Úvod do klasických a moderních metod šifrování ALG082
Elektronický podpis
Ver 1.0

Pavel Vondruška
pavel.vondruska@ct.cz, pavel.vondruska@crypto-world.info
http://crypto-world.info

Cíl přednášky:

- seznámit posluchače s problematikou elektronického podpisu a souvisejícími pojmy (typy elektronických podpisů, certifikát, poskytovatel certifikačních služeb a jejich typy, požadavky na jednotlivé subjekty) a základními souvisejícími právními předpisy a standardy v ČR a EU
- přednáška má za cíl dále poukázat na šíři dané problematiky, která přesahuje otázky kryptologie nebo informační bezpečnosti (legislativa, aktuální stav, vazba na standardy, vývoj, problémy)

Obsah :

I. Cvičení (co nesprávného jsme se již naučili)

Na základě znalostí, které již máte si předvedeme, jak lze za jistých okolností získat podpis nějaké osoby pod (námi připravený) text, aniž by daná osoba vědomě tento konkrétní text podepsala.

Pro jednoduchost a srozumitelnost výkladu si vše předvedeme na následujícím jednoduchém podpisovém schématu.

I.1 Podpisové schéma MFF UK

V podstatě se jedná o klasické podpisové schéma, založená na RSA, kde je však vynechána hashovací funkce a text není formátován podle PKCS #1.5, ale podle námi zadaných pravidel, která označíme jako MFFUK #1.0.

I.1.1 – použitý asymetrický algoritmus

Vyjdeme z klasického RSA. Zvolíme prvočísla p a q a vypočteme

$N = p*q$

$\Phi(N) = (p-1)*(q-1)$

Dále zvolíme náhodné číslo e, kde

$1 < e < \Phi(N)$, takové, že e a $\Phi(N)$ jsou nesoudělná.

Vypočteme číslo d takové, že

$1 < d < \Phi(N)$ a

$e*d \equiv 1 \mod \Phi(N)$

Dvojici (N,d) nazveme soukromý klíč (resp. data na vytváření podpisu) a (N,e) veřejný klíč (resp. data na ověření podpisu).

I.1.2 Formátování zprávy (MFFUK#1.0)

Zprávu M překódujeme nejprve do číselného tvaru. K tomu použijeme některou vhodnou převodovou tabulku. Např. tuto tabulku:

	0	1	2	3	4	5	6	7	8	9
6	**0**	**Mezera**	**2**	**3**	**4**	**A**	**B**	**C**	**D**	**E**
7	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
8	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**
9	**Z**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**

Zprávu M pak zformátujeme do posloupnosti čísel pevné délky (délka bude rovna délce modulu N). K tomu použijeme vlastní formátování, která pracovně nazveme MFFUK#1.0:

Formátování MFFUK#1.0 :

1) Má-li modul délku k, budeme zprávu v dekadickém tvaru dělit na skupiny délky k-1.
2) Všechny skupiny musí mít délku k-1, nemá-li poslední skupina tuto délku, doplníme ji zprava příslušným počtem nul.
3) Skupiny nyní doplníme zleva jednou nulou. Délka každé skupiny je tedy rovna k.
4) Výsledek po podpisové transformaci má délku rovnou maximálně k, nemá-li ji doplníme výsledek zleva nulami.

Získaný výsledek po formátování M označme $M= m_1\ m_2\ m_3\ \ldots..$

I.1.3 Podpis a ověření zprávy M

Podpisem zprávy M pak nazveme řetězec
$P = C_1\ C_2\ C_3$ ..... , kde
$C_1 \equiv m_1^d \bmod N$, $C_2 \equiv m_2^d \bmod N$, $C_3 \equiv m_3^d \bmod N$ ..... $C_i \equiv m_i^d \bmod N$

Ověření podpisu zprávy M se pak provede tak, že vypočteme pomocí dat na ověření podpisu následující výrazy
$V_1 \equiv C_1^e \bmod N$, $V_2 \equiv C_2^e \bmod N$, $V_3 \equiv C_3^e \bmod N$ .... $V_i \equiv C_i^e \bmod N$

Pokud $V_i = m_i$ pro všechna i, řekneme, že ověření podpisu bylo úspěšně provedeno.

Pokud podepisující osoba dokáže udržet svá data na podepisování v tajnosti (a čísla p a q byla dostatečně velká), pak je výpočetně složité ze znalosti podpisu zprávy a dat na ověření podpisu vypočítat soukromý – podepisovací klíč.

I.2 Zneužití

Ukážeme, jak získat podpis majitele soukromého klíče (N,d) pod zprávu M, aniž by to dotyčný majitel věděl.

Celá myšlenka je založena na tom, že RSA je multiplikativní vzhledem k násobení ($\forall a,b \in Z , k \in N : (ab)^k \equiv a^k b^k \bmod N$).

Mějme zprávu M, ke které chceme získat podpis nějaké osoby (Boba), tj. hodnotu $M^d \bmod N$. Bobovi předložíme místo vlastní hodnoty M, kterou by Bob mohl odmítnout podepsat, (zdánlivě) náhodnou hodnotu X. Tuto hodnotu X však předem pečlivě připravíme a to jako $M\ c^e \bmod N$. Zde c je náhodně zvolená veličina, (N,e) veřejný klíč Boba, M zpráva. Pokud Bob takovýto zdánlivě „nesmyslný“ text podepíše (např. v rámci autentizace) a my se k výsledku dostaneme (např. v rámci autentizace), pak jsme schopni poměrně jednoduše vypočítat podpis Boba pro zprávu M.

I.2.1 Příklad - část 1 - klíče

Vše si ukážeme na konkrétním příkladě:
Nejprve vytvoříme nějaký Bobův soukromý a veřejný klíč.

Zvolíme prvočísla: p=47, q=71,
Spočteme modul : $N = p*q = 47*71 = 3337$
a dále: $\Phi(N) = (p-1)*(q-1) = 46*70 = 3220$
Zvolíme veřejný exponent e (nesmí mít společné dělitele s 3220) , volíme např. 79
Spočteme soukromý exponent d:

d …… $79*d \equiv 1 \bmod 3220$
$d \equiv 79^{-1} \bmod 3220$
d = 1019 (k výpočtu použijeme Eukleidův algoritmus)

Získali jsme:

e …….. veřejný klíč (3337, 79) ,
d …..…... soukromý klíč (3337, 1019)

I.2.2 Příklad – část 2 - text

Předpokládejme, že chceme získat Bobův podpis zprávy M=DLUH JE 10 USD
Nejprve si převedeme text zprávy M pomocí kódové tabulky do číselné posloupnosti .

M= D L U H J E 1 0 U S D
M= 68 76 85 72 61 74 69 61 91 60 61 85 83 68

M dále zformátujeme podle pravidla MFFUK#1.0 na bloky m_1 m_2 m_3 …..
M = m_1 m_2 m_3 ….. = 0687 0685 0726 0174 0696 0191 0606 0185 0836 0800

Předpokládejme, že Bob má k dispozici program / prohlížeč, který by mu tuto zprávu zobrazil jako : DLUH JE 10 USD

Kdyby Bob podepsal pomocí svého soukromého klíče d tuto přímo tuto zprávu M (tj. spočte $M^d \bmod N$, pro N=3337, d=1019) dostaneme (viz pomocný program RSAM):
1592 0585 1494 3172 644 3080 0647 1855 0707 1740 (*).

Naším cílem je tedy získat tuto posloupnost jiným způsobem, tedy bez toho, aby Bob podepsala přímo zformátovanou zprávu M.

K tomuto účelu si připravíme jinou – pomocnou zprávu.

I.2.3 Příklad – část 3 – pomocný text

Zvolíme nějaké libovolné číslo c, např. 105 a dále spočteme číslo $x \equiv c^e \bmod N$.
Pro konkrétní hodnoty Bobova veřejného klíče dostaneme $x \equiv 105^{79} \bmod 3337 \equiv 193$.
Dále připravíme k podpisu (zdánlivě) náhodnou „Bobovi nic neříkající“ hodnotu M c^e mod N.

Pro naše konkrétní hodnoty spočteme (např. využitím standardní kalkulačky ve Windows):
M = m_1 m_2 m_3 ….. = 687 685 726 174 696 191 606 185 836 800
M c^e mod N = m_1 c^e mod N m_2 c^e mod N m_3 c^e mod N ….. =
687*193 mod 3337 685*193 mod 3337 726*193 mod 3337 …..

M	0687	0685	0726	0174	696	0191	0606	0185	0836	800
M c^e mod N	2448	2062	3301	0212	848	0156	0163	2335	1172	898

Bob by při prohlížení tohoto textu svým prohlížečem viděl text, který zdánlivě nemá žádný smysl.

I.2.4 Příklad – část 4 – útok

Vraťme se k našemu příkladu. Pomocný text, který jsme si připravili, je tento:
M c^e mod N 2448 2062 3301 0212 848 0156 0163 2335 1172 898
Takto připravený text předložíme Bobovi k podpisu.

a) Bud v rámci autentizace, kde místo náhodného řetězce pošleme tento text
b) Předložíme mu je k podpisu přímo (např. v rámci výuky – jak se elektronicky podepisovat…). Bob vidí nesmyslný obsah a text proto klidně podepíše. Bob tedy spočte $(M*c^e)^d \bmod N$ a dostane (viz program RSAM):

   0310 1359 0031 2697 880 3048 1195 1229 0821 2502

Podívejme se, co po podpisu připraveného textu dostaneme (řada kroků je vynechána nebo jen naznačena)
$(M\ c^e \bmod N)^d \bmod N \equiv M^d * c^{ed} \bmod N \equiv M^d * c \bmod N$ (využito $e*d \equiv 1 \bmod \Phi(N)$)
Výsledek lze zapsat jako $M^d * c \bmod N$.

Dále je zřejmé, že ze znalosti hodnoty $M^d * c \bmod N$ a hodnoty c lze již snadno vypočítat podpis zprávy M tj. hodnotu $M^d \bmod N$.

K tomu totiž stačí postupně řešit následující modulární rovnice:
$0310 \equiv 105 * M^d \bmod 3337$
$1359 \equiv 105 * M^d \bmod 3337$
$0031 \equiv 105 * M^d \bmod 3337$
$2697 \equiv 105 * M^d \bmod 3337$
....
$2502 \equiv 105 * M^d \bmod 3337$

(Řešení těchto rovnic lze poměrně snadno realizovat i pro velká čísla.)

```
Procedure Equation;
Begin
writeln('Reseni modularni rovnice A=C*X mod N pro ruzna A');
        j:=0; M:=1;
        repeat
                inc(j);
                M1:=C*j-A;
                if M1>0 then
                begin
                M2:=((c*j-A) div N)*N;
                M:=M1-M2;
                end;
        until M=0;
        writeln('A=C*X mod N, X=',j);
end;
```

Vyřešením (viz program Equation) dostaneme následující hodnoty. Označíme je jako posloupnost (**).
1592 0585 1494 3172 644 3080 0647 1855 0707 1740

Posloupnost (**) je Bobův podpis zprávy M = DLUH JE 10 USD
(viz. posloupnost * z úvodu přednášky).

I.3 Závěr

Aby v praxi takovéto problémy nenastávaly a mohly jsme jim předcházet – potřebujeme upravit použití toho, čemu říkáme podpisové schéma (nebo digitální podpis). Zatím je to jen algoritmus. Dané postupy nemají žádnou právní váhu. Chceme-li takovéto postupy v digitálním světě používat - potřebujeme standardy (kvůli kompatibilitě), nezávislé hodnocení bezpečnosti vybraných postupů (kvůli bezpečnosti), potřebujeme upravit chování jednotlivých subjektů (kvůli právní akceptaci) – **POTŘEBUJEME ZÁKON O ELEKTRONICKÉM PODPISU.**

II. Elektronický podpis („podle zákona“)

II.1 Základní pojmy zákona o elektronickém podpisu č. 227/2000 Sb.

Řada dokumentů v posledních letech je vytvářena na počítači a je v této elektronické podobě dále zpracovávána, rozesílána a archivována. Také je řada dokumentů převáděna z klasické písemné podoby do podoby digitální a to buď z důvodu jednodušší následné manipulace, výhod automatického zpracování nebo z důvodu levnějších nákladů s rozesíláním, případně nižšími náklady na archivování. Dokumenty, které byly vytvořeny v digitálním světě, mají často význam listin, které v klasickém světě bývají podepsány (smlouvy, nabídky, dopisy…). Podepsané dokumenty, které byly do tohoto digitálního světa převedeny z původně listinných dokumentů, o tento klasický vlastnoruční podpis při převodu přijdou. Přitom elektronických dokumentů stále více přibývá a uživatelé si uvědomují výhodnost pohybu a zpracování materiálů pouze v elektronické podobě. Je tedy vhodné zavést vedle klasického vlastnoručního podpisu nový právně akceptovatelný způsob podpisování, který by mohl být použitelný při zpracování elektronických dokumentů. Začala se tak zcela logicky hledat metoda, která umožní v elektronickém světě provést úkon, který bychom mohli nazvat elektronickým podpisem.

U dokumentů podepisovaných elektronicky je potřeba zajistit podobné vlastnosti, které zajišťuje podpis na klasickém dokumentu. Především chceme, aby již podepsaný dokument nemohl být následně změněn. Této vlastnosti se říká integrita nebo chcete-li českým slovem ***neporušenost.*** Další důležitou vlastností je možnost identifikace, tedy možnost určit, kdo se vlastně elektronicky podepsal. Zde se vyžaduje existence těsné vazby mezi elektronickým podpisem a osobou, která se podepsala, a to tak silné vazby, aby zajistila v případě nutnosti ***identifikaci*** podepsané osoby. V elektronickém světě je také nutné zajistit, aby osoba, která se podepsala, nemohla později popřít, že tento úkon vykonala. Této vlastnosti se říká ***nepopiratelnost.*** Poslední důležitou vlastností je zajistit akceptaci takovéhoto podpisu v právním řádě a zajistit neodmítnutí elektronického podpisu v případě právního sporu, tedy zavést ***právní akceptovatelnost*** elektronického podpisu.

Na elektronický podpis lze klást samozřejmě i další požadavky, např. požadavek na utajení obsahu dokumentu před nepovolanou osobou nebo na prokázání existence dokumentu (nebo podepsaného dokumentu) v daném čase. Tyto požadavky však nepatří mezi vlastnosti vlastnoručního podpisu a tedy se nestaly ani požadavky na definici elektronického podpisu. V elektronickém světě je však možné tyto požadavky v případě potřeby zajistit a to pomocí dalších dodatečných služeb. V prvním případě pomocí šifrování, v druhém případě pomocí tzv. časových razítek.

Je zřejmé, že takovéto požadavky nemůže splnit „přidělení“ nějakého řetězce znaků dané osobě – tedy pouze jakási bezpečná evidence něčeho, co by pak bylo nazýváno a používáno jako elektronický podpis dané osoby. Musí být použita bezpečná metoda, která dokáže spojit dokument a data na vytváření podpisu, která mohou zůstat výhradním tajemstvím podepisující se osoby, a dále je potřeba zajistit důvěryhodnou distribuci dat na ověření takovéhoto elektronického podpisu.

II.2 Typy elektronických podpisů, certifikátů a poskytovatelů

Výše uvedené vlastnosti splňuje teprve tzv. zaručený elektronický podpis. Než si jej definujeme, podívejme se nejprve na obecnou definici elektronického podpisu, která je uvedena v našem zákoně o elektronickém podpisu v §2 písmeno a).

Elektronickým podpisem se rozumí (pro účely tohoto zákona) údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.

Takovýto „podpis“ nemá pro příjemce příliš velkou vypovídací hodnotu. Důvěra v takto vytvořený podpis by měla být osobou spoléhající se na podpis zcela minimální. Slouží spíše pouze pro informaci příjemce. Příkladem může být „podpis“ vložený pod klasický e-mail, ale i např. jméno autora uvedené v záhlaví článku, který je v elektronické podobě distribuován (dokument v MS Word, obsah www stránky apod.).

Vlastnosti, které jsme si vytyčili jako požadavek na námi hledaný vhodný typ elektronického podpisu, zajišťuje teprve podpis definovaný ve stejném zákoně v §2, písmeno b). Tento podpis se nazývá zaručený elektronický podpis.

Zaručeným elektronickým podpisem je elektronický podpis, který splňuje následující požadavky:

1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Pro úplnost dodám, že v důležitém dokumentu evropského společenství - Směrnici 1999/93ES o zásadách Společenství pro elektronické podpisy je tento typ podpisu definován stejným způsobem. V tomto ohledu je tedy náš zákon zcela s touto Směrnicí kompatibilní. Ve Směrnici a dalších dokumentech EU je tento typ podpisu nazýván „advanced electronic signature“.

Tento podpis má pro příjemce vysokou vypovídací hodnotu. Důvěra v takto vytvořený podpis je vysoká. Slouží pro styk příjemce a odesílatele, kteří se předem na takovéto komunikaci dohodnou. Příjemce musí od podepisující se osoby získat důvěryhodným způsobem jeho data pro ověření elektronického podpisu. Neslouží tedy k „anonymnímu“ styku (nákup služeb na Internetu, vstup do předplaceného prostoru atd.). Příkladem komunikace za použití zaručeného podpisu může být např. některý z dohodnutých protokolů pro komunikaci klient – banka , obchodník – zákazník. Patří sem i využívání celosvětově známého programu PGP (pokud se nepoužívají certifikáty k předání dat na ověření podpisu).
Z legislativně-právního hlediska se k uznání této komunikace využívá uzavření smlouvy podle obchodního nebo občanského zákoníku.

Dále rozšíříme pojem zaručeného elektronického podpisu o to, zda se k přenosu dat na ověření využívá certifikát resp. kvalifikovaný certifikát. V takovém případě říkáme, že je podpis založen na certifikátu resp. kvalifikovaném certifikátu.

Začněme opět definicemi. K použití tohoto podpisu se zavádí pojmy certifikát, kvalifikovaný certifikát a pojem poskytovatele certifikačních služeb. Poskytovatelé certifikačních služeb se dále dělí na poskytovatele, kteří vydávají certifikáty, na poskytovatele, kteří vydávají kvalifikované certifikáty a na akreditované poskytovatele certifikačních služeb.
Definice jednotlivých typů certifikátů jsou uvedeny v zákoně o elektronickém podpisu §2, písm. g) a h).

Certifikátem se rozumí (pro účel tohoto zákona) datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost.
Kvalifikovaným certifikátem se rozumí (pro účel tohoto zákona) certifikát, který má náležitosti stanovené tímto zákonem (§12) a byl vydán poskytovatelem certifikačních služeb,

splňujícím podmínky, stanovené tímto zákonem pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty (§6).

Definice jednotlivých poskytovatelů certifikačních služeb jsou uvedeny v zákoně o elektronickém podpisu §2, písm. e) a f).

Poskytovatelem certifikačních služeb je subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy.

Akreditovaným poskytovatelem certifikačních služeb je poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona.

Požadavky a povinnosti poskytovatele certifikačních služeb, který vydává kvalifikované certifikáty, jsou obsaženy v §6 zákona o elektronickém podpisu a dále jsou upřesněny v prováděcí vyhlášce č.366/2001 Sb.

Každý poskytovatel certifikačních služeb může požádat MI ČR o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. Podmínky udělení akreditace pro poskytování certifikačních služeb jsou uvedeny v §10 zákona o elektronickém podpisu. Ve Směrnici 1999/93ES se požaduje, aby se jednalo o akt dobrovolný. Akreditovaný poskytovatel certifikačních služeb by měl být pak společností chápán jako důvěryhodný poskytovatel těchto služeb

II.3 Zaručený elektronický podpis založený na kvalifikovaném certifikátu a elektronická značka

Tento typ podpisu je základním typem elektronického podpisu, kterým se zákon o elektronickém podpisu zabývá. Takovýto podpis má pro příjemce vysokou vypovídací hodnotu. Důvěra v takto vytvořený podpis je vysoká. Tato důvěra je podpořena právními aspekty, které vyplývají z použití takovéhoto podpisu a které plynou z českého zákona o elektronickém podpisu. Zejména jsou stanovena práva a povinnosti jednotlivých subjektů a případná odpovědnost za nedodržení povinností vyplývajících z tohoto zákona. Slouží pro styk příjemce a nějakého jiného subjektu, který vlastní kvalifikovaný certifikát. Příjemce podepsanou osobu nemusí osobně znát, data pro ověření získá příjemce z kvalifikovaného certifikátu. Právní jistotu v tuto komunikaci má dánu platností zákona o elektronickém podpisu, nemusí tedy na rozdíl od předchozího případu uzavírat speciální smlouvy pro legislativní podporu této komunikace. Důvěra v obsah certifikátu je dána důvěrou v poskytovatele certifikačních služeb, který certifikát vydal, a z možných právních dopadů, které vyplývají z nutnosti dodržovat zákon o elektronickém podpisu těmito poskytovateli. Tento typ může být použit i k „anonymnímu“ styku (místo jména může být uveden pseudonym). V případě právního sporu je „anonymní“ držitel certifikátu dohledán prostřednictvím údajů, které má k dispozici poskytovatel certifikačních služeb. Lze použít všude tam, kde se v českém zákoně o elektronickém podpisu umožňuje nahradit podpis elektronickým podpisem

Obecně se považuje tento typ za vhodný pro přímou komunikaci mezi subjekty. Není vhodný k archivaci dat a tam, kde je nutné zpětně prokazovat, kdy přesně byl dokument podepsán.

Chystaná novela zákona o elektronickém podpise zavádí ještě pojem elektronické značky.

Elektronické značky jsou z technického hlediska obdobou zaručeného elektronického podpisu, resp. mohou mít obdobný účinek a mají stejné vlastnosti vůči označovaným datům jako zaručený elektronický podpis vůči podepisovaným datům. Požadavky na zaručený elektronický podpis a na elektronické značky jsou proto obdobné. Přínos zavedení možnosti jejich používání tkví v tom, že na rozdíl od zaručeného elektronického podpisu, který vytváří

fyzická osoba vždy pro jednu určitou datovou zprávu, mohou být elektronickými značkami datové zprávy označovány tak, že je iniciována funkce prostředku, který je vytváří, a označování datových zpráv může probíhat bez další přímé součinnosti označující osoby.

Zapamatujte si

Zákon o elektronickém podpisu č.227/2000 Sb.

1. Rozlišuje tyto typy elektronických podpisů:
   - elektronický podpis
   - zaručený elektronický podpis
   - zaručený elektronický podpis založený na certifikátu / kvalifikovaném certifikátu
   - (zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb)
   - elektronická značka

2. Rozlišuje tyto typy poskytovatelů certifikačních služeb:
   - poskytovatel certifikačních služeb
   - poskytovatel certifikačních služeb vydávajících kvalifikované certifikáty
   - poskytovatel certifikačních služeb vydávajících kvalifikované certifikáty, který je pro tuto činnost akreditován (akreditovaná certifikační autorita)

3. Rozlišuje tyto typy certifikátů
   - certifikát
   - kvalifikovaný certifikát
   - kvalifikovaný certifikát vydaný akreditovaným poskytovatelem certifikačních služeb.

II.4 Povolená podpisová schémata

Podpisové schéma	Asymetrický algoritmus	Parametry asymetrického algoritmu	Algoritmus na generování klíčů	Metoda určená pro padding	Hašovací funkce
001	Rsa	MinModLen= 1020	rsagen1	emsa-pkcs #1-v1.5	sha1
002	Rsa	MinModLen= 1020	rsagen1	emsa-pss	sha1
003	rsa	MinModLen= 1020	rsagen1	emsa-pkcs #1-v1.5	ripemd160
004	rsa	MinModLen= 1020	rsagen1	emsa-pss	ripemd160
005	dsa	pMinLen=1024 qMinLen=160	dsagen1	–	sha1
006	ecdsa-F_p	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	–	sha1
007	ecdsa-F_2^m	qMinLen=160 r0Min=10^4 MinClass=200	ecgen2	–	sha1

V tabulce jsou uvedeny povolené kryptografické algoritmy a jejich parametry pro vytváření dat pro vytváření elektronických značek, kterými poskytovatel označuje vydávané

certifikáty, seznamy certifikátů vydaných jako kvalifikované, které byly zneplatněny, a kvalifikovaná časová razítka, a pro prostředky pro bezpečné vytváření a ověřování elektronických podpisů jsou uvedeny v příloze č.2 prováděcí vyhlášky k zákonu o elektronickém podpisu.

Zapamatujte si
Při stanovení povolených podpisových schémat se vycházelo z doporučení skupiny EESSI (European Electronic Signature Standardisation Initiative).

Konkrétně z dokumentu Algorithms and Parameters for Secure Electronic Signatures
Verze : V.2.1, Oct 19th 2001 , http://www.ict.etsi.org/eessi/EESSI-homepage.htm

II.5 Certifikát, kvalifikovaný certifikát

Certifikát je datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost. Certifikát je zpravidla zasílán současně s datovou zprávou a elektronickým podpisem této datové zprávy. Vydané certifikáty zpravidla poskytovatelé certifikačních služeb zveřejňují v seznamu vydaných kvalifikovaných certifikátů a umožňují k nim dálkový přístup.

Kvalifikovaným certifikátem je certifikát, který má náležitosti § 12 zákona o elektronickém podpisu č. 227/2000 Sb. a byl vydán poskytovatelem certifikačních služeb, splňujícím podmínky pro poskytovatele certifikačních služeb vydávající kvalifikované certifikáty. Žadatel o kvalifikovaný certifikát musí osobně navštívit s žádostí o vydání tohoto certifikátu některou registrační autoritu, která spolupracuje s poskytovatelem, který vydává kvalifikované certifikáty. Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí zajistit, aby údaje uvedené v kvalifikovaných certifikátech byly přesné, pravdivé a úplné, před vydáním kvalifikovaného certifikátu bezpečně musí ověřit totožnost osoby, které kvalifikovaný certifikát vydává, případně i její zvláštní znaky, vyžaduje-li to účel kvalifikovaného certifikátu a zjistit, zda v okamžiku vydání kvalifikovaného certifikátu má žadatel o certifikát data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů, která obsahuje kvalifikovaný certifikát. Poskytovatel si vytvoří kopie předložených osobních dokladů žadatele o certifikát a uchovává informace a dokumentaci o vydaných kvalifikovaných certifikátech po dobu nejméně 10 let od ukončení platnosti kvalifikovaného certifikátu. Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí zajistit provozování bezpečného a veřejně přístupného seznamu vydaných kvalifikovaných certifikátů, a to i dálkovým přístupem, a údaje v něm obsažené při každé změně okamžitě aktualizovat,

V odstavci 1, §12 (Náležitosti kvalifikovaného certifikátu) zákona o elektronickém podpisu č. 227/2000 Sb. je taxativně vyjmenováno, co musí kvalifikovaný certifikát obsahovat.

Každý kvalifikovaný certifikát musí obsahovat následující údaje:
a) označení, že byl vydán jako kvalifikovaný certifikát podle tohoto zákona (jinak by osoba, která se spoléhá na podpis, nepoznala, že se jedná o kvalifikovaný certifikát),
b) obchodní jméno poskytovatele certifikačních služeb a jeho sídlo, jakož i údaj, že certifikát byl vydán v České republice,

c) jméno a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym (díky pseudonymu je např. možné „anonymně“ používat některé placené nabízené služby),
d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu
(např. to, že majitel certifikátu je starší 18-ti let a může se tedy zúčastnit hazardní hry po Internetu, nebo že je statutárním zástupcem nějaké organizace a může elektronicky podepisovat elektronické dokumenty této organizace),
e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby (důvěryhodné předání těchto dat je vlastně smysl certifikátu !),
f) zaručený elektronický podpis poskytovatele certifikačních služeb, který kvalifikovaný certifikát vydává (tento podpis musí být vytvořen pomocí speciálního nástroje, který je k tomuto účelu vyroben, je vysoce bezpečný a je „schválen“ pro tuto činnost Úřadem pro ochranu osobních údajů, seznam těchto nástrojů zveřejňován),

g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb (jednou vydané číslo již nesmí být znovu použito a to i poté, co byl certifikát zneplatněn, číselná řada určující certifikát však nemusí být „spojitá“),
h) počátek a konec platnosti kvalifikovaného certifikátu (doba platnosti bývá zpravidla od šesti do dvanácti měsíců),
i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití (např. omezení, že certifikát byl vydán jen pro použití v určité agendě např. jen v rámci jedné firmy, nebo pro konkrétní aplikaci nebo pro nákup v konkrétním e-obchodě atd.),
j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít (lze omezit nejen výši transakce, ale např. lze i použít k oznámení, že majitel certifikátu neobchoduje za použití elektronického podpisu) .

Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby. Jedná se především o údaje jako adresa bydliště majitele certifikátu, rodné číslo, přesné datum narození, zaměstnavatel apod.

Standardizace certifikátu vychází z doporučení ITU (dříve CCITT) X.509. Původní verze číslo 1 certifikátu podle normy X.509 z roku 1988 byla postupně rozšířena, dnes je nejběžnější verze 3 (návrh verze 4 je již schválen, ale není běžně používán).

Pro studium obsahu významu jednotlivých polí se doporučuji seznámit s doporučeními řady RFC a to části : Internet X.509 Public Key Infrastructure .
RFC 2459 -Certificate and CRL Profile
RFC 3039 -Qualified Certificate Profile
RFC 3279 - Certificate and Certificate Revocation List (CRL) Profile
RFC 3280 - Certificate and Certificate Revocation List (CRL) Profile
RFC 3709 -Logotypes in X.509 Certificates

Kromě certifikátů podle doporučení RFC se v praxi můžeme setkat i s certifikáty jiných formátů - např. EDI, WAP. Formy takovýchto certifikátů jsou sice jiné, ale princip zůstává stejný.

Zapamatujte si

1. certifikát spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost
2. osobě, která se spoléhá na podpis a ověřuje jej, umožňuje získat důvěryhodným způsobem data na ověření elektronického podpisu
3. co musí obsahovat kvalifikovaný certifikát, je taxativně vymezeno v zákoně o elektronickém podpisu
4. další osobní údaje v něm mohou být uvedeny pouze se souhlasem žadatele o certifikát
5. poskytovatel certifikačních služeb před vydáním kvalifikovaného certifikátu provede kopii našich osobních dokladů a ty předepsaným způsobem archivuje
6. ani z kvalifikovaného certifikátu se nemusíme dozvědět jméno podepisující osoby nebo jeho bydliště, k tomu není certifikát určen (tyto údaje však zná poskytovatel certifikačních služeb)
7. certifikáty jsou detailně specifikovány např. v doporučeních RFC, nejpoužívanějšími certifikáty jsou certifikáty verze X.509 v.3.

II. 6 Nástroj elektronického podpisu

Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje svým zaručeným elektronickým podpisem kvalifikované certifikáty (uživatele i své další certifikáty) a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Nástroj elektronického podpisu používaný pro toto podepisování nelze použít pro jiné než tyto účely! Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, je povinen používat pouze bezpečné nástroje elektronického podpisu. Nástroj elektronického podpisu je bezpečný, pokud odpovídá požadavkům stanoveným zákonem č.227/2000 Sb., které jsou upřesněny v prováděcí vyhlášce č.366/2001 Sb. Používání takovéhoto nástroje musí poskytovatel certifikačních služeb vydávající kvalifikované certifikáty mít ověřeno Ministerstvem informatiky ČR.

Ministerstvo vyhodnocuje nástroj na základě písemné žádosti shodu nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, s požadavky stanovenými zákonem o elektronickém podpisu.

Pokud nástroj elektronického podpisu splňuje požadavky stanovené zákonem o elektronickém podpisu a Ministerstvo vysloví shodu, je nástroj považován za bezpečný. Seznam nástrojů, u nichž byla vyslovena shoda, je zveřejňován Úřad ve Věstníku a na www stránkách ministerstva.

Žádné jiné subjekty (tj. např. podepisující se osoba, elektronická podatelna, poskytovatel certifikačních služeb, který nevydává kvalifikované certifikáty) nemají za povinnost takovýto nástroj používat. Cena takovéhoto nástroje je vysoká a pohybuje se v tisících USD.

Za podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky se platí správní poplatek 10 000,- Kč.

Poznámka

Pozor při překladu originálních dokumentů EU. V anglicky psaných materiálech se používá pro nástroj elektronického podpisu termín „product“ („electronic-signature product“ – nástroj elektronického podpisu) nebo HSM (hardware seucurity modul) zatímco termín „device“ je určen pro český termín prostředek (např. Secure Signatur-Creation Device - prostředek pro bezpečné vytváření elektronických podpisů).

V následující tabulce je v souladu s § 8 odst. 3 vyhlášky č. 366/2001 Sb. uveden seznam všech nástrojů, u nichž Odbor elektronického podpisu vyslovil shodu. Seznam byl také zveřejněn ve Věstníku ministerstva informatiky 2003/částka 1.

Poř. číslo	Nástroj elektronického podpisu	Výrobce
1.	**CSA8000;** Firmware Version 1.1, Hardware Revision: G, pracující ve FIPS módu	Eracom Technologies Australia, Pty. Ltd. Burleigh Heads Queensland Austrálie
2.	**nShield F3 SCSI;** Firmware 5.0, Hardware Version nC4032W-150, pracující ve FIPS módu	nCipher Corporation Ltd. Jupiter House Station Road Cambridge CBI 2JD United Kingdom
3.	**PrivateServer 3.0;** Firmware Version 3, Hardware Version 3.0, pracující ve FIPS módu	Algorithmic Research, Ltd. 10 Nevatim St., Kiryat Matalon Petah Tikva Israel
4.	**Luna CA^3;** Firmware Version 3.2., Hardware	Chrysalis-ITS, Inc. One Chrysalis Way Ottawa K2G6P9 Ontario
5.	**ACCE** **/Advanced Configurable Crypto Environment/** Firmware Version 2.2 Hardware 2640-G3	AEP Systems International Ltd. Innovation House 39 Mark Road Hemel Hemstead Hertfordshire HP2 7DN United Kingdom
6.	**nShield F3 Ultrasign PCI** Firmware Version 2.0.0 a 2.0.2 Hardware Version nC4032P-300 pracující v módu FIPS 140-2 level 3	nCipher Corporation Ltd. Jupiter House Station Road Cambridge CBI 2JD United Kingdom
7.	**Luna CA^3;** Firmware Version 3.9., Hardware	Chrysalis-ITS, Inc. One Chrysalis Way Ottawa K2G6P9 Ontario

Zapamatujte si

1. Nástroj elektronického podpisu se používá k podepisování kvalifikovaných certifikátů a seznamu certifikátů, které byly zneplatněny
2. Poskytovatelé certifikačních služeb, kteří vydávají kvalifkované certifikáty, musí takovýto nástroj používat
3. Shodu nástroje s požadavky zákona o elektronickém podpisu vyslovuje Ministerstvo informatiky ČR
4. Nástroj elektronického podpisu není totéž co prostředek pro bezpečné vytváření (resp. ověřování) elektronického podpisu
5. Obecně platí, že musí splňovat záruky bezpečnosti podle FIPS 140-1 nebo FIPS 140-2 na Level 3

II.7 Prostředky pro bezpečné vytváření a ověřování elektronických podpisů

Tyto prostředky jsou definovány v §17 zákona o elektronickém podpisu č.227/2000 Sb. Požadavky na tyto prostředky vycházejí z obdobných obecných požadavků Směrnice 1999/93ES o zásadách Společenství pro elektronické podpisy a jsou uvedeny v příloze č.III. tohoto dokumentu.

Jedná se především o to, aby prostředek pro bezpečné vytváření podpisu za pomoci odpovídajících technických a programových prostředků a postupů zaručil, že data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno, že data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie. Tento prostředek musí dále zajistit, aby data pro vytváření podpisu mohla být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou. Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.

Navržená novela zákona o elektronickém podpisu nově zavádí, že prostředky pro bezpečné vytváření elektronických podpisů musí být před svým použitím bezpečným způsobem vydány a data pro vytváření elektronických podpisů musí být důvěryhodným způsobem v těchto prostředcích vytvořena nebo do nich přidána.

Obdobné jsou i bezpečnostní a procesní požadavky na prostředek pro bezpečné ověřování podpisu a pro prostředek pro vytváření značek (opět až v návrhu novely zákona). Nově se u prostředku pro ověřování elektronického podpisu zavádějí požadavky související se zobrazením výsledku ověření, případně se spolehlivým zobrazením dat uvedených v certifikátu. Zejména to jsou tyto požadavky: podpis musí být spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen, ověřující osoba musí mít možnost spolehlivě zjistit obsah podepsaných dat, spolehlivě musí být zjištěna pravost a platnost certifikátu při ověřování podpisu, výsledek ověření a případné použití pseudonymu musí být řádně zobrazeno.

Tyto obecné požadavky upřesňuje prováděcí vyhláška č. 366/2001 Sb. v paragrafu 7. Konkretizuje zde alespoň některé z požadavků, např. vyžaduje, aby podepisující se osoba byla informována, že používá tento prostředek a musela před jeho použitím zadat přístupové heslo nebo použít jiný obdobný autentizační mechanismus. Upřesněny jsou i požadavky na kryptografické algoritmy a jejich parametry. Tyto požadavky jsou uvedeny v příloze č. 2 této vyhlášky (odstavec II.4 této přednášky).

Prostředek pro bezpečné vytváření zaručeného elektronického podpisu vyžaduje dostatečnou záruku bezpečnosti; tento požadavek se považuje za splněný, pokud prostředek

odpovídá požadavkům technické normy upravující oblast informační bezpečnosti. Touto normou je ČSN ISO 15408 a příslušná úroveň záruky je EAL 4.

Splnění požadavků na prostředek pro bezpečné vytváření zaručeného elektronického podpisu stanovených v § 17 zákona o elektronickém podpisu se dokládá výsledkem hodnocení prostředku pro bezpečné vytváření zaručeného elektronického podpisu a seznamem technických norem upravujících oblast informační bezpečnosti, podle kterých byl hodnocen. Nikde není stanoveno, kdo takovéto hodnocení může provést. Předpokládá se přebírání hodnocení ze vznikajících laboratoří v EU. Časem pravděpodobně vznikne nějaké hodnotitelské pracoviště i v ČR. Aby bylo uznáno hodnocení tohoto pracoviště i v zemích EU, je nutné zapojení tohoto pracoviště do evropského akreditačního schématu. Některé detaily této koncepce lze najít již ve Směrnici 1999/93/ES o zásadách Společenství pro elektronické podpisy.

Náš zákon o elektronickém podpisu nestanoví žádnému subjektu povinné používání takovéhoto prostředku. Je pouze na podepisující osobě nebo na osobě, která se spoléhá na podpis, zda takový prostředek (např. z důvodu vyšší bezpečnosti a tedy i právní jistoty) používá nebo ne. Poněkud deklarativně se o tomto podpisu mluví pouze v odstavci 2, paragrafu 3.

„Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.“

V dokumentech Evropské Unie se vžilo označení pro takovýto podpis – tedy zaručený elektronický podpis, založený na kvalifikovaném certifikátu a vytvořený pomocí prostředku pro bezpečné vytváření elektronického podpisu - zkrácené označení „kvalifikovaný podpis“.

Osoba, která se spoléhá na kvalifikovaný podpis, má samozřejmě velikou důvěru v takovouto komunikaci. Nemá však možnost z podpisu přímo zjistit, zda se jedná o kvalifikovaný nebo nekvalifikovaný podpis (přesněji zda při vytváření podpisu byl nebo nebyl použit prostředek pro bezpečné vytváření elektronického podpisu). Navrhuje se tedy, aby osoba, která vlastní prostředek pro bezpečné vytváření elektronického podpisu, si tuto informaci nechala zapsat do svého kvalifikovaného certifikátu. Pokud by vytvořila podpis založený na tomto certifikátu bez použití tohoto prostředku – musí o tom druhou stranu (např. v podepsaném textu) informovat.

V dokumentech Evropské unie se doporučuje pro tento typ podpisu zavádět v příslušných legislativních úpravách stejnou právní akceptovatelnost jako u podpisu vlastnoručního. Upozorňuji, že pouhé konstatování, že se jedná o kvalifikovaný (bezpečný) elektronický podpis nestačí, aby byl takovýto podpis právně akceptovatelný všude tam, kde se používá vlastnoruční podpis. Toto tvrzení se mylně v médiích uvádí, ale není pravdivé. Je nutné provést příslušné legislativní změny, které použití jakéhokoliv typu elektronického podpisu (tedy případně i kvalifikovaného podpisu) v příslušném procesu umožní.

Jak se dále dočteme v části, která se zabývá standardizačním a normotvorným procesem v EU, stále ještě nejsou k dispozici všechny normy a standardy, které jsou nutné pro hodnověrné určení bezpečnosti takovéhoto prostředku. Základní problém bezpečnosti se často shrnuje do jediné věty: „What You See is What You Sign“. Zajištění toho, aby podepisující osoba měla jistotu, že skutečně podepsala (a vyjádřila tak svoji vůli) to, co vidí, je technicky nesmírně náročné a vede k odborným diskusím, zda je vůbec možné toto zajistit v běžném počítači vybaveném komerčním systémem. Obecně lze konstatovat, že se (tak jako u nás) požaduje hodnocení takovýchto prostředků podle ISO 15408 na úroveň EAL 4. V současné době se dokončují metodiky takovéhoto hodnocení, příslušné bezpečnostní profily (PP-Protecion Profiles) a dokončují se administrativní záležitosti kolem vzájemného uznávání hodnocení v různých zemích společenství. Zvláštní význam se klade definici tzv. „lidského rozhraní“ , předpokládá se vývoj a výroba speciálních bezpečných klávesnic, „monitorů“,

speciálních čipových karet atd. Problematika je velice široká a překračuje svým rozsahem rámec této krátké publikace.

Zapamatujte si

1. V zákoně o elektronickém podpise není stanovena žádnému subjektu povinnost používat prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů.
2. používáním těchto prostředků se zvyšuje důvěra v tuto komunikaci
3. kvalifikovaný podpis je zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvářený prostředkem pro bezpečné vytváření elektronického podpisu
4. zjednodušeně řečeno - prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů musí splňovat bezpečnostní požadavky podle ISO 15408 , na úroveň záruky EAL 4, v ČR je toto hodnocení uznáváno z libovolné testovací laboratoře, která je schopna tyto testy provádět

II.8 Časové razítko

Pojem nově zavádí a upravuje jeho poskytování navržená novela zákona o elektronickém podpisu. Časové razítko je zde chápáno jako jedna ze služeb, které může poskytovatel kvalifikovaných služeb provozovat.

Definice: kvalifikovaným časovým razítkem je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Definice je opět technologicky neutrální. Podívejme se, jak v praxi celý proces poskytování takovéto služby vypadá.

Žadatel nejdříve zašle TSA (Time Stamping Authority) žádost o časové razítko. Přesný formát žádosti specifikuje dokument RFC 3161. V požadavku je **vždy** obsažen otisk dokumentu pro nějž má být časové razítko vystaveno. TSA po přijetí žádosti zkontroluje její formální správnost a postoupí ji do „programu“ pro vytváření časových razítek (tento program musí mít především zajištěnu synchronizaci s kvalitním časovým zdrojem). Zde se vytváří „časové razítko“ jako datová zpráva, jejíž součástí je hodnota času (v definovaném/světovém formátu), sériové číslo razítka !, identifikátor politiky TSA a datum. Program do auditní databáze zapíše vytvoření takovéto zprávy. Dále se k takto předdefinované zprávě připojí zaslaný otisk a tato dvojice se podepíše soukromím klíčem TSA ve speciálním tomu určeném zařízení (zpravidla hodnocené podle FIPS 140-1 (resp. 2) na Level 3). Tím vznikne tzv. časový token, který se zasílá žadateli zpět ve formátu ASN.1, der nebo pem.

Zapamatujte si

- časové razítko prokazuje, že dokument existoval v čase, kdy byla přijata žádost o tuto službu
- vydávání kvalifikovaných časových razítek je upraveno v novele zákona o elektronickém podpisu

II.9 Elektronický podpis a legislativa v ČR (akceptování jednotlivých typů certifikátů)

Zjednodušeně lze říci, že v legislativním procesu zavedení elektronického podpisu v České republice vystupovaly tři hlavní subjekty: Úřad pro ochranu osobních údajů (měl na starosti vydání prováděcí vyhlášky, proces akreditace, hodnocení nástrojů pro elektronický podpis, dohled a dozor), vláda (připravila nařízení, kterým se provádí zákon o elektronickém podpisu), Úřad pro veřejné informační systémy (připravil standard pro elektronické podatelny a atestace- hodnocení shody podatelen s tímto standardem). Od 1.1.2003 převzalo všechny kompetence k zákonu o elektronickém podpisu na základě zákona č. 517/2002 Sb. nově vzniklé Ministerstvo informatiky. Základem nového ministerstva je bývalý ÚVIS (Úřad pro veřejné informační systémy) a dále pod toto ministerstvo přešel z ÚOOÚ (Úřad pro ochranu osobních údajů) i odbor elektronického podpisu.

Zákon, nařízení vlády, standard pro elektronické podatelny

Před čtyřmi lety, konkrétně 1.10.2000, vstoupil v účinnost zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (dále jen „zákon č. 227/2000 Sb.“). Poté následovala celá řada dalších, neméně důležitých kroků nutných k tomu, aby mohl být elektronický podpis v komunikaci občan – stát používán. Důležitým krokem se stalo vydání nařízení vlády č. 304/2001, kterým se zmiňovaný zákon provádí. To stanoví povinnost orgánů veřejné moci zřídit elektronické podatelny a zajistit jejich provoz. Těmi se zabývá standard ISVS pro provoz elektronických podatelen ve vztahu k používání zaručeného elektronického podpisu. Byl uveřejněn ve Věstníku ÚVIS, ročník III, částka 1, 2002. Účinný je od 25.6.2002, kdy byl vyhlášen. Řeší především provoz a atestaci elektronických podatelen. Elektronická podatelna je podle tohoto standardu informačním systémem veřejné správy. Pro prokázání shody elektronické podatelny s tímto standardem se ovšem nevyžaduje její atest. Ten je vyžadován pouze na technické vybavení podatelny a související dokumentaci. Technické vybavení musí splňovat požadavky článku 4.5 standardu. Jedná se především o požadavky na funkčnost - ukládání přijatých zpráv, ověřování elektronických podpisů, formáty a kódování zpráv apod. Standard doporučuje, aby atest byl prováděn i s ohledem na bezpečnost, bezporuchovost a použitelnost vybavení.

Prováděcí vyhláška k zákonu o elektronickém podpisu

Úřad pro ochranu osobních údajů vydal na základě zmocnění zákona č.227/2000 Sb. vyhlášku, která upřesňuje některé požadavky pro vydávání kvalifikovaných certifikátů a dále požadavky na „nástroje“ elektronického podpisu. Celá vyhláška se tedy týká především poskytovatelů certifikačních služeb, kteří hodlají vydávat kvalifikované certifikáty, a poskytovatelů, kteří chtějí pro tuto činnost získat akreditaci. Činnost akreditovaných poskytovatelů je pro komunikaci stát - občan nezbytná, jak je vidět z dikce § 11 tohoto zákona („V oblasti orgánů veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb“.)

V říjnu roku 2000 vstoupil v účinnost Zákon o elektronickém podpisu a o změně některých dalších zákonů č.227/2000 (dále jen Zákon č.227/2000 Sb.). Následovala řada dalších kroků nutných k tomu, aby mohla být realizována komunikace podle tohoto zákona. Na základě zmocnění v Zákoně č.227/2000 Sb. připravil Úřad pro ochranu osobních údajů znění návrhu vyhlášky, ale se zahájením legislativních kroků k jejímu přijetí musel ještě počkat do května 2001. Čekalo se na novelu zákona č.101/2000 Sb., která Úřadu (zjednodušeně řečeno) umožnila nejen vyhlášku připravit, ale také publikovat ve sbírce zákonů. Po rozsáhlém připomínkovém řízení byla vyhláška předána k projednání v příslušných komisích Legislativní rady vlády ČR. Vyhláška byla publikována 10.10.2001. Je určena především poskytovatelům certifikačních služeb a upřesňuje požadavky na ty

poskytovatele, kteří hodlají vydávat kvalifikované certifikáty, upřesňuje postup akreditace těch poskytovatelů certifikačních služeb, kteří zažádali ve správním řízení o akreditaci a dále upřesňuje požadavky na nástroje elektronického podpisu.

Vydání této vyhlášky bylo předpokladem pro zahájení činnosti poskytovatelů certifikačních služeb vydávajících kvalifikované certifikáty a akreditovaných poskytovatelů certifikačních služeb.

Dalším nutným krokem k využívání elektronického podpisu bylo vydání Nařízení vlády č.304/2001 Sb. ze dne 25. července 2001. Toto nařízení upravuje některou komunikaci v oblasti občan-stát (podání) a současně stanovuje vytvoření podmínek pro tuto komunikaci v oblasti orgánů veřejné moci – především zřízení tzv. „elektronických podatelen“. Podle tohoto nařízení mají být pracoviště pro příjem a odesílání datových zpráv vybavena potřebnými zařízeními připojenými k veřejné datové síti, popřípadě k jiným datovým sítím a budou muset splňovat požadavky na technické a programové vybavení podle standardů, které připravil Úřad pro veřejné informační systémy.

Od 1.1.2003 má všechny kompetence k zákonu o elektronickém podpisu Ministerstvo informaticky České republiky (http://www.mice.cz/). Pracovníci odboru elektronického podpisu MI ČR připravili návrh novely zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů. Zákon odstraňuje drobné legislativní nedostatky (vyplývající ze změny gesce), rozšiřuje služby, které kvalifikovaný poskytovatel může provozovat, zavádí kvalifikovaná časová razítka, elektronické značky. Ministerstvo připravuje i novelu prováděcí vyhlášky a vyhlášku upravující povinnost provozovat elektronické podatelny.

Uvedený návrh novely zákona byl vládou schválen dne 5. 11. 2003 a následně byl postoupen k projednání Poslanecké sněmovně, kde byl schválen 31.3.2004. Novelu musí nyní schválit senát a podepsat prezident.

Zapamatujte si

Přehled platných legislativních předpisů

[1] Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) č. 227/2000 Sb.
Datum přijetí: 29. června 2000
Datum účinnosti od: 1. října 2000
http://www.mvcr.cz/sbirka/2000/sb068-00.pdf

[2] Zákon č.226/2002 Sb. ze dne 9.5.2002, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů, a zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
Datum účinnosti od : 1. července 2002.
http://www.mvcr.cz/sbirka/2002/sb087-02.pdf

[3] Návrh zákona o změně zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů.
Uvedený návrh novely zákona byl vládou schválen dne 5. 11. 2003 a následně byl postoupen k projednání Poslanecké sněmovně, kde byl schválen 31.3.2004. Novelu musí nyní schválit senát a podepsat prezident.
http://www.micr.cz/scripts/detail.php?id=201

[4] Nařízení vlády č.304/2001 ze dne 25. července 2001
(Nařízení vlády č.304 ze dne 25. července 2001, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)). Datum účinnosti od: 1. října 2001
http://www.mvcr.cz/sbirka/2001/sb117-01.pdf

[5] Standard ISVS pro provoz elektronických podatelen ve vztahu k používání zaručeného elektronického podpisu, 016/01.01
Uveřejněn ve Věstníku ÚVIS
Datum vyhlášení : 25. června 2002

[6] Dobrým přehledovým zdrojem je sekce „Právní předpisy a standardy pro EP“
http://crypto-world.info/pravo/index.htm na mé www stránce (http://crypto-world.info/)
Právní předpisy a standardy pro EP
I. Ochrana osobních údajů /
II. Elektronický podpis /
III. Elektronické podatelny
IV. Standardy ISVS související se standardem pro provoz elektronických podatelen

II.10 Evropská Unie (legislativa, standardy a normy)

Tato kapitola je věnována legislativnímu procesu v oblasti elektronického podpisu a současnému normotvornému a standardizačnímu procesu v Evropském společenství. V legislativním procesu za EU nezaostáváme, ba dokonce máme mírný náskok (viz některé moderní prvky v novele zákona o elektronickém podpisu: zavedení kvalifikovaných časových razítek, elektronické značky). V čem je však zásadní rozdíl, je promyšlenost technického nasazení a především v nedostatku nosných agend a aplikací, které by byly pro uživatele zajímavé. Chybí pilotní projekty a analýza výsledků takto získaných zkušeností. Chybí technické laboratoře a zkušebny, které by dokázaly hodnověrně prokazovat kvalitu a bezpečnost připravovaných technických řešení. V naší společnosti se mylně očekává (a tato představa je živena výroky v médiích), že k nějakému datu – např. až se začnou vydávat hromadně kvalifikované certifikáty - se prostě nastartuje „neomezené“ používání elektronického podpisu.

Evropský parlament a Rada přijaly v prosinci roku 1999 Směrnici 1999/93/ES o zásadách Společenství pro elektronické podpisy. Tento dokument ukládá členským státům Evropské Unie přijmout právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí (požadavky na právní akceptovatelnost e-podpisu, vytvoření dobrovolných akreditačních schémat, vzájemné uznávání certifikátů apod.). Termín, do kdy měly být tyto zásady v jednotlivých právních systémech implementovány, byl 19. červenec 2001. V současné době mají tedy členské státy EU již přijaty adekvátní legislativní úpravy elektronického podpisu v souladu s výše uvedenou směrnicí.

V Evropském společenství však neprobíhá jen bouřlivý legislativní proces, který má za úkol harmonizaci příslušných zákonů s požadavky Směrnice, ale probíhají také velice rozsáhlé práce v oblasti přípravy příslušných norem a standardů. Byly zahájeny v lednu 1999 z podnětu ICTSB (*Information Communications Technologies Standard Board)*. Za podpory Evropské komise zahájila svoji koordinační činnost iniciativa **EESSI *(The European Electronic Signature Standardization Initiative)***. Tato iniciativa pracuje speciální formou širokého diskusního fóra expertů ze sféry průmyslu, veřejné správy a dalších zainteresovaných subjektů. Během pěti let svého působení prokázala tato iniciativa schopnost

účinně iniciovat a koordinovat přípravu a přijetí standardů nezbytných pro naplnění rámcových technických a bezpečnostních ustanovení Směrnice.

Tato skupina také vydala jeden z velice významných dokumentů zabývající se kryptografickými moduly (Algorithms and Parameters for Secure Electronic Signatures). Tento dokument byl také zapracován při tvorbě naší prováděcí vyhlášky č. 366/2001 Sb. a stal se podkladem k výběru algoritmů a jejich parametrů tak, jak jsou uvedeny v příloze č.2 této vyhlášky (odstaveec II.4 této přednášky). Důvodem, proč vydala tento dokument přímo EESSI, je možnost v případě potřeby reagovat rychleji než v klasickém procesu změny standardu či normy (např. při nutnosti odvolat z důvodu bezpečnosti používání některého algoritmu nebo naopak v případě vhodnosti mít možnost pozměnit doporučený parametr, či umožnit používání nového bezpečného algoritmu).

Dalšími důležitými standardizačními orgány v oblasti elektronického podpisu a rozvije PKI jsou ETSI a CEN/ISSS.

ETSI

The European Telecommunications Standards Institute je nezisková organizace, která působí od roku 1988 s cílem připravovat telekomunikační standardy pro dlouhodobé využití. Je oficiálně uznána jak Evropskou komisí, tak i sekretariátem EFTA (European Free Trade Association). Standardizace prostředků elektronického podpisu, včetně standardů pro činnost podpůrných infrastruktur (PKI), je v kompetenci technické komise TC SEC (Security), v jejímž rámci byla ustanovena samostatná pracovní skupina pro oblast elektronického podpisu (Working Group on Electronic Signatures and Infrastructures - ESI WG).

CEN/ISSS

European Committee for Standardization / Information Society Standardization System byl zřízen v roce 1997 Evropským výborem pro standardizaci (CEN) s cílem podpory informačních a komunikačních technologií v podmínkách rozvoje informační společnosti, kdy tradiční postupy standardizace a normalizace již nemusí zcela vyhovovat. Vlastní realizační práce jsou organizovány v pracovních skupinách (Workshops), uspořádaných do pěti kmenových větví. Z toho ve větvi na podporu legislativního procesu EU v oblasti elektronického podpisu je činná pracovní skupina pro elektronický podpis (E-SIGN Workshop).

Užitečné zdroje k tomuto tématu:

[1] Dobrým přehledovým zdrojem je sekce „Některé vybrané normy a standardy pro EP“
http://crypto-world.info/normy/index.htm na mé www stránce http://cyrpto-world.info
I. EESSI
II. CEN/ISSS
III. ETSI
IV. RFC

[2] Directive EU: Evropská komise DG XV - Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures,
http://crypto-world.info/pravo/podpis/dir_99_93_EC_CZ.pdf
http://crypto-world.info/pravo/podpis/dir_99_93_EC_EN.pdf

III. A ještě trochu podpisů na závěr

Kdo se prokousal naším zákonem o elektronickém podpisu (včetně chystané novely) a naučil se rozeznávat různé zde použité kategorie (elektronický podpis, zaručený elektronický podpis, zaručený elektronický podpis založený na certifikátu, zaručený elektronický podpis založený na kvalifikovaném certifikátu, zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele, kvalifikovaný podpis, elektronická značka) a vnímá rozdíl mezi elektronickým podpisem a digitálním podpisem, může si myslet, že jej v této oblasti kategorizace podpisů již nic příliš překvapit nemůže. Jenže existují i další typy podpisů, které se do předchozích škatulek tak úplně nevejdou. Právě několika takovým případům je věnován závěr této přednášky.

Níže uvedené typy *„elektronických podpisů“* nejsou jen kryptologickou hrátkou na sestavování nových možných protokolů, ale vzhledem k zajímavým „ekonomickým“ vlastnostem při ověřování podpisu, případně vzhledem k zcela novým možnostem (podpis se zachováním plné anonymity, prokazatelnost příslušnosti ke skupině apod.) se dá očekávat, že budou využívány pro speciální situace nebo se dokonce stanou běžným vybavením podpisových prostředků.

III.1 Vícenásobné podpisy (Multi-Signatures)

Tento zdánlivě jednoduchý problém, jak uvidíme, bude motivací k definování celé řady podpisů, které se od sebe svými vlastnostmi výrazně liší.

Popis problému : mějme zprávu M, kterou chceme opatřit podpisy skupiny n různých uživatelů.

První přirozené řešení je, že každý z n uživatelů podepíše svým soukromým klíčem SK_i (i = 1, .., n) zprávu M a získáme tak celkem n podpisů (S_1 , S_2 , … , S_n). Při ověření musí ověřovatel postupně pomocí veřejných klíčů VK_i (i = 1, .., n) ověřit všechny podpisy S_1 až S_n.

Druhé přirozené řešení je, že první z n uživatelů podepíše svým soukromým klíčem SK_1 zprávu M, tuto zprávu opatřenou jeho podpisem označme $S_1(M)$. Druhý z uživatelů podepíše svým soukromým klíčem SK_2 zprávu M včetně přidaného elektronického podpisu – tedy $S_1(M)$ a tak postupujeme dále. Poslední n-tý podepisující podepíše svým soukromým klíčem SK_n zprávu $S_{n-1}(S_{n-2}(S_{n-3}(….(S_2(S_1(M)))…)))$. Při ověření musí ověřovatel postupně pomocí veřejných klíčů VK_i (i = n, .., 1) ověřit všechny podpisy S_n až S_1. Výhodou této metody je, že je jednoznačně určeno pořadí, ve kterém se podepisující osoby 1 až n podepisovaly.

Motivací pro další úvahy bude hledání řešení, kdy nebude muset ověřovatel ověřovat n podpisů. Neexistuje nějaké „jednodušší“ řešení pro vytváření podpisu skupiny n uživatelů ke zprávě M (nebo dokonce k více zprávám), kdybychom jedním ověřením zjistili, že všichni uživatelé se podepsali a jejich podpisy jsou platné? Co když budeme pomocí podpisů skupiny uživatelů potřebovat zajistit a ověřit jen některé specifické vlastnosti? Možné návrhy některých řešení těchto problémů si ukážeme v následujících odstavcích.

III.2 Kruhový podpis (Ring Signatures)

Začneme podpisem, který předchozí problém zdaleka ještě neřeší, ale pro další úvahy může být užitečný.

Mějme skupinu n různých uživatelů, kterou označíme U. Každý z těchto n uživatelů má svá párová data (soukromý a veřejný klíč). Párová data i-tého uživatele označíme : (SK_i , VK_i) . Kruhový podpis skupiny uživatelů U se vytváří pomocí všech n veřejných klíčů uživatelů této skupiny a jednoho soukromého klíče libovolného (např. i-tého) uživatele ze skupiny U. Formálně se tedy dá zapsat kruhový podpis skupiny U jako R(VK_1 , VK_2 , … , VK_n , SK_i), kde i je libovolná hodnota od 1 do n. Podmínkou, abychom takovou hodnotu R mohli nazývat kruhovým podpisem je, že :

- ověřovatel musí být schopen ověřit podpis ze znalosti všech n veřejných klíčů,
- nelze podpis R vytvořit bez znalosti alespoň jednoho z n soukromých klíčů,
- ověřovatel nezjistí, čí soukromý klíč SK_i byl použit ! (tato vlastnost se označuje jako podpisová nejednoznačnost)

Jinými slovy takto zkonstruovaný podpis může vytvořit každý ze skupiny U. Ověřovatel pouze zjistí, že podpis vytvořil jeden z uživatelů této skupiny, nezjistí však který. Kruhový podpis se hodí k prokazování příslušnosti ke skupině U. Může být použit jako podpis za skupinu U, ale se zachováním anonymity podepisujícího a s možným nesouhlasem ostatních členů skupiny.

Definice a možné aplikace takovéhoto podpisu naleznete například v příspěvku Rivesta, Shamira a Taumana How to leak a secret.

R.Rivest, A.Shamir, Y.Tauman : How to leak a secret. In Proceedings of Asiacrypt 2001, volume 2248 of LNCS, pages 552-65. Springer - Verlag, 2001.

III.3 Skupinové podpisy (Group Signatures)

Existuje již celá řada různých modifikací schémat skupinového podpisu. Ve schématu představeném Chaumem a Heystem v roce 1991 se předpokládá vytvoření skupiny n uživatelů, která je spravována jedním manažerem. Pro tuto skupinu je vytvořen jeden ověřovací klíč nazývaný gpk (group public key). Každý člen skupiny má svůj vlastní podepisovací soukromý klíč, který je vytvořen tak, že „relativně odpovídá“ veřejnému skupinovému klíčí gpk.

Vlastnosti :

- každý může ověřit, že někdo ze skupiny, kterou manažer spravuje, zprávu podepsal
- manažer skupiny pomocí speciálního klíče gmsk může zjistit, kdo ze skupiny zprávu podepsal (traceability)
- kdo nemá k dispozici maskovací klíč, nemůže zjistit, kdo ze skupiny podpis vytvořil (anonymity)
- zveřejnění klíče gmsk nevede k „oslabení“ podpisového schématu (tj. podpisy, které lze ověřit klíčem gpk, mohou i nadále vytvořit pouze členové skupiny daného manažera)

Postupem času bylo schéma modifikováno a byla zapracována a analyzována řada dalších možných požadavků např. neoddělitelnosti ze skupiny (unlinkabilita), omluvitelnost (exculpabilita), různé typy odolnosti (collusion resistence, framing resistence), plná anonymita (full anonymity) . Přesné definice najdete například ve známých pracích G.Ateniesse.

D.Chaum, E. van Heyst: Group Signatures. In Proceedings of Eurocrypt 1991, volume 547 of LNCS, pages 257-265. Springer - Verlag, 1991.

G.Ateniese, G.Tsudik: Some open issues and directions in group signatures. In Financial Crypto ´99, volume 1648 of lNCS, pages 196-211. Springer - Verlag, 1999.

M.Bellare, D.Micciancio, B.Warinschi: Foundations of Group Signatures : Formal Definitions. Simplified Requirements, and a Construction Based on General Assumptions. In Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 614-30. Springer - Verlag, 2003.

III.4 Hromadné podpisy (Aggregate Signatures)

Zobecněním předchozího problému je tzv. hromadný podpis. Stručně jej lze charakterizovat takto: hromadný podpis je podpisové schéma, které umožňuje shlukování stávajících podpisů – tj. z n podpisů n různých zpráv, které vytvořilo n osob, lze vytvořit jediný krátký podpis, jehož ověřením se ověří všech n dílčích podpisů n osob k n zprávám.

Pravděpodobně je to jasné, ale přece jen uvedu, že hromadným podpisem není podpis S nějaké osoby (byť by to byl některý z výše uvedených uživatelů u_i), který vznikne podepsáním zprávy sestavené z podpisů $S_1 \dots S_n$. Takovýto podpis není závislý na platnosti, či neplatnosti jednotlivých podpisů S_i , a proto nesplňuje požadavek, že jeho ověřením se ověří jednotlivé podpisy S_i.

Formální konstrukce hromadného podpisu je následující :

Označíme-li S_i podpis i-tého uživatele u_i ke zprávě M_i , pak hodnota A bude hromadným podpisem vytvořeným pomocí hromadného podpisového schématu AS , pokud $A= AS ((u_1 , S_1 , M_1) , (u_2 , S_2 , M_2), \dots , (u_n , S_n , M_n))$, splňuje následující podmínky :

- A nelze vytvořit bez podpisů $S_1 \dots S_n$.
- ověření A je možné pouze tehdy pokud jsou platné všechny podpisy $S_1 \dots S_n$.

Hromadný podpis je výhodný vzhledem k tomu, že umožňuje snížit počet ověření n podpisů na jedno ověření a velkou výhodou je i snížení počtu certifikačních cest (chain).

S.Kent, C.Lynn, K.Seo: Secure border gateway protocol (Secure-BGP).IEEE J.Selected Areas in Comm., 18(4), pages 582-92, April 2000.
D.Boneh, C.Gentry, B.Lynn, H.Schaham: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 416-32. Springer - Verlag, 2003.