

Od praktických skúseností k návrhu zákona O ELEKTRONICKOM PODPISE

Aj keď na Slovensku ešte nie je prijatý zákon o elektronickom podpise (ďalej ZoEP), v praxi sa elektronický podpis (ďalej EP) už niekoľko rokov používa. V elektronickom bankovníctve sa dnes napríklad používajú rôzne druhy EP – statické kódy, jednorazové kódy na báze symetrických kľúčov a digitálny podpis na báze asymetrických kľúčov. Zachytiť obsah právneho úkonu a určiť osobu, ktorá právny úkon elektronickými prostriedkami urobila, dnes technicky umožňuje digitálny podpis za predpokladu vhodnej metodiky a právneho rámca. V súvislosti s návrhmi ZoEP sa v nasledujúcom príspevku zamyslíme nad praktickými aspektmi elektronického podpisu.

Elektronický podpis je kľúčovým prvkom seriózneho elektronického obchodu a ďalších elektronických služieb s prívlastkom e-. Aby takýto podpis mal právnu váhu porovnateľnú s vlastnoručným podpisom, musí v súlade s § 40 ods. 4 Občianskeho zákonníka umožňovať „zachytiť obsah právneho úkonu a určiť osobu, ktorá právny úkon elektronickými prostriedkami urobila“.

Pri elektronickej výmene informácií splneniu podobných právnych požiadaviek veľmi účinne napomáha moderná kryptografia. Na splnenie požiadavky „zachytenia obsahu právneho úkonu“ kryptografia umožňuje „overenie integrity elektronického dokumentu“, t. j. odhalenie akejkoľvek modifikácie elektronického dokumentu po jeho podpísaní. Rovnako kryptografia umožňuje overiť podpisovateľa elektronického dokumentu. Služí jej na to tzv. digitálny podpis s asymetrickou dvojicou kľúčov.

V nasledujúcej časti sa pozrieme na praktické použitie takéhoto podpisu na príklade z elektronického bankovníctva. Zameriame sa na 5 hlavných okruhov súvisiacich s digitálnym podpisom:

1. Generovanie kľúčov

Ide o generovanie dvojice kľúčov – tajného (TK – tzv. informácia na vytváranie digitálneho podpisu) a verejného (VK – tzv. informácia na overovanie digitálneho podpisu). Táto dvojica kľúčov spolu vzájomne súvisí (platnosť podpisu vytvoreného TK je možné overiť iba zodpovedajúcim VK), pričom jeden nie je možné v reálnom čase a pri súčasne dostupných počítačových kapacitách odvodiť zo znalosti druhého (platí to za predpokladu určitej dĺžky kľúča – dnes to je minimálne 768 bitov). Už sám názov tajný kľúč napovedá, že by malo ísť o informáciu, ktorá je tajomstvom jej majiteľa-podpisovateľa, aby nemohlo dôjsť k zneužitiu tejto informácie druhou osobou.

Spočiatku bol generátor kľúčov väčšinou na bankovej strane, kde na počítači banky boli príslušným pracovníkom banky generované kľúče pre jednotlivých klientov. TK na diskete, resp. čípo-

Protokol k verejnému kľúču odovzdaného klientom banky

Majiteľ účtu/účtov *)
obchodné meno/meno *) :

sídlo/adresa trvalého pobytu *) :

IČO/rodné číslo *) :

DRČ *) :

č. tel. : č. faxu :

Týmto splnomocňujem svojho zamestnanca/zamestnancov *)

Priezvisko a meno : č. OP :

Priezvisko a meno : č. OP :

pre odovzdanie vygenerovaného verejného kľúča pobočkou/expozitúrou *)

Banka :
(názov a sídlo pobočky/expozitúry *)

Klient: KLIANT
Užívateľ: klient

Opis verejného kľúča

Modulus N:

```

[5D 24 73 23 DF 52 16 C1]
[87 1F EC A3 20 C9 5E EA]
[93 48 2D 21 A3 52 31 DD]
[1C A9 2F E7 9D C7 C7 24]
[56 6D 6C F0 98 52 EB 88]
[DE 0C 19 B2 29 D6 EE 55]
[93 2D F1 A8 9D 39 63 AA]
[99 B6 82 C0 3E 21 3D C8]

```

Verejný exponent E: 11

V dňa V dňa

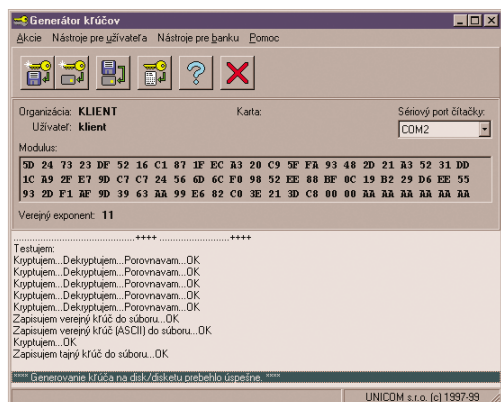
Za banku: Za klienta:

vej karte RSA, v zapečatenej obálke odovzdala banka klientovi. Zodpovedajúci verejný kľúč ostával na príslušnom serveri v banke.

Aby bolo možné vylúčiť, že kópia takto vygenerovaného TK klienta ostala k dispozícii v banke, presunulo sa generovanie kľúčov klienta z banky na stranu klienta. Klientovi na to slúži jednoduchý nástroj – generátor kľúčov – umožňujúci vygenerovať a uložiť TK na disketu, resp. číповú kartu RSA pre potreby klienta, a VK s príslušným protokolom (certifikátom) uložiť na ďalšiu disketu pre potreby banky.

2. Certifikácia verejného kľúča

Aby bolo možné priradiť VK ku konkrétnej osobe, je potrebné, aby sa majiteľ TK (tzv. podpisovateľ) prihlásil k zodpovedajúcemu VK. Robí sa to väčšinou na papierovom protokole s opisom VK. Podpisom takéhoto protokolu, obrazne povedané, majiteľ príslušného TK dáva súhlas na rozšírenie svojej autentifikácie (overenie pravosti osoby) pomocou klasického podpisu o elektronickej autentifikáciu prostredníctvom digitálneho podpisu, ktorého platnosť je overiteľná príslušným VK. Podpis druhej strany (banky, resp. nezávislej a uznávanej tretej strany – tzv. certifikačnej autority) je prejavom akceptácie a zároveň určitej garancie tohto VK. Pokiaľ neexistuje nezávislá certifikačná autorita, tento protokol s podpisom druhej strany (banky) chráni klienta pred podvrhnutím nepravého VK zo strany banky. Je zároveň jedným z dôkazových materiálov pri prípadnom súdom spore, v ktorom by sa malo dokázať, či napríklad príkaz na úhradu z účtu klienta obsahuje platný podpis klienta. V záujme zvýšenia bezpečnosti digitálneho podpisu sa odporúča pravidelná výmena kľúčov klienta (1 × za 6 mesiacov, resp. 1 × za rok), preto sa na protokole často udáva platnosť verejného kľúča, prípadne obmedzenie platnosti na určitú maximálnu sumu. Elektronicke forma takéhoto protokolu s príslušným VK sa nazýva certifikát a slúži na automatizované overovanie pravosti podpisu. Je zrejme, že do prijatia potrebných usmernení a vybudovania infraštruktúry nezávislých a uznávaných certifikačných autorít dobre posluží popri elektronickej forme certifikátu na

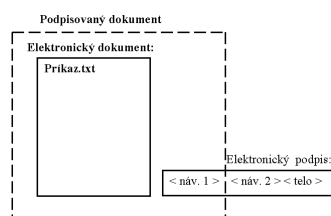


určité prechodné obdobie aj jeho papierová forma, tak ako je to dnes v elektronickom bankovníctve.

Za predpokladu, že si klient banky dáva pozor na svoj TK a ten je jeho výlučným tajomstvom, možno tvrdiť, že platobný príkaz s digitálnym podpisom, ktorého platnosť je overená príslušným VK, resp. jeho certifikátom, mohol byť podpísaný iba týmto klientom.

3. Podpisovanie dokumentu

Digitálny podpis sa v elektronickom bankovníctve používa na vytváranie podpisu k platobnému príkazu, žiadosti a podobne. Vytvára sa prostredníctvom niektorej z hash funkcií (napr. MD5, SHA-1), niektorého z asymetrických algoritmov (napr. RSA, DSA) a uchováva sa v určitom tvare. Podstatnou vlastnosťou digitálneho podpisu je schopnosť kontroly integrity podpísaného elektronického dokumentu, t. j. odhalenie zmeny v elektro-



nickom dokumente po jeho podpísaní. Ak napríklad dôjde k modifikácii platobného príkazu po jeho podpísaní, digitálny podpis k nemu stratí platnosť.

Digitálny podpis môže mať niekoľko častí, napríklad návstiev 1, návstiev 2, vlastné telo podpisu. V návsteví 1 sa nachádzajú dôležité informácie (čas podpisu, stručná informácia podpisovateľa, prípadne ďalšie),

pri ktorých podobne ako v samotnom podpísanom elektronickom dokumente je potrebné mať možnosť overiť ich integritu. Pri podpísaní sa táto časť podpisu pripája za podpísaný elektronický dokument a podpis sa vytvára k obom častiam ako celku – elektronickému dokumentu + návsteviu 1. V návsteví 2 sa nachádzajú informácie o asymetrickom algoritme, hash funkcii, formáte podpisu, kľúč ID, názve podpísaného súboru, prípadne ďalšie, ktoré vypovedajú o tom, ako bol podpis vytvorený. Samotný digitálny podpis sa nachádza v tele podpisu.

```
<TIMELABEL>17.08.2001 15:45:34</TIMELABEL> <INFO></INFO>
<SIGNATURE = "1.00"><ALGSIGN>sha1RSA</ALGSIGN> <FORMATSIGN>HEXA<
/FORMATSIGN> <FILE>PRIKAZ.TXT</FILE> <IDKEY>KLIENT/klient</IDKEY>
<SIGN>D2CE1D64F9B2CB21B8E54E5E3E1160D4B6DB8D170327ADB181FFAA185838B
0A28654B91C23D50C3776D1FC8E209603E540016BD78A60D935829ECC1A5EA29024<
/SIGN>
```

4. Potvrdzovanie dokumentu

Pre klienta banky je veľmi dôležité potvrdenie vydané bankou k ním doručenému platobnému príkazu. Toto potvrdenie platobného príkazu by ho malo chrániť, resp. slúžiť ako dôkazový materiál v prípade sporu s bankou, resp. sporu s dodávateľom či daňovým úradom v prípade hrozacej penalizácie. Pri klasickom platobnom príkaze toto potvrdenie predstavuje pečiatka banky s vyznačením dátumu a času podania príkazu a podpis konkrétnej pracovníčky v podateľni banky na kópii platobného príkazu. V prípade elektronického bankovníctva klienta chráni elektronická potvrdenka, čo je vlastne digitálny podpis k doručenému platobnému príkazu s vyznačením dátumu a času prijmu príkazu

```
<TIMELABEL>17.08.2001 16:03:15</TIMELABEL> <INFO>Informacia o stave:
Banka potvrdzuje realizáciu príkazu</INFO>
<SIGNATURE = „1.00“><ALGSIGN>sha1RSA</ALGSIGN> <FORMATSIGN>HEXA
</FORMATSIGN> <FILE>PRIKAZ.TXT</FILE> <IDKEY>BANKA/banka</IDKEY>
<SIGN>9842A636E869554AFC1F263C39CB3387EB89CA636B420D7A1655475EFOA089
DE7EA8B3102027C58D5841B804E5227F8BADD4E1652C95AEA2DCA4957D0E093E9A<
/SIGN>
```

a stručnej informácie (napríklad o realizácii platobného príkazu). Vystavená je príslušným serverom elektronického bankovníctva, tzv. elektronickou podateľňou, po prijíme platobného príkazu.

Elektronická podateľňa na rozdiel od klasickej podateľne dokáže po prijíme príkazu, žiadosti a pod. urobiť kontrolu platnosti podpisu a niektoré ďalšie základné kontroly. Dokáže súčasne poskytnúť informáciu o stave doručeného príkazu, žiadosti a pod. na základe výsledku tejto kontroly. Pretože čas doručenia a stručná informácia banky sú dôležité údaje v prípade sporu, nachádzajú sa opäť v návsteví 1 digitálneho podpisu. Na rozdiel od klasickej podateľne v tzv. elektronickej podateľni tento podpis – elektronickú potvrdenku – nevystavuje konkrétna osoba, ale príslušný server banky. V tomto prípade z praktického hľadiska nejde o podpis konkrétneho pracovníka, ale o podpis banky či jej príslušného servera.

5. Kontrola platnosti podpisu

Na základe VK, resp. zodpovedajúcich certifikátov jednotlivých klientov elektronického bankovníctva príslušný server automaticky kontroluje platnosť podpisu k príslušnému doručenému príkazu, žiadosti klienta a podobne. Do ďalšieho spracovania sa dostávajú iba doklady, ktoré majú platný podpis, t. j. nedošlo k ich modifikácii a podpísala ich oprávnená osoba daného klienta. Klient má rovnako možnosť overiť platnosť elektronickej potvrdenky, ktorú mu banka vrátila k jeho platobnému príkazu.

Okrem digitálneho podpisu na báze asymetrických kľúčov sa v elektronickom bankovníctve používajú ďalšie dva druhy „elektronického podpisu“:

1. statické kódy (PIN, heslo, kontrolné otázky, súbor hesiel na tzv. Grid karte),
2. dynamické kódy na báze symetrických kľúčov (OTP – One Time Password, MIC – Message Integrity Code). (Bližšie pozri R. Rexa a kol.: Bezpečnosť elektronického bankovníctva v praxi. PCR č. 6/2001.)

Bežný používateľ EP, ktorý nie je špecialistom v kryptografii, sa dnes pravdepodobne ešte nevie dostatočne zorientovať, ako ním používaný EP umožňuje „zachytiť obsah právneho úkonu a určiť osobu, ktorá právny úkon urobila“. Rovnako s tým bude mať problémy aj sudca, ktorý bude musieť rozhodnúť o prípadnom spore medzi dvoma stranami. Určiť jednoduché a pritom jasné pravidlá pri používaní EP má za úlohu zákon o elektronickom podpise (ďalej ZoEP).

Smernica 1999/93/EC Európskeho parlamentu

Základom pre vytvorenie právneho rámca v krajinách Európskej únie je smernica 1999/93/EC Európskeho parlamentu (http://europa.eu.int/eur-lex/en/com/dat/1999/en_599PC0626.html). Jej cieľom je napomôcť využívanie EP v krajinách EU a prispieť k ich vzájomnému uznávaniu. Smernica uvádza širšie definície 13 základných pojmov: elektronický podpis, zaručený elektronický podpis (ďalej ZEP), podpisovateľ, dáta na vytváranie podpisu, prostriedok na vytváranie podpisu, bezpečný prostriedok na vytváranie podpisu, dáta na overovanie podpisu, prostriedok na overovanie podpisu, certifikát, kvalifikovaný certifikát, poskytovateľ certifikačných služieb, produkt na elektronický podpis, akreditácia.

EP podľa smernice „predstavuje dáta v elektronickej forme, ktoré sú pripojené alebo logicky súvisia s inými elektronickejšími dátami a ktoré slúžia ako metóda autentifikácie“ (overenia pravosti). Ide o veľmi širokú definíciu, ktorej vyhovuje celá škála EP. Cieľom smernice však nie je regulovanie obyčajných EP, to má byť úlohou ZoEP príslušnej členskej krajiny EU. S ohľadom na snahu o medzinárodnú kompatibilitu sa smernica podrobnejšie zaoberá zaručeným elektronickým podpisom a s ním súvisiacimi ďalšími pojmami, ako sú kvalifikovaný certifikát, bezpečný prostriedok na vytváranie podpisu a poskytovateľ certifikačných služieb vydávajúci kvalifikované certifikáty.

ZEP v porovnaní s „obyčajným“ elektronickým podpisom na príklad musí navyše

- byť **jednoznačne** spojený s podpisovateľom,
- umožňovať **identifikáciu** podpisovateľa,
- jeho vytváranie má mať podpisovateľ **sám** pod svojou kontrolou,
- byť spojený s dátami, ku ktorým patrí, takým spôsobom, že bude **detectovateľná následná zmena** týchto dát.

ZEP má mať rovnakú právnu účinnosť ako vlastnoručný podpis a má byť prípustný ako dôkaz pri súdnom konaní. Neznamená to však, že zákonná účinnosť a prípustnosť môže byť upretá „obyčajnému“ elektronickému podpisu, prípadne inému podobnému podpisu dohodnutému v občianskoprávných vzťahoch.

Slovenský zákon o elektronickom podpise

Smernica EU nerieši všetky detaily EP, to je vecou ZoEP príslušnej členskej krajiny EU. Nemecko, Rakúsko, Česká republika už majú schválený zákon o elektronickom podpise. Na Slovensku sa schvaľovanie tohto zákona iba očakáva. V parlamente sú pripravené dva návrhy zákona, čo je spolu so skúsenosťami získanými pri zavádzaní a uplatňovaní zákona o elektronickom podpise v niektorých krajinách EU dobrým predpokladom na dopracovanie kvalitnej slovenskej právnej normy. [Návrhy zákonov sú na adrese: <http://www.nrsr.sk> Zákony-návrhy: vládny – ČT 1027 (ďalej VN), poslanecký – ČT 984 (ďalej PN), ich obhajoba, resp. recenzia je na adresách <http://www.saec.sk>, <http://www.informatika.sk>].

Je zrejmé, že k rýchlemu zavádzaniu elektronického podpisu neprispeje ani príliš tvrdý, ani príliš mäkký ZoEP. V prvom prípade pre nereálnosť splniť požiadavky zákona v bežnej praxi, v druhom prípade pre nedôveru k slabému elektronickému podpisu. Prijatím zákona, ktorý sa odvoláva na nepripravené právne predpisy, sa legislatívny proces nekončí, ale iba začína. Náznový je v tomto smere príklad z Českej republiky, kde sa už viac ako rok pracuje na vykonávacích predpisoch, ktoré by umožnili začať používať EP podľa schváleného ZoEP. Vkladať do zákona technické parametre, ktoré sa rýchlo menia, môže mať za následok nutnosť neustálej novelizácie zákona. Konečná verzia zákona musí byť preto citlivým kompromisom medzi uvedenými extrémami.

Od praxe k návrhu zákona

V nasledujúcej časti sa zamyslíme nad niektorými „úzkymi“ miestami predložených návrhov ZoEP:

1. Platnosť EP, ZEP a čas jeho vytvorenia

Časový údaj, kedy bol elektronický podpis vytvorený, má dôležitý význam. Podľa VN § 4 ods. 1, resp. podľa PN § 5 ods. 3b platnosť EP, resp. ZEP závisí od času ich vytvorenia a platnosti príslušného certifikátu. V definícii elektronického podpisu sa však v návrhoch ZoEP (VN § 2 ods. b, c, PN § 5) nehovorí o čase, kedy bol podpis vytvorený. Vzniká tak nežiaduca legislatívna diera. Nejde o neriešiteľný problém – jedno z riešení ponúka uvedený príklad z elektronického bankovníctva.

2. Overovanie podpisu notárom

V súčasnom klasickom „papierovom svete“ existujú právne úkony (spísanie závetu, prevod nehnuteľnosti a pod.), ktoré sa vykonávajú u notára, resp. za prítomnosti notára, ktorý okrem iného overuje slobodnosť vôle podpisovateľa podpísať takýto právny úkon. V podobných prípadoch by ZEP v žiadnom prípade nemal v „elektronickom svete“ nahradiť prítomnosť notára (VN dôvodová správa k § 3).

3. Elektronická potvrdenka – časová pečiatka

Vytvorenie a podpísanie elektronického dokumentu predstavuje prvú polovicu jeho osudu. Nemenej dôležitú úlohu má aj prijatie dokumentu adresátom, resp. jemu zodpovedajúcou elektronickou podateľňou. Aj v tomto prípade hrá čas nezanedbateľnú úlohu (včasné podanie daňového hlásenia, príkazu na úhradu dane a podobne). Právne relevantnú hodnotu má elektronická potvrdenka, ktorá predstavuje elektronický podpis elektronickej

podateľne k prijatému dokumentu, doplnenému o informáciu o čase prijmu dokumentu, prípadne o jeho stave.

Elektronická potvrdenka, ktorá napríklad dnes trápi aj tvorcov českého ZoEP (V. Smejkal a kol.: „Právo informačních a telekomunikačních systémů“, C. H. Beck, Praha 2001, s. 100.), by mala nájsť zodpovedajúce miesto v slovenskom ZoEP. V prípade, že sa rozšíri definícia EP o časový údaj a stručnú informáciu podpisovateľa, elektronická potvrdenka bude iba EP prijímateľa, resp. overovateľa k prijatému, resp. overovanému elektronickému dokumentu.

Časová pečiatka (časová značka)

Je zrejmé, že bežná elektronická podateľňa nebude vybavená drahým ciachovaným časovým zariadením, ktoré bude spĺňať rôzne ďalšie bezpečnostné požiadavky, a časový údaj elektronickej podateľne na elektronickej potvrdenke nemusí byť dostatočne presný. Preto je na mieste služba nezávislej časovej pečiatky (VN § 2 ods. m, § 6, PN § 3 ods. 23, § 11). Ide v podstate opäť o elektronickú potvrdenku, t. j. elektronický podpis tejto nezávislej tretej strany s garanciou presného údajja o čase.

Je zrejmé, že v bežnej praxi sa takáto služba nezávislej tretej strany bude využívať iba v sporných prípadoch, ak elektronická podateľňa poskytne nesprávny údaj o čase. V klasickom „papierovom svete“ podobná služba, ktorá by potvrdila, že hodinky pracovníčky v podateľni sú nepresné, a k určitému papierovému dokumentu by priradila presný, právne relevantný údaj o čase, dodnes neexistuje. Časová pečiatka nezávislej tretej strany však bez elektronickej potvrdenky druhej strany nemá zmysel.

4. Forma certifikátu

Iba elektronická forma certifikátu (VN § 2 ods. g, PN § 8) bude zbytočne brzdiť využívanie EP v čase od prijatia ZoEP do prijatia vykonávacích predpisov a vybudovania infraštruktúry certifikačných autorít.

5. Žiadosť o vydanie certifikátu

Pri rozširovaní autentifikácie pomocou klasického podpisu o elektronickú autentifikáciu prostredníctvom elektronického podpisu by mala byť podchytená vôľa danej osoby k takémuto rozšíreniu autentifikácie – napr. jej písomnou žiadosťou, kde je uvedený opis VK a klasický podpis tejto osoby.

6. Podpisovateľ

Zúženie podpisovateľa na fyzickú osobu bude v elektronickom svete s rôznymi automatickými elektronickými podateľňami znamenáť veľa praktických problémov.

7. Uzatvorený systém

Dnešná prax z elektronického bankovníctva dáva dostatok príkladov, ako poskytovateľ elektronickej služby poskytuje takéto služby na nízkej bezpečnostnej úrovni, so zmluvnými podmienkami, ktoré presúvajú zodpovednosť za zneužitie tejto nízkej bezpečnosti na používateľa bez toho, aby bol používateľ na toto riziko upozornený.

Vsunutie „legislatívnej vaty“ v podobe uzavretého systému (§ 1 ods. 3 VN i PN), na ktorý sa zákon o elektronickom podpise nevzťahuje, zbytočne „zahmlieva“ takýto systém v očiach znalých používateľov a zlegalizuje uvedený prístup zo strany poskytovateľa slabo zabezpečenej elektronickej služby.

Občiansky zákonník dáva dostatočný priestor na dohodu zmluvných strán o forme a podpise určitého právneho úkonu. Definovanie uzatvoreného systému z uvedených dôvodov nepovažuje za potrebné ani aktualizovaná smernica EU.

Existujú ešte ďalšie úzke miesta predložených návrhov ZoEP (<http://www.saec.sk>, <http://www.informatika.sk>), ktoré je tiež potrebné zvážiť pri príprave konečného znenia ZoEP. Na kvalitný a funkčný ZoEP na Slovensku už dlhší čas netrpezlivo čaká široká obec priaznivcov, používateľov, návrhárov a tvorcov rôznych elektronických služieb.