DITEC - Data Information technology & Expert Consulting

Profil 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.

Elektronický podpis a jeho použitie

Mýty a realita

Pavol Frič, DITEC a.s.

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

Obsah

- Prečo elektronický podpis
- Možné alternatívy k EP
- Fakty a mýty o EP

DITEC Data Information Technology & Expert Consulting

1. EP a dôvody jeho používania

- Rozporuplné názory na elektronický podpis
  - častokrát prezentovaný ako nádejná technológia použiteľná pre eGovernment a eBusiness
  - v poslednom čase v SR mnohokrát spomínaný ako brzda rozvoja eGovernmentu
- Kde je teda pravda ?
  - pri posudzovaní EP treba analyzovať možnosti jeho reálneho využitia v procesoch eGovernmentu
  - technológia a jej vyzretosť nie je kľúčovým faktorom (toto až následne)

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- eGovernment = el. výkon verejnej moci
  - reprezentácia procesov v el. forme tak, aby bola zachovaná právna záväznosť a nespochybniteľnosť
  - základom týchto procesov je **právny úkon**
    - » je **prejav vôle** smerujúci najmä k vzniku, zmene alebo zániku tých práv alebo povinností, ktoré právne predpisy s takýmto prejavom spájajú (Zák č. 40/1964 – Obč. zákonník)
    - » má zákonom predpísané náležitosti:
      - forma - akým má byť úkon realizovaný
      - obsah - potrebné údaje/informácie, ktoré musia byť viazané k danému úkonu
      - autorizácia - spravidla podpisom osoby (legislatíva môže stanovovať špecifické požiadavky, napr. pečiatka a pod.)
      - platnosť - naplnenie formálnych požiadaviek na úkon (napr. oprávnenie k realizovaniu úkonu)

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **Čo je potrebné pri elektronickej reprezentácii právneho úkonu dosiahnuť:**
  - identifikácia účastníka úkonu
    - » jasné určenie osoby/osôb, ktoré úkon zrealizovali
  - zachytenie obsahu úkonu
    - » jednoznačné previazanie právneho úkonu s jeho obsahom a zabezpečenie zachyteného obsahu úkonu pred neautorizovanými zmenami po vykonaní úkonu
  - zachytenie prejavu vôle (autorizácia)
    - » zabezpečenie nemožnosti následného popretia realizovania úkonu
  - nespochybniteľnosť
    - » nespochybniteľnosť vykonania úkonu a jeho náležitostí (t.j. bezpečné a „nepriestrelné“ riešenie zamedzujúce pochybnosti a prípadné následné spory)

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

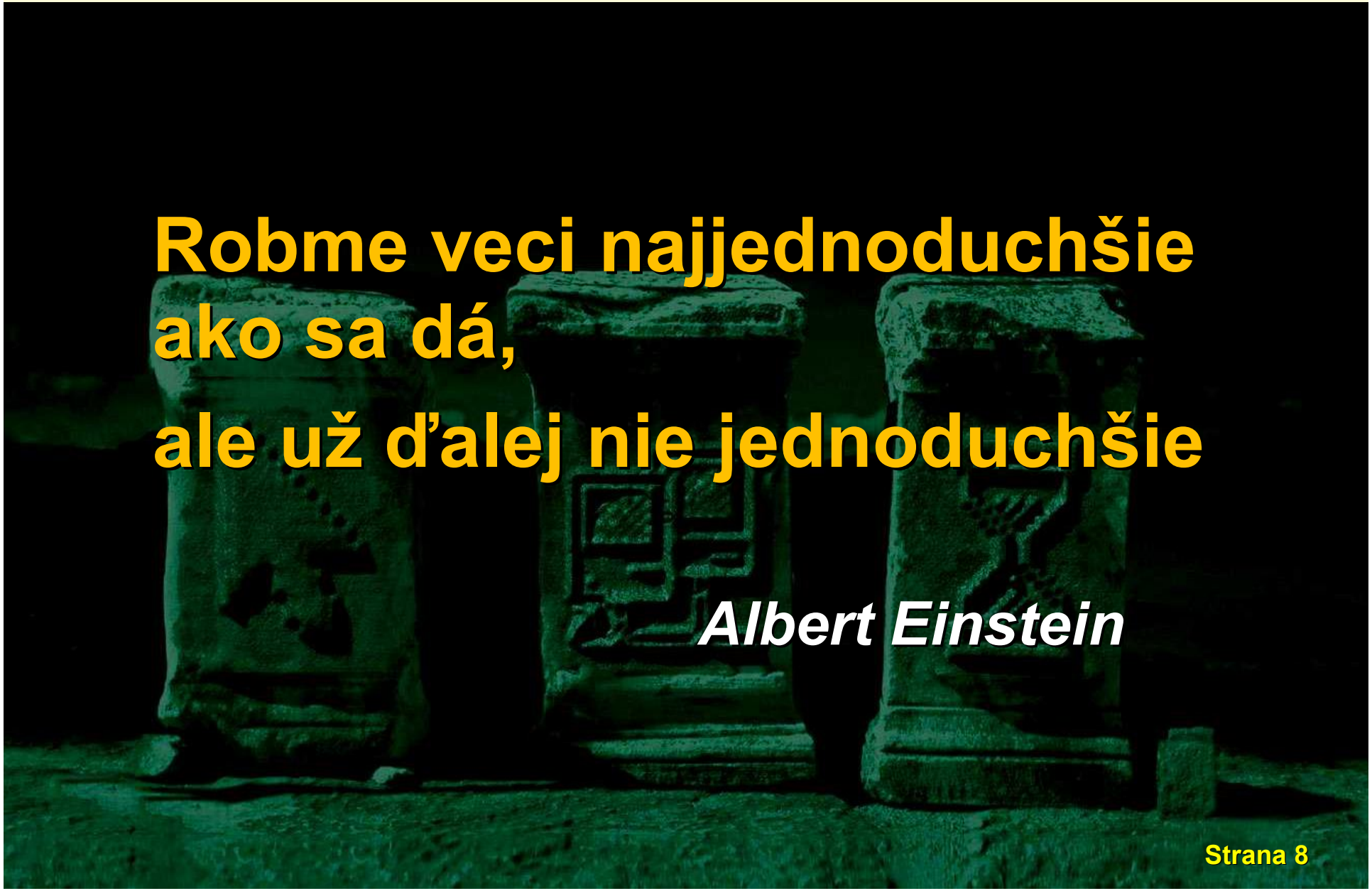
- **Čo je najväčšie riziko:**
  - **použitie riešenia, ktoré je možné následne spochybniť**
    - » **toto bude viesť k množstvu súdnych sporov, v ktorých môže byť dokazovacia pozícia orgánov verejnej moci oslabená práve riešením, ktoré je možné objektívne spochybniť (aj dôvodná pochybnosť „mohlo sa stať“, „nie je vylúčené“ postačuje)**
    - » **viedlo by to k spochybnenie eGovernmentu ako celku, nakoľko ho nie je možné „bezpečne“ a plnohodnotne realizovať ako reálnu alternatívu „papierových“ procesov**

2. Možné alternatívy

- Možnosti riešenia
  - definované súčasnou legislatívou
    - » elektronický podpis (EP)
    - » zaručený elektronický podpis (ZEP)
  - iné, legislatívne zatiaľ nepodporované alternatívy
    - » alternatíva – ZEP- alebo EP+ (zníženie požiadaviek na ZEP)
    - » bez autorizácie, iba identifikácia používateľa
    - » autorizácia gridovou kartou karty
    - » biometrický podpis
- Kritériá posudzovania
  - bezpečnosť a nespochybniteľnosť
  - garancie pre použitie v eGov (garančná schéma)

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise



DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **Elektronický podpis**
  - v podstate iba implementácia základných princípov bez ďalších požiadaviek na algoritmy, procesy a bezpečnosť
    - » asymetrické šifrovanie v súpojení s hash-funkciami
    - » PKI systém pre správu certifikátov verejných kľúčov
  - neposkytuje sám osebe záruky vyžadované pri reprezentácii požadovaných náležitostí el. úkonov:
    - » identifikácia účastníka úkonu
    - » zachytenie obsahu úkonu
    - » zachytenie prejavu vôle (autorizácia)
    - » nespochybniteľnosť

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **Zaručený elektronický podpis**
  - EP doplnený o ďalšie požiadavky
    - » použitie certifikovaného zariadenia pre uchovávanie privátneho kľúča
      - ochrana PK vlastníka pred neautorizovaným použitím (pri aktivácii PIN, nemožnosť exportu a kopírovania/duplikácie pPK
    - » použitie kvalifikovaného certifikátu
      - zabezpečenie procesu preverenia identity držiteľa a jej kontrolované uvedenie v kvalifikovanom certifikáte – výdávané ACA
      - ochrana pred vystavením viacerých certifikátov na identický privátny kľúč
      - možnosť reprezentácie oprávnenia – mandátny certifikát
    - » použitie certifikovanej aplikácie pre vytváranie a overovanie ZEP
      - použitie schválených „bezpečných“ algoritmov
      - definovaný proces vytvárania a overovania zabraňujúci spochybneniu vykonania úkonu
      - používateľ garantovane vidí čo podpisuje (predpísaným spôsobom)

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **výhody použitia**
  - » ukotvenie v legislatíve (**zrovnoprávnený s vlastnoručným a úradne osvedčeným podpisom**)
  - » priama väzba na podpisovaný dokument a identitu podpisovateľa
  - » kontrola používateľa nad procesom podpisovania
  - » jednoduchosť a dostupnosť procesu overovania platnosti ZEP
  - » ochrana podpisových údajov (privátneho kľúča)
  - » jasne určený postup pri diskreditáci VK (zrušenie certifikátu)
- **ZEP napĺňuje všetky požiadavky pre reprezentovanie náležitostí právneho úkonu v elektronickej forme**

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **ZEP- alebo EP+**
  - otázka je, ktorú požiadavku pre ZEP vypustiť tak, aby bezpečnostné záruky pre použitie v procesoch eGovernmentu ostali zachované, resp. aké požiadavky pre EP definovať
    - » vypustenie alebo „zmäkčenie“ niektorej z požiadaviek na ZEP vedie k spochybneniu reprezentácie požadovaných náležitostí právneho úkonu
    - » domnievame sa, že opäť skončíme v zásade u ZEP

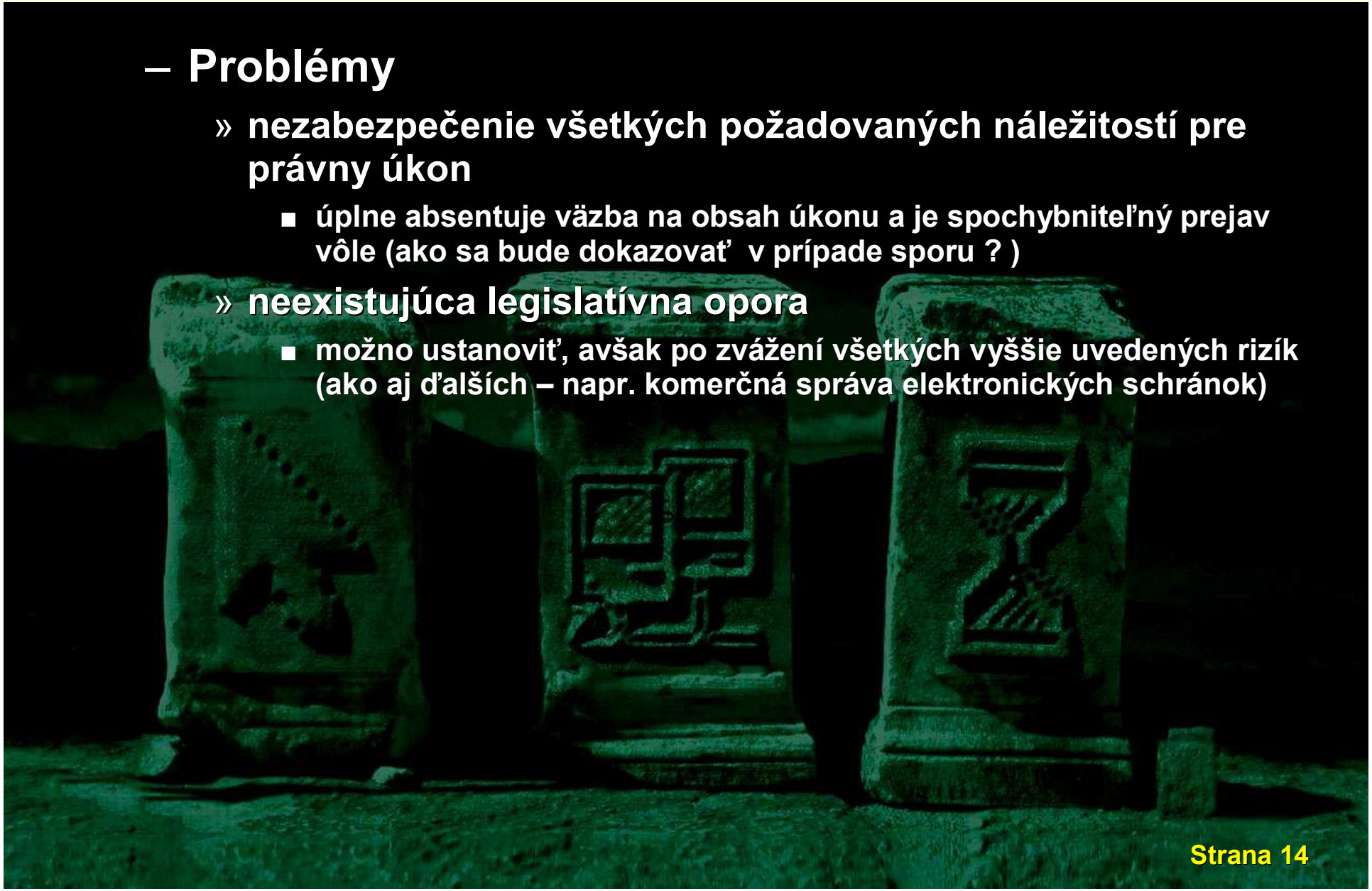
DITEC Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **Iba identifikácia používateľa**
  - Popis
    - » používateľ „sa prihlási“ do systému a následne bez vyžadovania autorizácie vykoná úkon (pošle dokument)
  - Dosiahnutie základných vlastností právneho úkonu
    - » preukázanie identity osoby vykonávajúcej úkon
      - vo väzbe na následnú absenciu autorizácie bude treba „silný“ autentifikačný mechanizmu, napr. založený na PKI (t.j. EP)
    - » väzba na obsah úkonu - integrita dokumentu
      - po vykonaní úkonu možná následná zmena obsahu
      - možné použitie iných mechanizmov, napr. TS, avšak mimo kontroly osoby, ktorá úkon vykonala
    - » prejav vôle - väzba identity a obsahu úkonu
      - kombinácia „slabej autentifikácie“ a nezabezpečenia integrity pod kontrolou osoby vykonávajúce úkon vytvára reálne podmienky pre spochybnenie úkonu (dokazovanie založené na čom ?)

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise



- **Problémy**
  - » **nezabezpečenie všetkých požadovaných náležitostí pre právny úkon**
    - úplne absentuje väzba na obsah úkonu a je spochybniteľný prejav vôle (ako sa bude dokazovať v prípade sporu ?)
  - » **neexistujúca legislatívna opora**
    - možno ustanoviť, avšak po zvážení všetkých vyššie uvedených rizík (ako aj ďalších – napr. komerčná správa elektronických schránok)

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

Autorizácia – gridová karta

- Popis
  - » pri autorizácii je používateľ zadaný k zadaniu hodnoty z grid-karty, pričom pozícia je „vypočítaná“ z obsahu dokumentu
- Dosiahnutie základných vlastností právneho úkonu
  - » východiská pre úvahu
    - karta 10x10 (väčšia ťažko použiteľná) – t.j. 100 pozícií
    - pozícia má 4 alfanumerické znaky, t.j. cca 1,5 mil možností
  - » preukázanie identity osoby vykonávajúcej úkon
    - zabezpečenie jedinečnosti hodnoty na pozícii pre používateľa – limit počtom 1,5 mil. používateľov a treba zabezpečiť jednoznačnosť na každej pozícii v procese generovania
    - možné zvýšenie počtu znakov

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- » väzba na obsah úkonu - integrita dokumentu
  - nedostatočný mechanizmus – možnosť transformácie obsahu do 100 pozícií, t.j. je možné vytvoriť iný dokument s rovnakou pozíciou – predpoklad pre spochybnenie akéhokoľvek dokazovania
  - pre ilustráciu – SHA-2 je (2)256, t.j cca (10)77 možných transformácií + je to auditovaný a „bezpečný“ algoritmus
- » prejav vôle - väzba identity a obsahu úkonu
  - kombinácia mechanizmu autentifikácie a „slabého“ mechanizmu zabezpečenia integrity vedie k reálnej možnosti spochybnenia úkonu ako takého. Dôkazová pozícia pre štát v prípade sporu v tomto prípade je veľmi nevýhodná

– Problémy

- » nezabezpečenie všetkých požadovaných náležitostí pre právny úkon
  - spochybniteľná väzba na obsah úkonu a následne prejav vôle
- » neexistujúca legislatívna opora

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

Biometrický podpis

- Princíp
  - » proces vytvárania podpisu je unikátny a prakticky nenapodobiteľný ako odtlačok prsta – jasná väzba na osobu
- deklarované prínosy
  - » neobmedzená doba platnosti - podpis nie je založený na expirujúcom certifikáte,
  - » ľahko "prenosný" - nie je nutné inštalovať certifikát a súvisiace kľúče na každý počítač
  - » cena - podpisový tablet je jednoduché a lacné zariadenie (otázne porovnanie s cenou čítačky a čipovej karty pre osobné použitie)
  - » jednoduchosť použitia - vidím, čo podpisujem, podpis má vizuálnu podobu. Tento podpis môže používať ktokoľvek, kto sa vie podpísať.

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- riziká použitia
  - » nemožnosť „zviazania“ podpisu s dokumentom
    - biometrický podpis (t.j. charakteristika zapísaných ťahov) existuje úplne samostatne
    - k dokumentu musí byť "prilepený" inými prostriedkami
    - u všetkých známych implementáciách sú tieto "iné prostriedky" práve asymetrická kryptografia, t.j. elektronický podpis
  - » možnosť získania "podpisového materiálu" podvodom
    - získanie dát k podpisu je pomerne jednoduché a možno ho pomerne ľahko vykonať aj bez vedomia užívateľa – zneužitie údajov pri vytvorenom podpise.
  - » obtiažnosť overenia podpisu
    - biometrický podpis v dokumente nemôže byť uvedený "len tak", v otvorenej podobe, pretože potom by bolo možné ho vyextrahovať a pridať k ľubovoľnému ďalšiemu dokumentu
    - vlastné biometrické dáta sú teda v dokumente uložené v zašifrovanej podobe a viazanej na dokument. A len vlastník tohto kľúča si môže podpis skutočne overiť porovnaním zaznamenaných biometrických dát s podpisom. Všetci ostatní musia spoliehať na vyhlásenia tohto vlastníka.

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

» **nedostatočná kontrola podpisovateľa**
- osoba sa spravidla **podpisuje na zariadení, ktoré nemá vo svojom vlastníctve a pod svojou kontrolou** - možnosť zachytenia "surových" podpisových dát
- osoba "vidí čo podpisuje„ - úplne iluzórne, pretože celý vnem je sprostredkovaný softvérom, ktorý bude typicky pod kontrolou niekoho iného ako podpisovateľa

» **nemožnosť revokácie "podpisového materiálu" v prípade kompromitácie**
- ak sú charakteristiky vôľou užívateľa vymeniteľné, znamená to minimálne zvykať si na iný podpis. Neexistujú relevantné informácie pre prípad, nakoľko je možné charakteristiky podpisu pri DBP zmeniť vôľou podpisujúcej osoby,
- ak sú nezmeniteľné, predastavuje daný stav v súčasnom režime používania vážny problém, pre riešenie ktorého je podobné implementovať podobné schémy ako pre PKI.

» **plošné použitie**
- potreba vytvorenia infraštruktúry pre vytváranie a overovanie podpisov, čo by však **výrazne znížilo dostupnosť podpisu** a kládlo ho na roveň - čo do zložitosti obstarania a pravdepodobne tiež nákladnosti - úradne overených podpisov

DITEC Data Information Technology & Expert Consulting

3. Mýty a realita

- **Elektronický podpis je drahý**
  - kvalifikovaný certifikát
    - » na trhu 3 ACA pôsobiace v konkurenčnom prostredí
    - » cena cca 20 Euro ročne, potenciál znižovania
  - HW zariadenie + čítačka
    - » v balíku s QC cca 65 Euro
    - » v budúcnosti možnosť bude možno možné využiť eID, v prípade bezkontaktného eID bude problém s cenou čítačky
  - certifikovaná aplikácia
    - » vo väčšine prípadov poskytovaná zdarma, v rámci elektronickej služby
  - **zľavy na správnych poplatkoch - 50% z poplatku, najviac 70 Euro**

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **Elektronický podpis sa aj tak nevyužíva**
  - je vytvorená ucelená infraštruktúra pre používanie ZEP
    - » široké spektrum certifkovaných HW zariadení a aplikácií
    - » vydávaných cca 32.000 QC ročne (celkovo skoro 150.000)
    - » časové pečiatky – cca 600.000 mesačne
  - aká je realita - sú implementované aplikácie a procesy reálne využívajúce ZEP
    - » Colná správa – cca 300.000 správ so ZEP mesačne, výhradne elektronický spôsob pre vybrané procesy
    - » Daňová správa – cca 400.000 el. podaní ročne
    - » Obchodný register – 40-50.000 ročne
    - » JKM – podania na DR – skoro 300.000 ročne
    - » UPVS – všeobecné podanie – viac ako 10.000 ročne
    - » ...

Mýty a fakty o elektronickom podpise

- zhodnotenie rozsahu využívania ZEP
  - komerčný sektor bez problémov – opakované aktivity, kde elektronická komunikácia je vyžadovaná legislatívou, alebo je jasným prínosom (úspory)
  - „súkromní“ používatelia – malé rozšírenie, najmä z dôvodu absencie pridanej hodnoty (neexistencia dostatočného portfólia služieb, ktoré by získanie a využívanie ZEP zdôvodnili)
    - možné riešenie je vytvorenie jednotného elektronického komunikačného prostredia s najväčšími poskytocvateľmi služieb (banky, telekomunikační a sieťové operátori, ...), ktoré vytvorí dostatočné portfólio služieb

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **Elektronický podpis je zložitý na používanie**
  - vydanie certifikátu
    - » návšteva ACA, podpora operátorov, cca 10-15 min
    - » v súčasnosti už plošné pokrytie územia SR
    - » elektronická obnova (návšteva RA nie je potrebná)
  - inštalácia prostriedkov
    - » otázka použitia na viacerých platformách – vzhľadom na certifikáciu a používanie auditovaných knižníc problematické (ale iba otázka, kto dané náklady zaplatí)
    - » niekedy problémy pri inštalácii v špecifickom prostredí
  - vlastné použitie – vytváranie ZEP
    - » aplikácia zložitosť ZEP „prenáša na seba“
    - » v praxi reálne „na dva kliky“
    - » dnes ZEP reálne využívajú „neznalí používatelia“

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **Premrštené bezpečnostné požiadavky na ZEP**
  - potrebná podrobná analýza bezpečnostných požiadaviek v kontexte požadovaných vlastností pre elektronickú reprezentáciu právneho úkonu
  - možné riešenie ZEP- alebo EP+
    - » treba stanovenie požiadaviek (podľa predbežných analýz asi nič zásadne iné ako ZEP asi nevznikne)
    - » potreba legislatívneho ukotvenia – rozdelenie úkonov na ZEP a niečo iné

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise

- **Elektronický podpis nie je potrebný a možno ho nahradiť inými mechanizmami**
  - legislatívna rovina
    - » v súčasnosti žiadna iná alternatíva pre reprezentáciu právneho úkonui nie je kodifikovaná
      - „uzavretý systém“ – pre plošné nasadenie nevhodný (potreba uzatvárania zmluvných vzťahov), nepoužiteľný pre IS VS
      - použitie elektronických schránok v „Zákone o eGov“ – otázka ako návrh v MPK dopadne, nakoľko už v súčasnosti sú k tomuto modelu vážne pripomienky
    - » „paneurópske služby“ – v strategických dokumentoch EU (Digital Agenda for Europe) sa s EP počíta
  - technická a bezpečnostná rovina
    - » aké riešenie dokáže zabezpečiť nespochybniteľnosť ?
      - v prípade možného popretia úkonu vzniká potreba dokazovania a implementované riešeniu musí k tomuto poskytnúť dostatočné a nespochybniteľné dôkazy

DITEC
Data Information Technology & Expert Consulting

Mýty a fakty o elektronickom podpise