Novela zákona o elektronickom podpise

Národný bezpečnostný úrad
Sekcia informačnej bezpečnosti a elektronického podpisu
http://www.nbusr.sk

Mgr. Zuzana Mikulášková

Novely zákona o EP

Zákon č. **215/2002 Z.z. o elektronickom podpise** a o zmene a doplnení niektorých zákonov zmenený a doplnený nasledovnými zákonmi :

- zákon č. **679/2004** Z.z., ktorým sa mení a dopĺňa zákon č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave finančných orgánov
- zákon č. **25/2006** Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov
- zákon č. **275/2006** Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov

1. novela zákona o EP

- zákonom č. 679/2004 Z.z (čl. IV)
- do vymedzení pojmov zákona o EP doplnený iba nový pojem „prenos pomocou elektronických prostriedkov“ (§ 2 písm. y)
- § 2 písm. y): „prenosom pomocou elektronických prostriedkov prenos s použitím elektronického zariadenia na spracovanie (vrátane digitálneho zhusťovania) údajov a použitie drôtového spojenia, rádiového prenosu, optických technológií alebo iných elektromagnetických prostriedkov“
- účinnosť od 1.1.2005

2. novela zákona o EP

- zákonom č. 25/2006 Z.z. (čl. II)
- na účely verejného obstarávania zavedená výnimka z obligatórneho používania zaručeného elektronického podpisu pri styku s orgánmi verejnej moci
  - § 5 ods.1 : „Ak možno v styku s verejnou mocou používať elektronický podpis, tento elektronický podpis musí byť zaručeným elektronickým podpisom.“
  - doplnený odsek 2 (§ 5 ods. 2) : „Ustanovenie odseku 1 sa nevzťahuje na použitie elektronického podpisu na účely verejného obstarávania.“
- účinnosť od 1.2.2006

3. novela zákona o EP

4 etapy:

I) Veľká novela (**MPK 04.07.2005 – LegRV 14.02.2006**)

II) **Malá novela (LegRV 20.02.2006 – NRSR 22.02.2006, ČPT 1496)**

III) **Poslanecký pozmeňovací návrh- novela prostredníctvom zákona o ISVS**

IV) **Čl. III zákona č. 275/2006 Z.z. o ISVS**

I. Veľká novela

- Pôvodný legislatívny zámer (v zmysle Plánu legislatívnych úloh vlády na rok 2005 + 2006): **úplná kompatibilita so Smernicou 1999/93/ES** Európskeho parlamentu a Rady z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy
- Zavedenie nových pojmov (pokročilý elektronický podpis, kvalifikovaná certifikačná autorita atď.)
- **oslobodenie** podaní a úkonov uskutočnených elektronicky podpísaných ZEP **od správnych poplatkov**
- obligatórne používanie e-podateľní orgánmi štátnej správy
- dobrovoľnosť akreditácie
- poskytovanie kvalifikovaných certifikačných služieb úradom pre vybrané rezorty štátnej správy
- vypustenie kontroly certifikačných autorít úradom
- **umožnenie používania EP aj ZEP pre orgány štátnej správy** (vypustenie § 5 ods. 1 zákona)
- nové znenie uznávania zahraničných certifikátov (§ 17) atď.

II. Malá novela

- vypustenie **negatívnej pôsobnosti zákona** (vypustenie nemožnosti aplikácie zákona na utajované skutočnosti)
- poskytovanie akreditovaných certifikačných služieb úradom pre vybrané rezorty štátnej správy (MV SR, MO SR, MS SR, SIS)
- obligatórne používanie e-podateľní orgánmi štátnej správy
- zavedenie pojmov ako certifikačná cesta, podpisová politika, koreňový certifikát
- nové znenie uznávania zahraničných certifikátov úplne kompatibilné so znením Smernice 1999/93/ES (§ 17)
- **umožnenie používania EP aj ZEP pre orgány štátnej správy** (zmena znenia § 5 ods. 1)

III. Pozmeňovací návrh poslanca Ľubomíra Vážneho

- „prenesenie“ malej novely do návrhu zákona o informačných systémoch verejnej správy – priama novela prostredníctvom čl. III návrhu zákona o ISVS (ČPT 1381)
- Úpravy reagujúce na problémy, ktoré vyplynuli z praktickej aplikácie zákona o EP
- Obsahoval **10 bodov**

III. Kľúčové body pozmeňovacieho návrhu:

1) Spresnenie negatívneho vymedzenia pôsobnosti zákona o EP v uzavretých systémoch
2) Vypustenie negatívneho vymedzenia pôsobnosti zákona- vypustenie nemožnosti aplikácie zákona na US
3) Nemožnosť vytvárať uzavreté systémy v ISVS
4) Doplnenie a vymedzenie pojmu elektronická podateľňa
5) Umožnenie používania EP (nielen ZEP ako dovtedy) pre orgány štátnej správy (zmena znenia § 5 ods. 1)
6) Vypustenie odseku 2 v § 5 : vypustenie výnimky z obligatórneho používania ZEP pre účely VO

III. Kľúčové body pozmeňovacieho návrhu (pokrač.):

7) **poskytovanie akreditovaných certifikačných služieb úradom** príslušníkom a zamestnancom NBÚ, MV SR, MO SR, SIS (iba pre vybrané oblasti ustanovené zákonom č. 575/2001 Z.z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy) - § 10 ods. 2 písm. l)
8) Poskytovanie takýchto služieb **nie je podnikaním**
9) CA, ktorá je akreditovaná v niektorej z krajín EÚ - **jednoduchší proces akreditácie v SR**
10) obligatórne používanie e-podateľní orgánmi štátnej správy

IV) Čl. III zákona č. 275/2006 Z.z. o ISVS

Prijaté body 1-6 z pôvodného pozmeňovacieho návrhu:

1) Spresnenie negatívneho vymedzenia pôsobnosti zákona o EP v uzavretých systémoch:

   § 1 ods. 2: „V uzavretých systémoch sa tento zákon použije, ak sa účastníci uzavretého systému nedohodnú inak.“

2) Vypustenie negatívneho vymedzenia pôsobnosti zákona- vypustenie nemožnosti aplikácie zákona na US

3) Nemožnosť vytvárať uzavreté systémy v ISVS

   V § 2 písm. j) sa na konci pripájajú slová: „uzavretým systémom nie je ISVS“

4) Doplnenie a vymedzenie pojmu elektronická podateľňa

   V § 2 písm. y) znie:

   „y) elektronickou podateľňou technické zariadenie slúžiace najmä na prijímanie, odosielanie a potvrdzovanie prijatia elektronických dokumentov, elektronických dokumentov podpísaných EP a elektronických dokumentov podpísaných ZEP“

IV) Čl. III zákona č. 275/2006 Z.z. o ISVS

Prijaté body 1-6 z pôvodného pozmeňovacieho návrhu(pokrač.):

5) Umožnenie používania EP (nielen ZEP ako dovtedy) pre orgány štátnej správy (zmena znenia § 5 ods. 1)

§ 5 ods. 1 znie: „ V styku s orgánmi verejnej moci alebo orgánmi verejnej správy sa používa EP alebo ZEP. Ak sa v styku s orgánmi verejnej moci alebo orgánmi verejnej správy používa ZEP, jeho kvalifikovaný certifikát musí byť vydaný ACA“

6) Vypustenie odseku 2 v § 5 : vypustenie výnimky z obligatórneho používania ZEP pre účely VO

Čo je potrebné k praktickému použitiu elektronického podpisu?

- k praktickému použitiu elektronického podpisu je potrebné PC pripojené do siete Internet s aplikáciami MS Explorer a MS Outlook alebo podobnými, znalosti o ich používaní a základné znalosti o elektronickom podpise
- k použitiu zaručeného elektronického podpisu, t. j. podpisu ktorý podľa zákona o elektronickom podpise môže byť použitý v administratívnom styku so štátnou správou musí byť v prvom rade zabezpečená podmienka „podpisuj to čo vidíš“
- k tomu je potrebná úradom certifikovaná aplikácia (SCVA), ktorá umožňuje podpísanie dokumentu a aj overenie podpisu a úradom certifikované bezpečné zariadenie na vyhotovovanie elektronického podpisu (SSCD)
- bezpečným zariadením môže byť napríklad certifikovaná kryptografická karta (obdoba platobnej karty) so zariadením, ktoré umožňuje komunikovať počítaču s touto kartou, tzv. čítačka kariet alebo USB token
- v takomto prípade bezpečné zariadenie pre vyhotovovanie elektronického podpisu plní aj funkciu bezpečného uchovávania tajného kľúča majiteľa

Čo je potrebné k praktickému použitiu elektronického podpisu (pokrač.)?

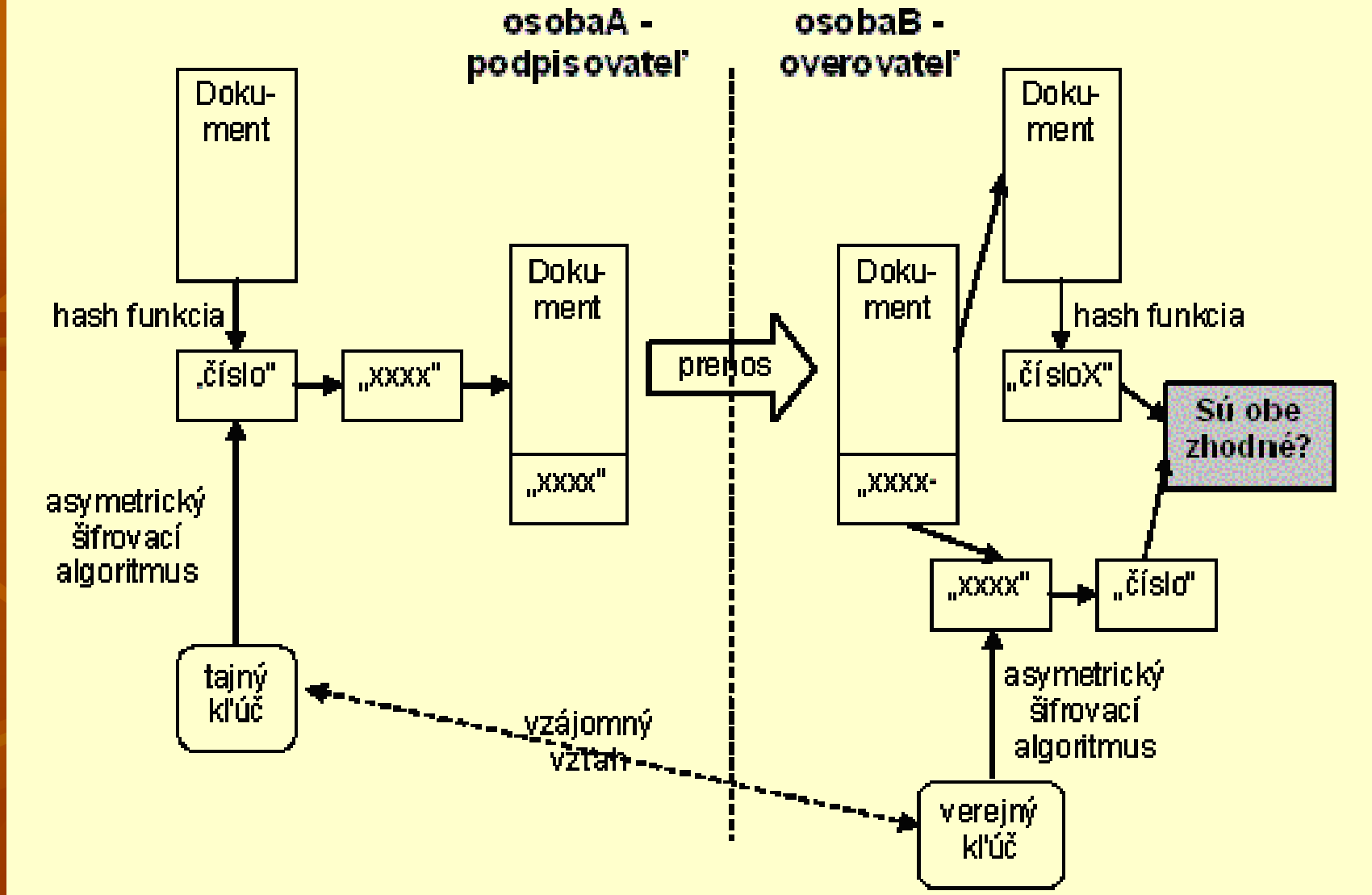
- ďalšou dôležitou podmienkou je vystavenie kvalifikovaného certifikátu konkrétnej osobe, túto úlohu by mala zabezpečovať úradom akreditovaná CA
- samotný proces elektronického podpisovania dokumentu je pre podpisovateľa obmedzený len na zasunutie kryptografickej karty do čítačky, zadanie PIN kódu a v aplikácií určenej na podpisovanie „odkliknutie“, že uvedený dokument sa má podpísať, takto upravený, podpísaný dokument je potom možné distribuovať
- na strane overovateľa prebieha overenie podobným spôsobom, nie je potrebné vkladať kryptografickú kartu a zadávať PIN kód, stačí len v príslušnej aplikácií kliknúť na voľbu overiť elektronický podpis
- bezpečné aplikácie by však aj pri overovaní ZEP mali vyžadovať vloženie tokenu (nie však zadanie PIN), pretože certifikát ACA alebo NBÚ by sa mal načítať z tohto tokenu, čiže z bezpečného úložiska, kde nie je možné jednoduchým spôsobom tieto certifikáty zameniť za falošné
- po overení sa na monitore objaví správa o úspešnom overení alebo správa o nemožnosti overenie, a ak je to možné tak aj príslušný dôvod

EP – digitálny podpis

- založený na **asymetrickom šifrovaní**
- používajú sú dva rôzne, navzájom súvisiace údaje, údaj na vytvorenie elektronického podpisu (**tzv. súkromný kľúč**) a údaj na overenie elektronického podpisu (**tzv. verejný kľúč**) – tzv. kľúčový pár
- Podpisovanie (vyhotovovanie podpisu) sa vykonáva s využitím súkromného kľúča
- Overovateľ overuje digitálny podpis pomocou verejného kľúča podpisovateľa
- na základe tohto verejného kľúča nie je schopný v reálnom čase odvodiť súkromný kľúč podpisovateľa
- umožňuje zároveň kontrolu integrity podpísaného elektronického dokumentu

Postup pri vyhotovovaní a overovaní EP

- EP má podobu krátkeho elektronického súboru (!nie zoskenovaný podpis!)
- Vznikne spracovaním podpisovaného elektronického dokumentu a súkromného kľúča v prostriedku, ktorého jediným a výlučným vlastníkom je podpisovateľ (hash dokumentu sa zašifruje tajným kľúčom podpisovateľa)
- Takto spracovaný elektronický dokument sa napokon pripojí k podpisovanému dokumentu (viď nasl. obrázok)
- Podpis môže vytvoriť len podpisovateľ, lebo len on pozná svoj súkromný kľúč
- Keďže verejný kľúč podpisovateľa je známy všetkým, každý si môže overiť pravosť podpisu



Obr. 1.: Princíp elektronického podpisu

Ďakujem za pozornosť!

Otázky, dotazy?!

info@nbusr.sk
mikulaskova@nbusr.sk