Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 3/2001 12. březen 2001

3/2001

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR.
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>260 e-mail výtisků)

OBSAH : **Str.**

Příloha : návrh vyhlášky ÚOOÚ k "Zákonu o elektronickém podpisu"
(rozeslán v pátek 9.3.2001)

A. Typy elektronických podpisů

Mgr. Pavel Vondruška, ÚOOÚ

Celý systém elektronického podepisování dokumentů podle Zákona o elektronickém podpisu č.227/2000 (dále ZoEp) je založen na několika základních pojmech. Definice těchto primitivů jsou v §2 ZoEP. Patří sem především:

- elektronický podpis
- zaručený elektronický podpis
- datová zpráva
- podepisující osoba
- poskytovatel certifikačních služeb
- akreditovaný poskytovatel certifikačních služeb
- certifikát
- kvalifikovaný certifikát
- data pro vytváření elektronických podpisů
- data pro ověřování elektronických podpisů
- prostředek pro vytváření elektronických podpisů
- prostředek pro ověřování elektronických podpisů
- prostředek pro bezpečné vytváření elektronických podpisů
- prostředek pro bezpečné ověřování elektronických podpisů
- nástroj elektronického podpisu
- akreditace

V našem článku se zastavíme u dvou podle našeho názoru stěžejních pojmů - elektronický podpis a poskytovatel certifikačních služeb.

Pojem elektronický podpis není ještě nejširší veřejností zcela správně chápán. Není zcela zřejmé, že existuje více typů elektronických podpisů a vžité jsou i špatné představy o významu elektronického podpisu a o jeho bezpečnosti.

- Mezi laickou veřejností se vyskytují následující mylná tvrzení :
- Elektronický podpis je 1000x bezpečnější než podpis vlastnoruční
- Elektronický podpis chrání text před nepovolanou osobou šifrováním
- Podpis pod e-mailem není elektronický podpis
- Bezpečný podpis je zaručený elektronický podpis
- Rozlišuje se pouze elektronický podpis a zaručený elektronický podpis.

K zakořenění těchto omylů a nesprávných tvrzení pravděpodobně přispěly výroky některých osob, které se snažily popularizovat elektronický podpis na veřejnosti.
Dále k tomu přispěla absence definic některých typů elektronického podpisu v našem ZoEP (chybí např. důležitý pojem kvalifikovaného podpisu).

Cílem tohoto odstavce je seznámit veřejnost s přesnou definicí nejběžnějších typů elektronických podpisů.

K vymezení jednotlivých typů použijeme následující kategorie: politika kvalifikovaného certifikátu, formát elektronického podpisu, formát kvalifikovaného certifikátu, časové razítko, požadavek na bezpečný systém, požadavek na bezpečný systém (PBVP) . Podle požadavků na tyto konkrétní kategorie pak definujeme profil pro následující typy elektronických podpisů:

- elektronický podpis
- zaručený elektronický podpis
- zaručený elektronický podpis založený na kvalifikovaném certifikátu
- (zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb)
- kvalifikovaný podpis
- kvalifikovaný podpis určený pro archivaci

Takto definované podpisy se vyskytují v různých souvislostech ve Směrnici EU a dokumentech ETSI a ISSS/CEN.

Elektronický podpis
(General Electronic Signature)

Vyjdeme z definice, která je zavedena v našem zákoně o elektronickém podpisu ZoEP, §2, 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,

Tato definice je zcela ve shodě s definicí uvedenou v Směrnici EU (definice 1):
'electronic signature 'means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

Požadavky na námi sledované kategorie jsou minimální. Nepožaduje se časové razítko, není definován žádný formát nebo standard, který by popisoval tvar vytvořených nebo předávaných dat. Není použit certifikát nebo jiný způsob zveřejnění pomocných dat (dat pro ověření podpisu, zveřejnění dat určení identity) ani tato data nejsou definována. Nejsou kladeny žádné specifické požadavky na použitý systém nebo podpisový prostředek (prostředek pro ověření podpisu se nedefinuje).
Uvedené požadavky sestavíme do následující tabulky - tabulku se stejnou strukturou použijeme následně k definici všech dále uvedených typů elektronických podpisů.

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	**Nezveřejnění nebo přímé poskytování politiky**	Zveřejnění politiky	Zveřejnění užívání PBVP
Formát elektronického podpisu	Elektronický podpis	Elektronický podpis + testování dat	Elektronický podpis + Testování dat + Časová razítka
Formát kvalifikovaného certifikátu	Profil kvalifikovaného certifikátu		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	**Nižší úroveň**	Kvalifikovaná úroveň	
Požadavek na bezpečný systém (PBVP)	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Takovýto „podpis“ nemá pro příjemce příliš velkou vypovídací hodnotu. Důvěra v takto vytvořený podpis je minimální. Slouží spíše pro informaci příjemce. Příkladem může být „podpis“ vložený pod klasický e-mail, ale i např. jméno autora uvedené v záhlaví článku (v elektronické podobě, dokument v MS Word apod.).

Zaručený elektronický podpis (Advanced Electronic Signature)

Začněme opět definicemi. Porovnáním definice uvedené v našem zákoně ZoEP (§2, písmeno b) a ve Směrnici (definice 2) zjistíme, že tento pojem je zaveden stejným způsobem a nemůže dojít k jeho odlišnému chápání.

ZoEP, §2, b) zaručeným elektronickým (se rozumí pro účely tohoto zákona) podpisem elektronický podpis, který splňuje následující požadavky:
- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Directive, 2 ‘advanced electronic signature ’means an electronic signature which meets the following requirements:
(a)it is uniquely linked to the signatory;
(b)it is capable of identifying the signatory;
(c)it is created using means that the signatory can maintain under his sole control;
(d)it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Požadavky na námi sledované kategorie se vzhledem k předchozí definici mění. Stále se nevyžaduje časové razítko, nevyžaduje se použití certifikátu ke zveřejnění dat pro ověření podpisu. Nově se zavádí přesné formáty pro vytváření a přenos elektronických podpisů. Toto je nutné především z hlediska kompatibility a interoperability. Základním dokumentem v této oblasti je Electronic Signature Formats (ETSI TS 101 733 V1.2.2, 2000-12).
Nově se zavádí požadavek na důvěryhodnost operačního systému, ve kterém se dokument podpisuje . Nejsou kladeny žádné specifické požadavky na podpisový prostředek nebo ověřovací prostředek. Bezpečnost těchto prostředků (použití, zabezpečení, ochrana) se zcela nechává na podepisující se o sobě (případně na osobě, která se spoléhá na podpis).

Uvedené požadavky opět sestavíme do tabulky:

EESSI Standard	Volba standardu		
Politika kvalifikovaného certifikátu	**Nezveřejnění nebo přímé poskytování politiky**	Zveřejnění politiky	Zveřejnění užívání PBVP
Formát elektronického podpisu	**Elektronický podpis**	Elektronický podpis + testování dat	Elektronický podpis + Testování dat + Časová razítka
Formát kvalifikovaného certifikátu	Profil kvalifikovaného certifikátu		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň	**Kvalifikovaná úroveň**	
Požadavek na bezpečný systém (PBVP)	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Takovýto 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. Příkladem takovéto komunikace může být klient – banka , obchodník – zákazník. Patří sem i využívání celosvětově známého programu PGP.
Z legislativně-právního hlediska se k uznání této komunikace využívá uzavření smlouvy podle obchodního nebo občanského zákoníku.

Zaručený elektronický podpis založený na kvalifikovaném certifikátu (Electronic Signature Using Qualified Certificate)

Začněme opět definicemi. K použití tohoto podpisu se zavádí pojem certifikátu, kvalifikovaného certifikátu a pojem poskytovatele certifikačních služeb. Poskytovatelé certifikačních služeb se dělí na poskytovatele, kteří vydávají certifikáty, na poskytovatele, kteří vydávají kvalifikované certifikáty a na akreditované poskytovatele certifikačních služeb.

Definice typů certifikátů jsou uvedeny v ZoEP (§2, písmeno g a h).
g) 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,
h) 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 poskytovatelů certifikačních služeb, jsou uvedeny v ZoEP (§2, písmeno e a f).

e) poskytovatelem certifikačních služeb (je) subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,

f) 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 paragrafu 6 ZoEP a dále jsou upřesněny v připravované vyhlášce ÚOOÚ.

Každý poskytovatel certifikačních služeb může požádat ÚOOÚ o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb. Podmínky udělení akreditace pro poskytování certifikačních služeb jsou uvedeny v §10 ZoEP. Ve Směrnici EU se požaduje, aby se jednalo o dobrovolný akt. Akreditovaný poskytovatel certifikačních služeb by měl být chápán jako důvěryhodný poskytovatel těchto služeb. V našem ZoEP je však jeden paragraf, který podle nás tento princip dobrovolnosti narušuje. Tímto paragrafem je paragraf 11, který nařizuje, že v oblasti veřejné moci se smí používat pouze kvalifikované certifikáty od akreditovaného poskytovatele. Tedy, kdo chce své služby nabízet pro využití v této oblasti musí být akreditovaný. Dobrovolnost akreditace se tedy stává pro tyto poskytovatele nutností.

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	Nezveřejnění nebo přímé poskytování politiky	**Zveřejnění politiky**	Zveřejnění užívání PBVP
Formát elektronického podpisu	Elektronický podpis	**Elektronický podpis + testování dat**	Elektronický podpis + Testování dat + Časová razítka
Formát kvalifikovaného certifikátu	**Profil kvalifikovaného certifikátu**		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň	**Kvalifikovaná úroveň**	
Požadavek na bezpečný systém (PBVP)	**Nižší úroveň**	Kvalifikovaná úroveň	Vyšší úroveň

Vrátíme se k popisu jednotlivých typů podpisů. Požadavky na námi sledované kategorie se vzhledem k předchozímu typu dále rozšiřují. Stále se ještě nevyžaduje časové razítko. Zpřísňují se požadavky na přesné formáty pro vytváření a přenos elektronických podpisů. Používání formátů se rozšiřuje o stanovení požadavků na formáty kvalifikovaných certifikátů a o další související formáty (žádost o vydání certifikátu apod.) . Toto je upraveno např. dokumentem ETSI : Qualified Certificates Profile (ETSI TS 101 862 V1.1.1, 2000-12). Požadavek na důvěryhodnost operačního systému, ve kterém se dokument podpisuje, je

stejný jako u předchozího typu. Požadavky na poskytovatele certifikačních služeb vydávajících kvalifikované certifikáty řeší připravovaná vyhláška ÚOOÚ. V Evropské unii řeší tuto otázku dokument Policy Requirements for CSPs Issuing Qualified Certificates (ETSI TS 101 456 V1.1.1 , 2000 -12).
Ani u tohoto typu podpisu stále není součástí profilu požadavek na používání bezpečného podpisového nebo ověřovacího prostředku.

Tento typ podpisu je základní typ elektronického podpisu, kterým se zabývá ZoEP. Takovýto podpis má pro příjemce vysokou vypovídací hodnotu. Důvěra v takto vytvořený podpis je vysoká. Tato důvěra je také podpořena právními aspekty, které vyplývají z použití takovéhoto podpisu a které plynou z českého ZoEP. 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 ZoEP, 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 ZoEP 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 v českém ZoEP se umožňuje nahradit podpis elektronickým podpisem.V českém ZoEP je tento typ podpisu přímo vyžadován v paragrafu 11, který stanoví způsob komunikace v oblasti veřejné moci. Tento profil je, jak jsme se již zmínili, je zpřísněn – nestačí, aby byl kvalifikovaný certifikát vydán poskytovatelem, který vydává kvalifikované certifikáty, ale poskytovatelem, který byl akreditován pro tuto činnost ÚOOÚ.
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.

Kvalifikovaný podpis
(Qualified Electronic Signature)

Dostáváme se k velice důležitému pojmu kvalifikovaný podpis. Tento termín není v českém ZoEP přímo použit. Přesto je na několika místech zmíněn. Vždy se však o něm mluví opisem. Poprvé se s ním můžeme setkat ve třetím paragrafu.
(ZoEP, §3 (2)) 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.

Od předchozího typu se liší požadavkem na použití prostředku pro bezpečné vytváření podpisu. Požadavky na takovýto prostředek jsou v českém ZoEP uvedeny v §17 . V EU se otázkou bezpečných prostředků zabývá celá řada dokumentů. Řada otázek však v době psaní tohoto příspěvku ještě nebyla dořešena. Příkladem těchto dokumentů mohou být následující dokumenty CEN/ISSS :
Secure Signatur-Creation Devices (EAL 4 and EAL 4+), (CWA Draft on Area F)
Security Requirements for Signature Creation Systems (CWA Draft on Area G1)
Procedures for Electronic Signature Verification V1.0.3 (2001-01-25,CWA Draft on Area G2)
EESSI Conformity Assessment Guidance; Version 2.0 (2001-01-22, CWA Draft on Area V)

Právě pojem bezpečného podpisového a ověřovacího prostředku je jeden z nejproblematičtějších pojmů celého systému elektronického podepisování. Přesné požadavky na takovýto prostředek nebyly dosud zformulovány. Obecně lze říci, že se tyto požadavky dají rozdělit na tři oblasti : požadavky technicko - kryptografické, požadavky na začlenění tohoto prostředku do informačního systému, legislativně právní požadavky. Nejsou uzavřeny ani otázky související s hodnocením bezpečnosti takovéhoto prostředku. Celá problematika je natolik komplexní a složitá, že si zaslouží samostatnou přednášku a není možné v rámci tohoto příspěvku se podrobněji těmito otázkami zabývat.

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	Nezveřejnění nebo přímé poskytování politiky	Zveřejnění politiky	**Zveřejnění užívání PBVP**
Formát elektronického podpisu	Elektronický podpis	**Elektronický podpis + testování dat**	Elektronický podpis + Testování dat + Časová razítka
Formát kvalifikovaného certifikátu	**Profil kvalifikovaného certifikátu**		
Časové razítko	Použití protokolu pro časová razítka		
Požadavek na bezpečný systém	Nižší úroveň	**Kvalifikovaná úroveň**	
Požadavek na bezpečný systém (PBVP)	Nižší úroveň	**Kvalifikovaná úroveň**	Vyšší úroveň

Kvalifikovaný podpis se považuje z hlediska důvěry za nejdokonalejší. Takovýto podpis má pro příjemce nejvyšší vypovídací hodnotu. V dokumentech EU se uvažuje, že by mohl být používán v situaci, kde se v písemné podobě vyžaduje vlastnoruční podpis.V české legislativě by to znamenalo úpravu příslušných zákonů , např. takto … toto musí být podepsáno vlastnoručně nebo pomocí kvalifikovaného podpisu …

“Vylepšený“ elektronický podpis (Enhanced electronic signature)

Tento typ je obecně použitelný s libovolným předchozím typem. Liší se přidáním některého z požadavků (např. časová značka, rozšířené požadavky na verifikaci, rozšířené požadavky na podpisový prostředek, rozšířená ochrana proti jedné konkrétní hrozbě).

Kvalifikovaný podpis určený pro archivaci dat (Qualified Electronic Signature with Long-term Validity)

Nejdůležitějším typem, který vznikl jako vylepšený elektronický podpis z kvalifikovaného podpisu, je kvalifikovaný podpis určený pro archivaci dat.

Tento podpis bude blíže představen v chystaném dokumentu ETSI Policy requirements for CSPs issuing trusted time stamps . Zde budou zformulovaná minima pro požadavky v oblasti bezpečnosti a kvality zabezpečení důvěryhodného ověření dlouhodobých (long-term) elektronických podpisů. Novým základním požadavkem je pojem časového razítka. Tento prvek byl specifikován v dokumentu ETSI Time Stamping Profile (draft ETSI TS 101 861 V.1.1.4).
Vzhledem k tomu, že musí být zajištěna odolnost proti útokům po celou dobu archivace, je v kategorii bezpečný podpisový prostředek vznesen požadavek zvýšené bezpečnosti.

EESSI Standard	**Volba standardu**		
Politika kvalifikovaného certifikátu	Nezveřejnění nebo přímé poskytování politiky	Zveřejnění politiky	**Zveřejnění užívání PBVP**
Formát elektronického podpisu	Elektronický podpis	Elektronický podpis + testování dat	**Elektronický podpis + Testování dat + Časová razítka**
Formát kvalifikovaného certifikátu	**Profil kvalifikovaného certifikátu**		
Časové razítko	**Použití protokolu pro časová razítka**		
Požadavek na bezpečný systém	Nižší úroveň		**Kvalifikovaná úroveň**
Požadavek na bezpečný systém (PBVP)	Nižší úroveň	Kvalifikovaná úroveň	**Vyšší úroveň**

Vzhledem ke specifickým požadavkům je využití zřejmé - dlouhodobá archivace podepsaných elektronických dokumentů. V této souvislosti se připomíná, že pokud tuto službu zajišťuje poskytovatel certifikačních služeb, měl by zajistit i uchování příslušného software, který umožní otevření a zobrazení podepsaných dat i v době, kdy tento software již není běžně používán.

Literatura

Směrnice EU : Directive EU , Evropská komise DG XV - Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures

http://www.ict.etsi.org/eessi/e-sign-directive.pdf

ICTSB – Information and Communications Technologies Standards Board - iniciativa tří evropských standardizačních organizací CEN, CENELEC, ETSI a v oblasti ICT.
ETSI : European Telecommunication Standards Institute
http://www.etsi.org/sec/el-sign.htm
CEN/ISSS : http://www.ni.din.de
http://www.cenorm.be/isss/worksho/e-sign
EESSI : European Electronic Signature Standardization Initiative http://www.ni.din.de
http://www.ict.etsi.org/eessi/EESSI-homepage.htm
ZoEP : Zákon o elektronickém podpisu č. 227/2000 , http://www.uoou.cz
e-zin **Crypto-World** http://www.mujweb.cz/veda/gcucmp

B. **Tiskové prohlášení č.14, Microsoft, 15.2.2001**

NBÚ spolupracuje se společností Microsoft při ochraně dat

Národní bezpečnostní úřad zavádí technologii společnosti Microsoft, která umožňuje ochranu utajovaných skutečností a informací v informačních systémech státní správy včetně elektronického podpisu.

Česká republika dostala prostřednictvím Národního bezpečnostního úřadu (NBÚ) do rukou technologii společnosti Microsoft, která umožňuje implementovat libovolný šifrovací algoritmus do produktů Microsoft i do aplikací třetích stran provozovaných na operačních systémech Microsoft.

Tato technologie byla donedávna embargována a v době, kdy ji NBÚ získal, byla k dispozici pouze v USA a v Kanadě. Česká republika tedy byla třetí zemí na světě, která ji díky snaze české pobočky společnosti Microsoft dostala volně k dispozici.

NBÚ byl vybrán proto, že ze zákona odpovídá za vývoj a certifikaci kryptografických prostředků. Poskytnutá technologie umožňuje NBÚ vyvinout modul, který šifruje nebo elektronicky podepisuje za použití algoritmů, které do něho NBÚ vložil. Tyto algoritmy je možné později měnit nebo je možné k nim přidávat další algoritmy dle potřeb, aniž by bylo nutné měnit aplikace. Licenčně je použití takového modulu omezeno na orgány státu a veřejné správy, přičemž licenční podmínka ze strany společnosti Microsoft zněla, aby byl tento modul poskytován zdarma. Jeho distribuci zajišťuje NBÚ.

Výběrové řízení vyhlášené NBÚ vyhrála českobudějovická firma Decros, s. r. o., jedna z vedoucích firem na českém trhu zabývajících se vývojem a výrobou bezpečnostních produktů. Tato firma spolu s NBÚ vloni úspěšně dokončila vývoj zmiňovaného modulu.

Nyní na NBÚ probíhá certifikace vyvinutého modulu. Dokončení certifikace se očekává v brzké době. Předpokládá se, že vyvinutý modul bude mít certifikaci na stupeň „Vyhrazené“. To znamená, že bude moci být používán v informačních systémech veřejné správy, které zpracovávají utajované informace až do stupně „Vyhrazené“. Za předpokladu splnění dalších požadavků definovaných zákonem a vyhláškami NBÚ ho eventuálně bude možné použít i v informačních systémech certifikovaných pro nakládání s utajovanými skutečnostmi i vyššího stupně utajení. Kontrolu nad zdrojovým textem modulu má NBÚ.

Tento modul je jeden z důležitých prvků při zajištění požadované úrovně bezpečnosti všech zákonem dotčených informačních systémů veřejné správy vybudovaných na základě produktů Microsoft.

NBÚ ve spolupráci s firmou Decros, s. r. o., vyvíjí pro vyšší stupeň utajení další verzi modulu, která je založena na kombinaci softwaru a hardwaru.

Využití se předpokládá v systémech veřejné správy, na internetu nebo intranetu při ochraně komunikace mezi webovými servery a stanicemi, v elektronické poště, v oblasti elektronického podpisu a v informačních systémech, které zpracovávají utajované informace.

C. Kryptografický modul MicroCzech I.

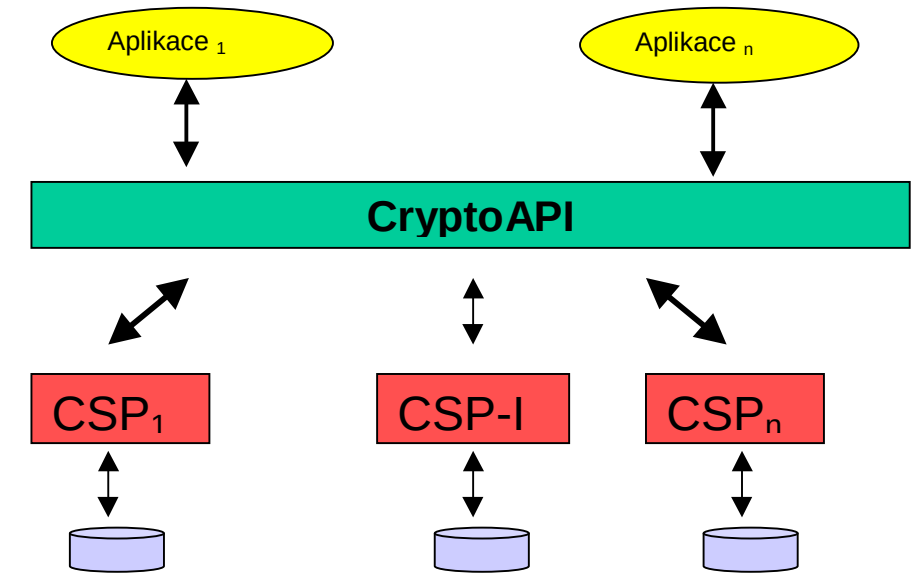
Mgr. Pavel Vondruška, ÚOOÚ

A. Modul CSP-I

V roce 1999 díky snaze české pobočky společnosti Microsoft dostala ČR k dispozici vývojový prostředek, který umožňuje vytvoření vlastního modulu CSP. Tato technologie nebyla v té době určena pro vývoz a byla k dispozici pouze v USA a v Kanadě. Česká republika se stala třetí zemí na světě, která ji dostala volně k dispozici. Národní bezpečnostní úřad se rozhodl ji využít k vytvoření kryptografického modulu, který mimo implementace silné kryptografie bude mít začleněno řadu dalších bezpečnostních vylepšení.

Pracovní název tohoto modulu byl zvolen jako kryptografický modul "CSP-I MicroCzech" (dále jen "CSP-I"). Na základě konkurzu byla k jeho realizaci vybrána firma Decros spol.s r.o.. Tento modul byl pak touto firmou vyvíjen podle zadání a pod dohledem Národního bezpečnostního úřadu. Tým, který vývoj CSP v Decrosu realizoval vedl ing. Rosa, za kryptografii odpovídal mediálně známý český kryptolog Dr.Vlastimil Klíma. Oponenti nejen kontrolovali postup prací, ale svými doporučeními ovlivnili jednotlivé dílčí cíle vývoje a podíleli se na přijetí řady nadstandardních bezpečnostních opatření. Oponenti projektu byli Mgr. Pavel Vondruška (NBÚ), Dr.Bohuslav Rudolf (VTUE), Mgr. Antonín Beneš, Dr. Vojtěch Jákl (oba MFF UK).

Využívání tohoto kryptografického prostředku je určeno pouze pro potřeby orgánů státu. V současné době probíhají závěrečné testy nutné k certifikaci na stupeň utajení "Vyhrazené". Kryptografický softwarový modul CSP-I MicroCzech je určen pro začlenění do subsystému CryptoAPI v prostředí operačního systému Windows NT 4.0. Poskytuje kryptografické služby všem aplikacím, které subsystém CryptoAPI využívají.



Obr. 1 Architektura CSP

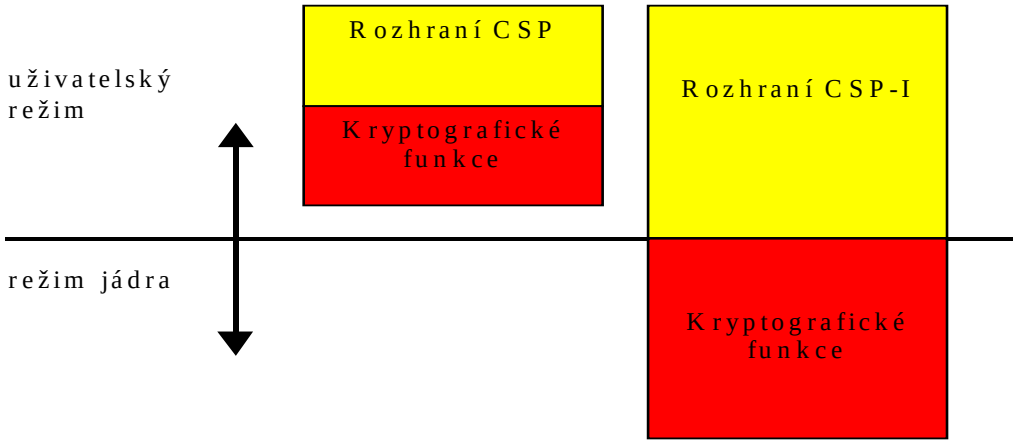
Nejznámějšími takovými aplikacemi jsou produkty firmy Microsoft, jedná se zejména o Outlook a Internet Explorer (MS Outlook 2000 SR1, MS Outlook 2000, MS Outlook 98 , MS Internet Explorer 4.01, MS Internet Explorer 5.0, MS Internet Explorer 5.01). Předpokládá se produkce vlastních aplikací, které tento modul budou používat. Tento Modul by mohl být využit jako základ pro vytvoření bezpečného podepisovacího nebo ověřovacího prostředku, tak jak oněm hovoří Zákon o elektronickém podpisu č.227/2000 v paragrafu 17.

Modul "CSP-I MicroCzech" obsahuje následující druhy kryptografických služeb:
- elektronický podpis (založený na RSA)
- asymetrické šifrování symetrických klíčů (RSA)
  délka RSA modulu: 1024 až 4096 bitů s granularitou 64 bitů
  použitý exponent veřejného klíče RSA: e = F4 = 65537
  použitý standard RSA [PKCS #1], [RSA78], [ANSI X9.31], [FIPS 186-2].
- symetrické šifrování (3DES, RC2, RC4)
  3DES (efektivní délky bez paritních bitů): 112 bitů, 168 bitů
  použitý standard 3DES : [FIPS 46-3], ANSI X9.52
  RC2: délka klíče128 bitů , použitý standard RC2 [RFC 2268]
  RC4: délka klíče 128 bitů [otestována kompatibilita s oficiálním algoritmem RC4, použitým společností Microsoft v Microsoft Enhanced CSP]
- hashovací funkce (SHA-1, MD5, MAC)
  použité standardy - SHA-1: [FIPS180-1] , MD5: [RFC 1321]
- generátor náhodných čísel (typ Yarrow) [Yarrow-160]

Modul "CSP-I MicroCzech" dále implementuje řadu bezpečnostních mechanismů, které nejsou součástí standardně dodávaných modulů CSP. Tyto mechanismy vznikly na základě požadavků NBÚ nebo byly navrženy vývojovým oddělením firmy Decros spol. s r.o. Tyto mechanismy budou probrány v části B.

Poznámka ke vztahu CryptoAPI a CSP

Subsystém CryptoAPI je dodáván společně s Windows NT 4.0. Byl vyvinut za účelem zpřístupnění kryptografických funkcí uživatelským aplikacím. Modul CSP představuje v subsystému CryptoAPI základní výkonný element, který implementuje konkrétní



Obr. 2 Začlenění modulu CSP-I

kryptografické funkce a zajišťuje elementární služby klíčového hospodářství. Klíčové hospodářství je přitom dáno vlastní architekturou CryptoAPI. CSP jako takové musí být CryptoAPI přizpůsobeno. Konkrétní modul CSP řeší prakticky jen otázku uložení asymetrických klíčů a je odpovědný za bezpečnost těchto klíčů.
Softwarová realizace standardního CSP se řeší pomocí implementace dynamického knihovního modulu operačního systému (soubor .dll), který běží v uživatelském módu procesoru (z pohledu CPU Ring 3), kde je volně dostupný pro všechny aplikace operačního systému.

Základní specifičnost CSP-I

CSP-I je bezpečnostní modul, který byl navržen a řešen jako čistě softwarový produkt. Je realizován jako distribuovaný modul, který se skládá z vlastního rozhraní CSP a výkonného kryptografického modulu, který je implementován jako služba jádra operačního systému, tak jak ukazuje obr.2. Veškeré operace s tajným klíčovým materiálem jsou přesunuty z původně uživatelského režimu Ring3 do režimu jádra Ring0. Připomeňme, že do jádra (Ring0) již běžné aplikace nemají přímý přístup.

Hlavní rysy klíčového hospodářství

Jakékoliv CSP tedy i CSP-I, může, vzhledem ke své definici obsahovat:
- nejvýše jeden asymetrický algoritmus pro výměnu klíčů
- nejvýše jeden asymetrický algoritmus pro podpis
- žádný nebo několik symetrických algoritmů pro šifrování přenášených dat
- alespoň jednu hashovací funkci

Konkrétně pro vyvinutý produkt CSP-I platí:
- Každý uživatel má v daném CSP-I jednu nebo více klíčových schránek, která obsahuje vždy jeden pár asymetrických klíčů pro výměnu klíčů (AT_KEYEXCHANGE) a jeden pár asymetrických klíčů pro podpis a ověření podpisu klíčů (AT_SIGNATURE).
-Klíče pro symetrické šifrovací algoritmy jsou generovány pouze dočasně v rámci jednotlivých sezení nad CSP-I (náhodně nebo jako výsledek hashování) a po uzavření CSP-I nejsou uchovávány. To samé se týká importovaných symetrických klíčů.
Páry asymetrických klíčů mohou vznikat pouze generováním v CSP-I. CSP-I neumožňuje ani export ani import privátních částí asymetrických klíčů. Odtud vyplývá, že generování a úschova asymetrických klíčů je jedinou podstatnou částí klíčového hospodářství, kterou CSP-I zajišťuje. Zbytek klíčového hospodářství je potřeba budovat v rámci aplikace, která CSP-I používá.

B.Bezpečnostní rozšíření

Jak již bylo řečeno v úvodu, modul "CSP-I MicroCzech" implementuje řadu bezpečnostních mechanismů, které nejsou součástí standardně dodávaných modulů CSP. Tyto mechanismy zde představíme.

I. Kryptografické ochrany

1. Módy blokových šifer

U symetrických algoritmů jsou standardně definovány 4 přípustné módy. Jsou to ECB, CBC, OFB, CFB. Z hlediska bezpečnosti jsou diskutabilní pouze módy OFB a CFB, kde vyžadujeme z bezpečnostních důvodů zpětnou vazbu pouze v délce 64 bitů. CSP-I sice přijme požadavek na šifrování v uvedených módech se zpětnou vazbou menší než 64 bitů, ale provede zpětnou vazbu v délce 64 bitů. Při pokusu o její změnu ze strany aplikace CSP-I sice nehlásí chybu (z důvodu kompatibility), samotnou hodnotu ale nezmění.

2. Generování prvočísel

Pravděpodobnost, že vygenerované číslo p není prvočíslo, je pro všechny podporované délky modulů menší než 2^{-85}. Pro testování prvočíselnosti kandidátů je použit Miller-Rabinův test.

3. Generování privátního exponentu

Při výpočtu privátního exponentu d k veřejnému exponentu e=F4 a modulu n=p*q se postupuje následovně. Podle normy PKCS#1 se vypočte $d \equiv e^{-1} \bmod (\mathrm{lcm}(p-1,q-1))$, kde lcm(p-1,q-1) je nejmenší společný násobek čísel p-1 a q-1. Dále je z bezpečnostního důvodu zařazena dodatečná kontrola, která zamezuje útokům na nízký exponent RSA. Po vypočítání d podle výše uvedeného vztahu je kontrolováno, zda délka privátního exponentu d je větší nebo rovna třem čtvrtinám délky modulu. Jestliže ne, generuje se prvočíslo q znovu až do té doby, dokud tato podmínka není splněna.

4. Šifrování symetrických klíčů

Standardní CSP používají pro šifrování symetrických klíčů formát PKCS#1, verze 1.5. Proti tomuto formátu byl však nalezen efektivní útok prezentovaný v [CCA-98]. Z tohoto důvodu implementuje CSP-I pro tento účel formát PKCS#1, verze 2.1, který hrozbu zmíněného útoku odstraňuje. Tímto rozšířením je porušena kompatibilita (v oblasti výměny symetrických klíčů) s jinými moduly CSP, které používají verzi 1.5 tohoto formátu. Jedná se tedy o nekompatibilitu ze všemi v současné době komerčně dodávanými CSP. Tato změna zvyšuje výrazně bezpečnost systému a byla provedena na žádost NBÚ.
V oblasti digitálního podpisu, kde není možné zmíněný útok provést, byla ponechána verze 1.5 formátu PKCS#1, takže zde je CSP-I plně kompatibilní s ostatními moduly.

Důsledky přechodu na formát PKCS#1 verze 2.1:
- CSP-I není schopné přijmout klíče, zašifrované jiným CSP, které nepoužívá tento formát.
- Klíče, zašifrované CSP-I, bude schopné dešifrovat jedině CSP s kompatibilním formátem podle nové normy. To je v současné době jen CSP-I. V současné době je tedy možná výměna šifrovaných dokumentů jedině mezi stanicemi vybavenými CSP-I.
- V případě digitálních podpisů se používají podpisy podle staré normy. Z hlediska kompatibility bylo výhodné zde ponechat standardní formát 1.5 tak, aby bylo možné ověřovat digitální podpisy vytvářené různými aplikacemi podle této běžné normy.

5. RNG

V modulu CSP-I byla použita koncepce RNG na bázi rodiny Yarrow, která s ohledem na dostupné zdroje entropie produkuje kvalitní a statistickými metodami nenapadnutelný výstup. Aby byly odhaleny eventuální chyby v produkci tohoto generátoru způsobené například nevhodnou intervencí ze strany ostatních driverů v jádru systému, je aplikován na každou jeho posloupnost test dle FIPS 140-1. Pouze ty bloky, které tímto testem projdou, jsou postoupeny k dalšímu zpracování.

Jako zdroje entropie jsou používány tyto systémové informace :

systémový čas (8 bajtů) , informace o časovačích (8 bajtů), globální seznam synchronizačních objektů (resources, 8000 bajtů). Při reseedování dochází k vytvoření nové hodnoty K na základě staré hodnoty K a vstupu entropie ze systému. SW-RNG využívá jako stavebního prvku algoritmus 3DES se 168 bity klíče K a 64 bitový blok dat C, který slouží jako čítač.

6. Ochrana privátních klíčů uživatele

Asymetrické privátní klíče každého uživatele jsou uchovávány v zašifrovaném tvaru (RC2/128/CBC – Cipher Block Chaining) a dešifrují se pouze na dobu nezbytně nutnou pro provedení příslušné operace. Klíč pro jejich dešifrování zadává uživatel před každým jejich použitím. Přístup ke klíči je zaznamenán v sytémovém logu. Uživatel má tím, že musí zadat své heslo, zároveň i přesný přehled o používání klíče. Je to obrana proti nevyžádanému přístupu ke klíči např. aplikací typu trojský kůň.

Při zadávání hesla (z něhož se deterministicky počítá klíč) pro přístup k privátním klíčům si modul CSP-I zaznamenává počet neúspěšných pokusů o jeho zadání. Úspěšný pokus tento čítač vyprázdní. Pokud tato hodnota během intervalu 16 minut dosáhne pěti neúspěšných pokusů, je přístup k danému privátnímu klíči na 20 minut odepřen. Tyto pokusy jsou zaznamenány v auditu. Tímto způsobem se CSP-I brání slovníkovým útokům na heslo uživatele. Minimální délka uživatelského hesla je hlídána a je stanovena na 8 znaků.

II. Systémové ochrany

1. Dvojúrovňová architektura

Popis tohoto mechanismu, který řádově zvyšuje bezpečnost kódu a vnitřních datových struktur modulu CSP-I, již byl rozebrán v úvodu (viz obr.2).

2. Použití nestránkované paměti

Všechny sensitivní operace probíhají přímo v jádru operačního systému. Pro uložení všech citlivých dat je současně požadována výhradně nestránkovaná paměť. Za předpokladu správné funkce těchto mechanismů v jádře OS (která je pro celý návrh klíčová a implicitně se předpokládá) tak nehrozí nebezpečí, že by se nějaké citlivé informace mohly objevit ve swapovacích souborech.

3. Systémové logy / Audit

Pro včasné odhalení pokusů o útok na modul CSP-I jsou informace o všech potenciálně nebezpečných operacích zaznamenávány do systémových logů. Sledováním těchto záznamů má administrátor systému možnost na takové pokusy včas reagovat nasazením příslušných protiopatření.

4. Přístup ke kontextům

Při otevření daného kontextu (funkce CPAcquireContext) si modul CSP-I zaznamená číslo procesu (PID), který toto otevření provedl, a dále umožní k tomuto kontextu přistupovat pouze procesu se stejným číslem PID. Účelem této ochrany je zabránit neoprávněné manipulaci s obsahem a stavem kontextu jinou aplikací. Jedná se především o ochranu proti útokům typu trojský kůň, které mohou u standardních CSP využívat zejména mechanismu exportu symetrických klíčů.

5. Zákaz exportu privátního klíče

Vzhledem k užitému klíčovému hospodářství představují privátní klíče uživatele nejcitlivější část celého systému. Proto je také jejich ochraně před možnou kompromitací věnována odpovídající péče. Vzhledem k tomu, že současný standard CSP nedefinuje bezpečný způsob pro export/import privátních klíčů, není v CSP-I export privátních klíčů umožněn vůbec. Toto opatření nemá vliv na kompatibilitu s běžnými druhy aplikací (nebyly pozorovány žádné problémy). Naproti tomu tento mechanismus velmi efektivně chrání nejchoulostivější část celého systému před útoky typu trojského koně.

Autor děkuje touto cestou za možnost využít k přípravě referátu technickou dokumentaci prostředku CSP-I Microczech. Z této dokumntace také byly převzaty (po malé úpravě) i oba dva doprovodné obrázky.

Literatura

[A] Kryptografický prostředek CSP-I Microczech - Dokumentace, Decros, 2000
[B] Kryptografický prostředek CSP-I Microczech - Návod k obsluze, Decros, 2000
[C] DECROS Cryptographic Service Provider v 1.0 (SW) - Technická dokumentace, Decros 2000
[D] Oponentní posudky při vývoji CSP-I MicroCzech , Vondruška, (1999-2000)

D. Názor na článek J.Hrubý, I.Mokoš z 2/2001

Mgr. Pavel Vondruška, ÚOOÚ

Autoři Hrubý a Mokoš publikovali v minulém čísle e-zinu Cryptoworld 2/2001 článek „K návrhu zákona o elektronickém podpisu, jeho dopadu na ekonomiku a bezpečnostních hlediscích“ a předložili jej touto cestou k veřejné diskusi. Rád se do této diskuse také zapojím. Autora znám jako odborně fundovaného, zkušeného vědeckého pracovníka. Druhého z autorů osobně neznám. Musím však konstatovat, že tento jejich článek na mne působí dojmem nedokončené práce.

Pokusím se to ukázat na několika vybraných detailech příspěvku.

Prvním příkladem může být tato citace z třetí části článku : "Na poslední konferenci EUROCRYPT 2000 byla ukázána faktorizace RSA-155 s délkou klíče 512 bitů [3], pomocí klasických počítačů a byl vysloven jednoznačný závěr, že RSA s touto délkou klíče již není bezpečná [2].".
Zde je uvedena řada nepřesností . Faktorizace RSA-155 se týkala výzvy k řešení úlohy faktorizace čísla velikosti 155 dekadických cifer, tedy představujícího 512 bitový modul RSA - nikoliv klíč. RSA-155 bylo součinem dvou prvočísel, každé délky 78 dekadických cifer. Jinými použít výraz RSA-155 s délkou klíče 512 bitů je velice "nepřesné". Faktorizace tohoto čísla byla provedena v srpnu 1999 a nebyla "ukázána" na konferenci Eurocrypt 2000. Do této konference byla o tomto významném úspěchu napsána celá řada článků (viz i náš e-zin). Na konferenci Eurocrypt 2000 bylo autory projektu faktorizace RSA-155 , jako velikém úspěchu, pouze veřejně referováno a to v článku [2], nikoliv [3].

Zůstanu-li u faktorizace, pak hned v následujícím odstavci se dočteme, že : "Na tomto převodu pracoval vynálezce TWINKELU prof. A.Shamir společně s vynikajícím odborníkem na faktorizaci A.K.Lenstrou. V současnosti je útočeno na faktorizaci čísel větších než 768-bitů v reálném čase."

O tomto útoku bylo na již zmíněné konferenci Eurocrypt 2000 skutečně referováno a to v práci [2], která však byla autory citována v jiné souvislosti. Také nevím zda tvrzení : "... faktorizaci čísel větších než 768-bitů v reálném čase" , není trochu zavádějící, neboť v článku [2] se píše o hypotetické možnosti, faktorizovat číslo o velikosti 768 bitů (ne čísel větších) a to pomocí 5000 modifikovaných zařízení TWINKLE podporovaných 80 000 počítači a to za dobu přibližně půl roku ....

Podobných nepřesností je v článku celá řada. Např. v kapitole 4 se píše:
"Na konferenci Fast Software Encryption Workshop 2000 publikoval Adi Shamir, Alex Biryukov a David Wagner [15] nový útok na silnější verzi šifrového algoritmu A5/1, který se používá ve 130 milionech GSM mobilních telefonů, včetně ČR."
Odkaz na literaturu je nepřesný. Neodkazuje na nový útok, který je dále popisován , ale na útok předchozí. Dále použitý výraz "silnější verzi šifrového algoritmu A5/1" je opět nepřesný. Správně má být na silnější verzi algoritmu A5 a to algoritmus A5/1.

Na některých místech jsou pravděpodobně chyby vzniklé pouhým přehlédnutím. Ukážeme si to na citaci : "Skutečné nebezpečí představují ty pasivní jako jsou tzv. časované útoky [10]...". Nechce se mi věřit, že by autoři nevěděli, že Timing Attacks se nepřekládá časované útoky, ale "útoky založené na měření času" nebo méně (významově) přesně "časové útoky" . Ostatně termín "časový útok" sami autoři v jiné části článku používají.

Autoři dále používají na několika místech termín "veřejná akreditace". Nevím co tento výraz znamená. Náš platný zákon o elektronickém podpisu č. 227/2000 mluví pouze o akreditaci poskytovatelů certifikačních služeb.

K popisu činnosti poskytovatelů certifikačních služeb (tak jak je uváděno v článku) mám také řadu výhrad, a mám také dojem, že řada tvrzení je zde psána zcela účelově. Jedná se především o výhrady ke větám typu : " Pouze velké firmy v IT s vlastním výzkumem a prostřednictvím svých vysoce kvalifikovaných konzultantů na celém světě disponují hlubokými znalostmi v oblasti PKI...". Jako pracovník ÚOOÚ se však nechci k této části blíže vyjadřovat.

Oběma autorům doporučuji změnit i samotný název článku :
"K návrhu zákona o elektronickém podpisu, jeho dopadu na ekonomiku a bezpečnostních hlediscích.".
Návrh zákona byl již schválen (29.6.2000) a v současnosti by měli tedy psát spíše o "Realizaci zákona o elektronickém podpisu, ..."

Kde s nimi naopak souhlasím, je tvrzení, že téma je vysoce aktuální a bezpečnost služeb, které poskytovatelé certifikačních služeb nabízí je vhodné téma k odborné diskusi. Doporučoval bych zaměřit se na konkrétní detaily. Spíše doporučuji vyjmenovat oblasti, kde již lze systém úspěšně provozovat (on-line komunikace, e-komerce), kde jsou ještě legislativní problémy (akreditace poskytovatelů certifikačních služeb, oblast veřejné moci), kde mohou být objektivní bezpečnostní problémy (časová razítka, dlouhodobá archivace).

Osobně doporučuji vynechat některá témata, která s problémem souvisí jen okrajově (např. kvantové počítače, které jsou sice jistě "katy" celého systému, ale zaslouží si vlastní článek a ne je spojovat s budováním systému EP v ČR, algoritmus A5/1 je také poněkud "z jiného světa" atd.) .

Doporučuji rozšířit použitou literaturu o některé další citace, např. článku, který byl publikován přesně před rokem v našem e-zinu a ze kterého jsou některé odstavce doslova převzaty ("Zákon o elektronickém podpisu otevírá cestu do Evropy ?").

Můj celkový dojem po přečtení příspěvku pak byl asi jako z čtení pohádky "Jak pejsek s kočičkou vařili dort", jinými slovy, autoři jakoby stáli před problémem, co tam mají ještě "vrazit" k podpoře hypotézy, že je celý systém elektronického podpisu nedůvěryhodný, ale na druhé straně na podporu tvrzení, že velké firmy jej dokáží budovat bezpečně (zde již na připomínání kvantového počítače odpadlo).

E. Názor na článek: K návrhu zákona o elektronickém podpisu, jeho dopadu na ekonomiku a bezpečnostních hlediscích (autoři - J.Hrubý, I.Mokoš)

Jaroslav Pinkava, AEC spol. s r.o. & Norman Data Defense Systems

Přes polemický obsah článku vítám jeho zveřejnění na stránkách Crypto-Worldu. Vítám také výzvu autorů k diskusi k tomuto článku. Zcela souhlasím s kritickými formulacemi v úvodu, které konstatují stav problematiky elektronického podpisu v ČR (normy, testovací laboratoře, atd.).

Již v tomto odstavci však najdeme některé sporné formulace, resp. takové, které si vyžadují dalšího objasnění. Např. otázka jednotné kořenové struktury v ČR stojí trochu jinak než ji autor popisuje. Touto cestou je totiž vytvářena struktura certifikačních autorit jen v některých zemích EU, především se to pak týká Německa. Tj. vytváření jednotné kořenové struktury je pouze jednou z možností, rozhodně však nikoliv možností jedinou.

Obdobně z hlediska zmínky (v téže větě) o potřebě jednotných formátů pro elektronické podpisy a vůbec v návaznosti na zmínky o potřebě norem v ČR postrádám odkaz na připravované nebo již dokonce zpracované normativní dokumenty EU (viz např. článek autora v tomto a minulém čísle Crypto-Worldu). Cesta je zde zřejmá a jediná – je třeba převést tyto normy takovou cestou, aby jejich platnost byla v ČR stejná jako v členských zemích Evropské Unie. Nemá totiž smysl vytvářet nějaké zvláštní české normy, velice brzy by se totiž prokázala jejich nekompatibilita s evropskými a to by mohlo vést pouze k jedinému – snížení důvěryhodnosti a využitelnosti oblasti elektronických podpisů pocházejících z České republiky.

Formulace druhého odstavce nelze než podpořit (trochu rušivě zde působí pouze zmínka o kvantové kryptografii). Stěžejní částí článku je ovšem třetí odstavec (*Základy konstrukce elektronického podpisu z hlediska bezpečnostních rizik)*. Zde se autoři pouští do kryptologické problematiky - avšak poněkud nešťastným způsobem. Nad úvodní formulací typu:
„Digitální podpis využívá určitou matematickou vlastnost tzv. asymetrických šifrových systémů, která byla objevena asi před 20 lety. Bezpečnost je založena na složitosti matematické úlohy faktorizace velkých čísel.“ – zakroutí odborník hlavou. Složitost úlohy faktorizace – na jejím základě byly vytvořeny pouze některé konkrétní kryptosystémy s veřejným klíčem (RSA, Rabin-Williams) - rozhodně však není základem bezpečnosti obecné problematiky digitálních podpisů.

Obdobných formulací lze v článku nalézt více a při pečlivější redakci by se jim určitě šlo vyhnout.

To však ale není jádrem obsahu daného článku. Svůj přehled bezpečnostních rizik autoři zahajují uvedením problematiky kvantových výpočtů. Naprosto souhlasím s tvrzením autora, že pokud se podaří prakticky uskutečnit myšlenku kvantového počítače, pak dnešní kryptografie (a nebude se to týkat asi jen zmíněných konkrétních asymetrických systémů) bude stát před svým zánikem. To však asi nenastane hned zítra (reálně dnes existují techniky vytvářející maximálně pětibitové kvantové počítače, více dnešní přístupy neumožňují – pro ohrožení kryptografických algoritmů by však bylo zapotřebí uvést do praxe funkční qubitové řetězce v délce řádově nejméně stovek qubitů). Pokud ovšem tato situace nastane, sama

kvantová teorie nabízí řešení v podobě kvantové kryptografie, která je dnes analyzována celou řadou erudovaných odborníků (mezi ně patří i J. Hrubý). Praxe potom samozřejmě, pokud se tato potřeba přechodu na nové technologie objeví, bude na teorii požadovat zabezpečení plynulosti takovéhoto přechodu. Zatím však stojíme na (relativně) pevných nohách ve světě klasických Turingových počítačů a je tedy nutné vytvářet příslušné bezpečností koncepce na tomto základě.

Pokud se týká dalších připomínek k třetímu odstavci – měl jsem možnost se seznámit s připomínkami P.Vondrušky a samozřejmě s nimi zcela souhlasím (otázky faktorizace, útoky založené na měření času atd.). Opět – paradoxně na obrázku, který má za cíl ilustrovat elektronický podpis je použit pojem digitální podpis atd. Problematika analýzy bezpečnosti systému realizujících funkce CA a jejich „vnoření do informačních systémů organizace“ je nepochybně závažná a pouhý její popis by zasloužil samostatné zpracování. Některé cesty v tomto směru jsou však již v existujících dokumentech EU popsány a bohužel autoři se o nich nezmiňují.

Navazující čtvrtý odstavec se zabývá některými dalšími specifickými bezpečnostními problémy (poukázáno je zde na rozbití algoritmu A5 v GSM, elektronické tunelování). Z připomínek obsažených v těchto dvou odstavcích (3.a 4.) autoři vyvozují (bohužel díky nesourodosti jednotlivých faktů a nepřesným formulacím vážnost argumentace poněkud pokulhává) následující dva závěry:

- v ČR je co zlepšovat v bezpečnosti z pohledu nových výzkumů u již existujících certifikačních autorit
- pouze velké firmy v IT jsou schopny zabezpečit a pokrýt problematiku PKI a certifikačních autorit.

S tímto vyústěním článku nemohu souhlasit (nehledě na to, že druhý a asi z hlediska autorů hlavní závěr působí zcela zjevně lobbysticky, první závěr je pak poněkud nekonkrétní). Problematika elektronických podpisů a jeho praktického používání je problematikou širokospektrální a zcela jistě se netýká jen velkých firem IT. Tím vůbec nechci říci, že je opomíjitelná aktivita takovýchto firem.. Například na zpracování stěžejních dokumentů Evropské Unie v oblasti elektronických podpisů (legislativa, normy) se podílelo a stále podílí celá řada pracovníků významných soukromých podniků (Bull - Francie, Baltimore – Irská republika, id2 technologies – Švédsko, atd.), ale i pracovníků evropských univerzit. Legislativní a normalizované postupy vytvářené touto cestou netvoří pak východiska pro činnost pouze těchto průmyslových kolosů, ale jsou využitelné především pro celé vznikající průmyslové odvětví elektronických podpisů. Nepochybně i Hewlett-Packard je schopný svými zkušenostmi přispět těmto žádoucím aktivitám, ale jeho cílem určitě nemůže být zdůrazňování své výjimečnosti a jedinečnosti. Naopak – pokud však velké firmy svým ekonomickým a znalostním potenciálem přispějí ke komplexnímu rozvoji problematiky elektronických podpisů (např. právě v ČR) – co by mohlo být více žádoucí?

F. Letem šifrovým světem

(z nedostatku času - výjimečně zaměřeno pouze na přehled akcí)

1. Dne 9.3.2001 rozeslal Úřad pro ochranu osobních údajů do mezirezortního řízení návrh vyhlášky o povinnostech poskytovatelů vydávajících kvalifikované certifikáty a o požadavcích, které musí splňovat nástroje elektronického podpisu. Oslovené instituce mají nyní 15 dní na oficiální připomínky ke znění této vyhlášky a Úřad se pak následně musí vypořádat s těmito připomínkami v řádném připomínkovém řízení. Plné znění, včetně zdůvodnění, jsme tentýž den rozeslali čtenářům našeho e-zinu. Znění vyhlášky připravili zaměstnanci úřadu : Mgr. Dagmar Bosáková a Mgr. Pavel Vondruška. Legislativní úpravu provedl JUDr. Ján Matejka. Odborné otázky byly konzultovány se členy Odborné pracovní komise ÚOOÚ, kterou během října 2000 pro tento účel jmenoval předseda Úřadu RNDr. Karel Neuwirt. Členy této komise jsou : Ing. Petr Budiš, Dr. Ing. Petr Hanáček, CSc., Doc. Ing. Jan Staudek, CSc., Ing. Jaroslav Pinkava, CSc., RNDr. Petr Tesař, RNDr. Jaroslav Hrubý, CSc., RNDr. Antonín Beneš, RNDr. Jiří Souček, DrSc., RNDr. Ing. Jiří Peterka, Ing. Cvrček, Ing. Jiří Mrnuštík, CSc. Předkladatelé dále využili připomínek firem, které se podílely na veřejné diskusi, která proběhla po představení prvého návrhu vyhlášky (4.12.2000). Seznam těchto firem je dostupný na http://www.uoou.cz .
   (Doprovodná fotografie k textu je z 28.2.2001 z pořadu ČT 2 "21", kde poslanec Vladimír Mlynář a Mgr. Pavel Vondruška diskutovali o problémech s použitím elektronického podpisu v praxi.)

2. Šestý ročník konference zaměřené na ochranu a bezpečnost dat i na antivirovou ochranu Security 2001 se bude konat 7.června 2001 v Národním domě na Vinohradech. Každý účastník obdrží sborník s texty všech přednášek a dalšími informacemi z oblasti bezpečnosti dat a dále informační CD. Další informace na http://www.aec.cz/ .

3. 27.3.2001 od 16.00 hod pořádá ISACA CRC klubový večer. Místo konání je v konferenčním sále společnosti PricewaterhouseCoopers, Kateřinská 40, Praha 2. Téma večera je : "Ochrana osobních údajů v praxi" .

4. Konference "Bezpečnosť dát 2001" se koná 3.4.2001 v Kongresovém sále hotelu Holiday Inn v Bratislavě. Organizuje AEC Bratislava ve spolupráci se SASIBom. Na konferenci vystoupí i oba dva protagonisté tohoto e-zinu se svými příspěvky : Mgr.Pavel Vondruška představí prováděcí vyhlášku k zákonu o elektronickém podpisu a Ing.Pinkava, CSc. promluví na téma Certifikáty, certifikační autority a struktury PKI.

5. Ekonomický klub Mladých konzervativců pořádá 22.3.2001 v 18.00 hod ve svém sídle ve Zborovské ulici, Praha 5 diskusi na téma "Elektronický podpis a problémy při jeho implementaci". Jedná se o přednášky s následnou panelovou diskusí. Pozvání přijali : Ing. Ondřej Felix, CSc. (SPIS, Oracle), Ing. Petr Budiš (I.CA), Mgr.Pavel Vondruška (ÚOOÚ), Ing. Michal Faltýnek (Ministerstvo financí), Ing. Miroslav Vaněk (náměstek ministra práce a sociálních věcí), RNDr. Ivo Hrkal (MV ČR).

6. Do 15.3.2001 (!) je potřeba zaslat registraci na nejvýznamnější evropské setkání kryptologů - konferenci Eurocrypt´2001 (Innsbruck, Rakousko). po tomto datu je registrační poplatek zvýšen o USD 80. Další informace na http://www.iacr.org

7. Dne 5.3.2001 proběhlo zasedání EESSI, skupiny 12 (Advanced Electronic Signature) v Paříži. Zasedání se věnovalo především otázkám bezpečného podpisového prostředku, fungování poskytovatelů certifikačních autorit a hlavně připravovaným projektům využívajícím elektronický podpis. Jediným zástupcem mimo EU byl Mgr.Pavel Vondruška. Díky tomu plánujeme v našem e-zinu exkluzivní článek věnovaný přehledu plánovaných nejdůležitějších projektů elektronického podpisu v EU.

8. Brněnská společnost SkyNet oznámila vznik výhradního autorizovaného centra ČR a SR pro produkty PGP společnosti Network Associates (NAI). Produkty PGP tvoří ucelenou stavebnici pro řešení šifrování a elektronického podepisování souborů elektronické pošty, ochrany připojení do Internetu a nástroje na management virtuálních privátních sítí. Tato společnost v březnu 2001 představí server http://www.nai.cz , na němž nabídne lokalizované servisní programy pro podporu programů firmy NAI.

9. O čem jsme psali před rokem ?
   Crypto -World 3/2000
   http://www.mujweb.cz/veda/gcucmp/casop2/Crypto3_00.html

   A.Nehledá Vás FBI ?
   B.Aktuality z problematiky eliptických křivek v kryptografii
   C.Hrajeme si s mobilním telefonem Nokia
   D.Tiskové prohlášení -
   Pozměňovací návrhy k zákonu o elektronickém podpisu bude projednávat hospodářský výbor Parlamentu
   E.Digital Signature Standard (DSS)
   F.Matematické principy informační bezpečnosti

G. Závěrečné informace
1. Sešit

Crypto-World je oficiální informační sešit primárně určený pro členy "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Adresa URL , na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://www.mujweb.cz/veda/gcucmp .

Pokud se zajímáte pouze o sešit Crypto-World, můžete použít lépe dostupnou adresu:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Pokud máte zájem o zasílání tohoto sešitu, můžete se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@uoou.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@uoou.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků, informace
pavel.vondruska@uoou.cz alias **vondruskap@uoou.cz**

pavel.vondruska@post.cz