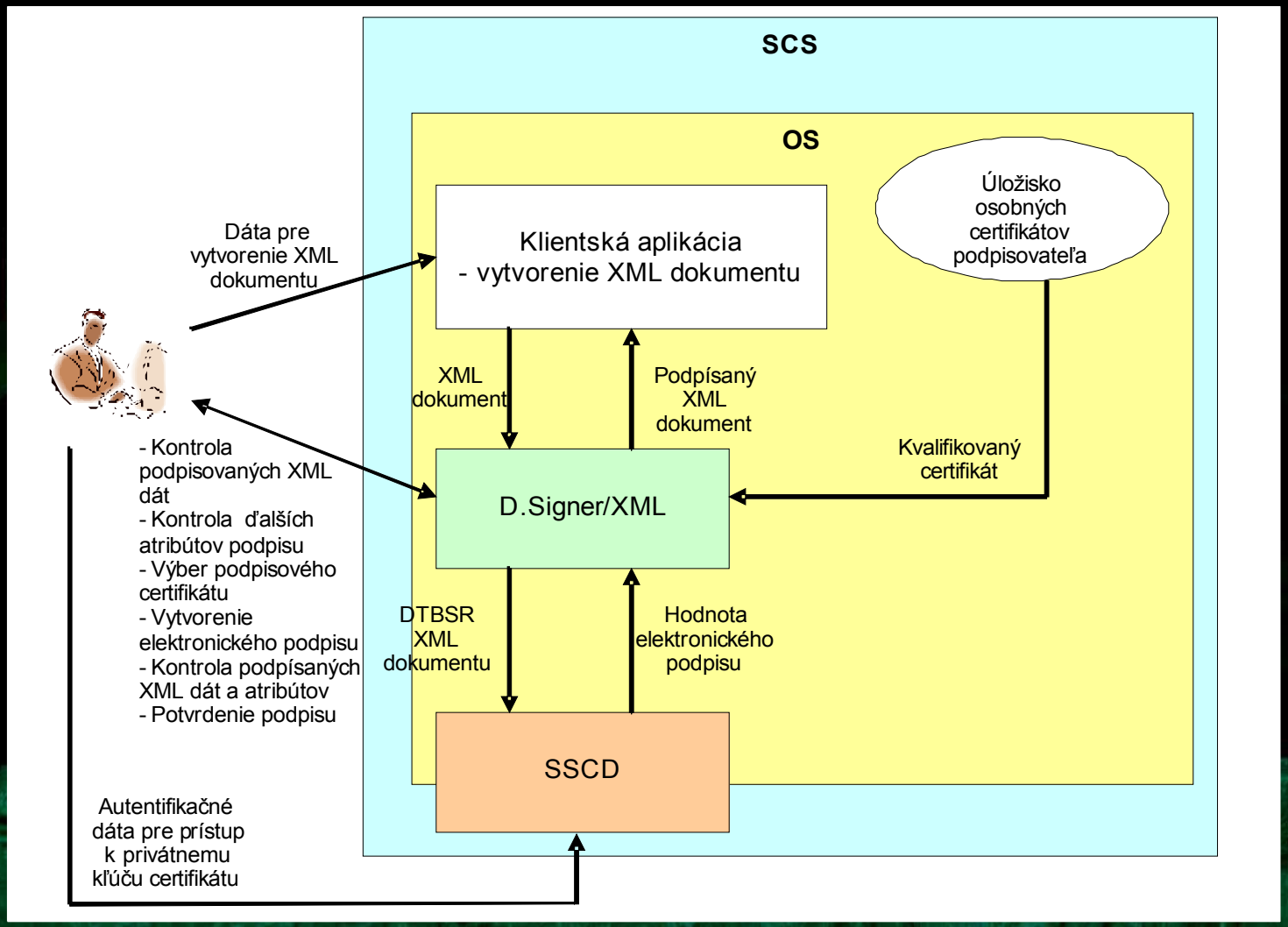
Národný bezpečnostný úrad
3

Aurel Ugor
riaditeľ NBÚ

Problematika XML

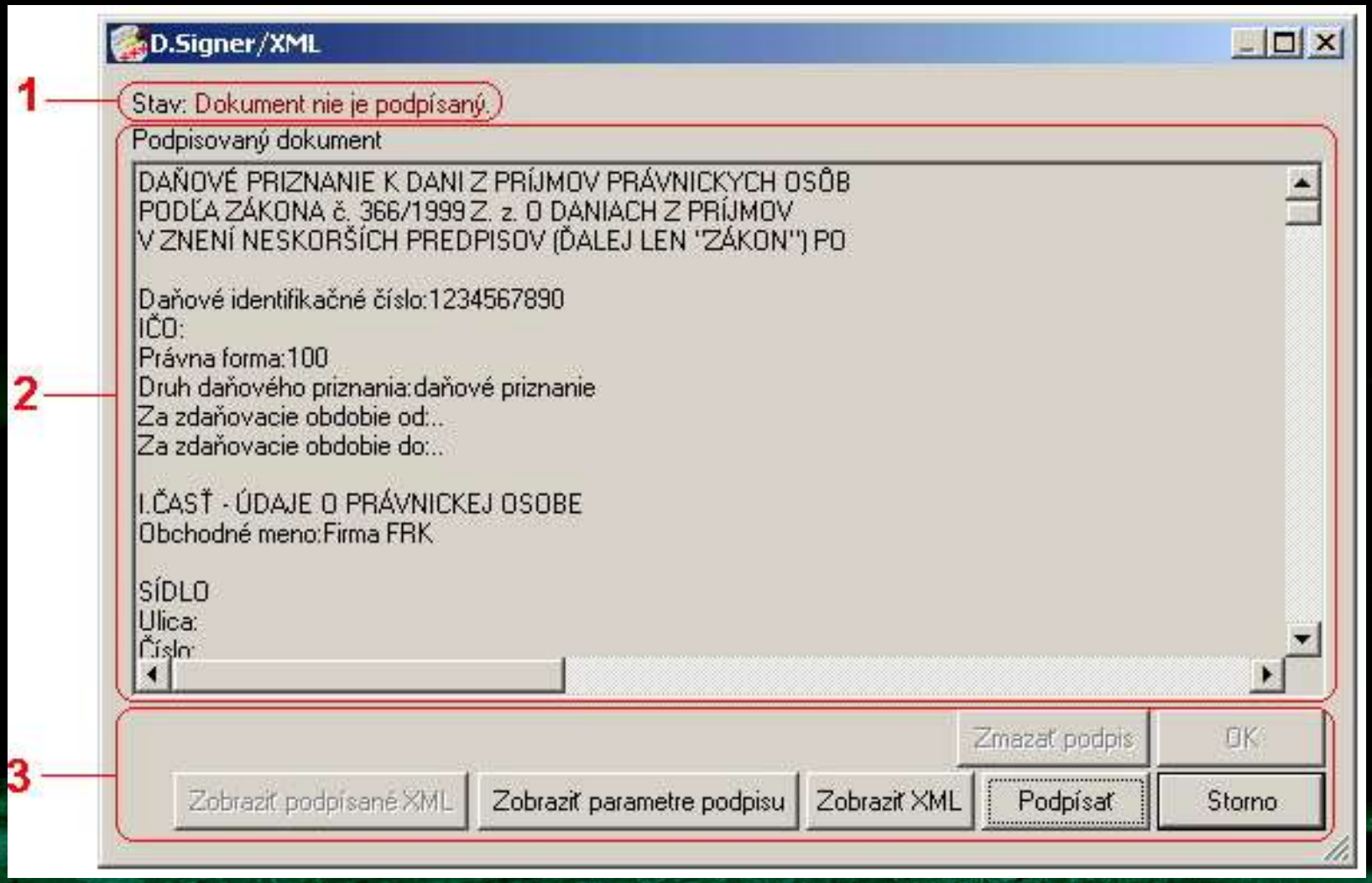
- XML – dátovo orientovaný formát rozšírene využívaný v elektronickej komunikácii
- Základné technológie:
  - XSD – definovanie XML schémy, validačné pravidlá
  - XSLT – transformácia XML schémy do vizualizačného formátu
- ZEP a XML
  - ZEP vyžaduje použitie správneho XSD a XSLT, ktoré musí publikovať „vlastník procesu“
  - potreba dôveryhodného získania a overenia správnosti informácii k ZEP (XSD, XSLT)

Architektúra SCA



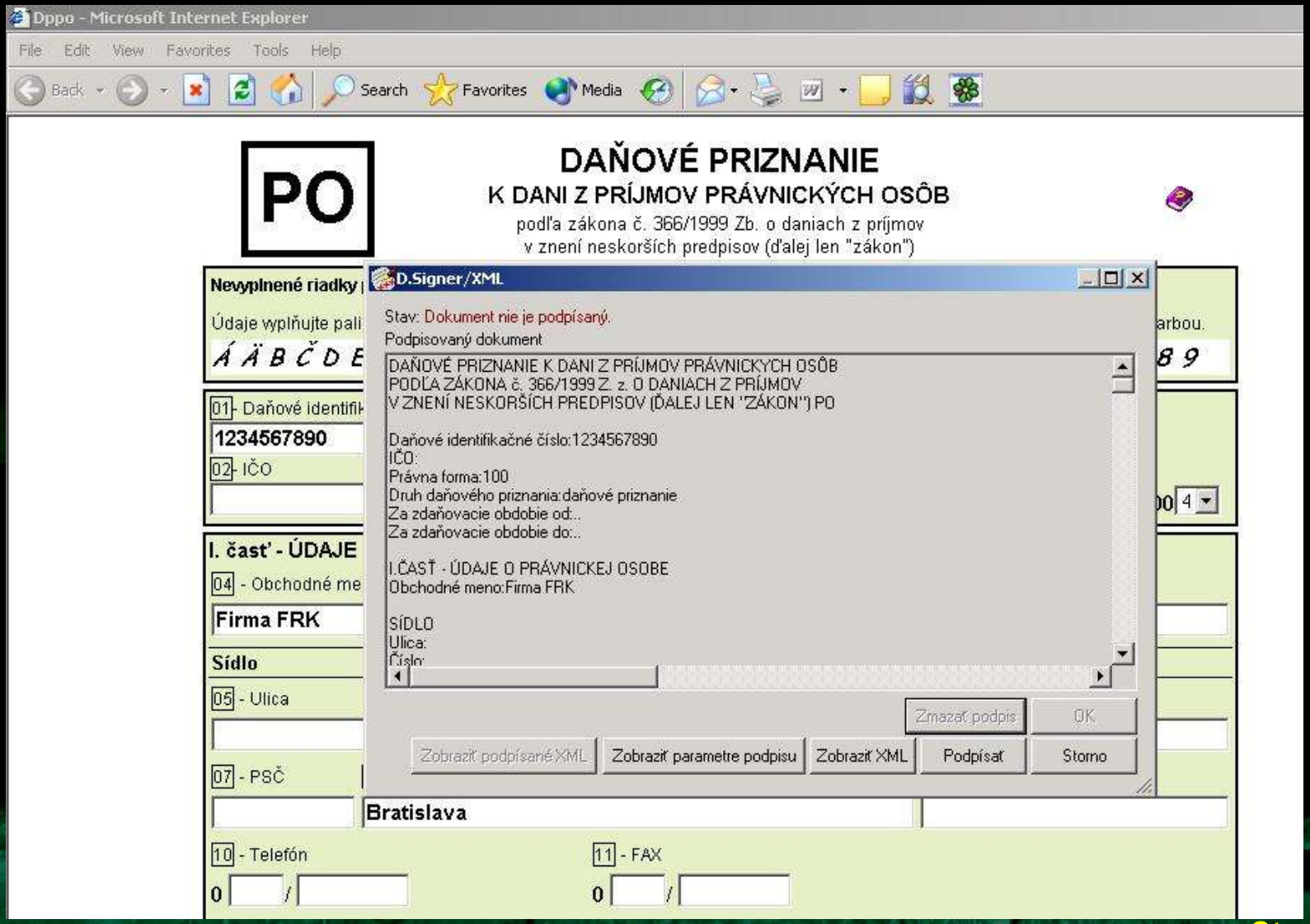
DITEC

ITAPA 2004



DITEC

ITAPA 2004



Formáty a štandardy

- Normy a štandardy
  - CWA14170 – Security requirements for SCA
  - XML
  - XML Signature Syntax and Processing
  - XML Signature Requirements
  - Canonical XML
  - XML Schema: Structures, Datatypes
  - XSL Transformation

DITEC
Data Information Technology & Expert Consulting

ITAPA 2004

- **Formát a štruktúra podpisu**
  - XML Signature rozšírený o atribúty vyžadované ZEP
    - » XML schéma dokumentu,
    - » XSL transformácia dokumentu,
    - » referencia na podpisovú politiku aplikácie D.Signer/XML,
    - » identifikátor certifikátu pre overenie podpisu (certifikát podpisovateľa)
- **Podporované podpisové schémy**
  - RSA-SHA1
  - DSA-SHA1

Podpisová politika

- Špecifické požiadavky – vyplývajúce z charakteru XML technológie
  - podpisovaný (zdrojový) elektronický dokument - štruktúra dokumentu definovaná v rámci XML schémy – XSD (syntax)
  - vizuálna transformácia dokumentu (XSLT)
- Základné identifikačné údaje:
  - URL: http://repository.dtca.sk/2004/common_sp-v1_0.pdf
  - URI: http://uri.dtca.sk/signature_policies/common/v1.0
  - OID: 1.3.6.1.4.1.19725.3.1.1

5. Prijatie ZEP - podateľňa

- Pre plné nasadenie ZEP do procesov je potrebné zabezpečiť overenie, resp.prijatie elektronického dokumentu
- Overenie ZEP
  - overenie platnosti certifikátu (zoznam ACA, CRL, resp. časové pečiatky)
  - overenie formátu podpisu
  - overenie súladu s podpisovou politikou (napr. typ záväzku)
  - dôveryhodné overenie ZEP
  - archivácia elektronického dokumentu

Scenáre použitia podateľne

- Podpisovateľ – občan, overovateľ – úrad
  - prevzatie úradom v záujme občana
- Podpisovateľ – úrad, overovateľ – občan
  - potvrdenie o doručení – prevzatie v záujme občana
  - doručenie dokumentu – problém s potvrdením prevzatia (poznám obsah až keď potvrdím prevzatie)
  - problém s vynúteným prevzatím

Elektronická podateľňa

- Základné vlastnosti:
  - potrebuje využívať službu časovej pečiatky
  - dôveryhodné overenie platnosti certifikátu v čase prijatia (ak sa nejedná o ZEP s ČP)
- Otvorené otázky:
  - konkrétny pracovník alebo „organizácia“ (zástupca organizácie)
  - automatizované podpisovanie
  - identifikácia podpisovateľa

DITEC
Data Information Technology & Expert Consulting

ITAPA 2004