Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 1/2007 **15. leden 2007**

1/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1290 registrovaných odběratelů)

Obsah : str.

A. Osobní doklady x identifikace, autentizace, autorizace

RNDr. Libor Dostálek, Siemens, (libor.dostalek@siemens.com)
Mgr. Michal Hojsík, Siemens, (michal.hojsík@siemens.com)

Abych byl zcela upřímný, tak celý život mám problémy se slovy identifikace, autentizace a autorizace. Jelikož jsem se nad jejich přesným vymezením asi nikdy nezamýšlel, tak jsem je i často zaměňoval. Čím o tom dnes ale více přemýšlím, tak je mi to stále nejasnější. A tak jsem se podíval do encyklopedie. Až na anglické verzi Wikipedie jsem našel uspokojivé vysvětlení (volně parafrázuji):

- **Identifikace** je přiřazení známé veličiny neznámé entitě, takže se sama stane známou. Zmíněná známá veličina se nazývá identifikátorem (často označovaným ID) přičemž se požaduje, aby identifikátor byl jedinečný alespoň v rámci sféry své působnosti. Jako ID může sloužit např. rodné číslo (nyní nediskutujeme o tom, že rodná čísla u nás zdaleka nejsou jedinečná).

- **Autentizace** je proces stvrzující, že něco je pravé (autentické). Autentizace objektů zpravidla znamená potvrzení jejich původu, autentizace osob zase znamená ověření jejich identity.
  V případě autentizace osob rozlišujeme následující způsoby (faktory) autentizace:
  - Autentizace na základě toho, že člověk něčím je. Tím se zpravidla míní, že má nějaké biometrické vlastnosti (např. otisky prstů).
  - Autentizace na základě toho, že něco má (např. občanský průkaz).
  - Autentizace na základě toho, že něco zná (např. heslo či PIN).
  - Někdy se ještě samostatně uvádí autentizace na základě toho, že něco umí (např. vytvořit jedinečný rukou psaný podpis).

  Pokud se využije kombinace několika způsobů autentizace, pak se hovoří o vícesložkové autentizaci.

- **Autorizace** je proces přiřazující osobě, programu nebo zařízení přístupová práva k datům nebo rozsah funkcionality poskytované služby.

Zásadní problém tedy není s autorizací, ale s rozlišování mezi identifikací a autentizací. I vzpomněl jsem si na detektivky, kde přece často žádají o identifikaci těla. Takové tělo nehybně leží na patologii a jeho blízcí ho jdou identifikovat. Kdežto pokud tělo ještě bylo živé, tak se např. pro přihlášení k počítači autentizovalo. V detektivkách se přitom nepíše jen o identifikaci těl, ale i o identifikaci pachatelů, kdy svědek vybírá (identifikuje) pachatele ze skupiny představených lidí.

Udělal jsem si z toho závěr, že identifikaci člověka provádí jiná osoba (pokud možno nezávislá) nebo tato osoba při identifikaci alespoň asistuje jako svědek. Kdežto autentizaci provádí uživatel sám vůči nějakému autentizačnímu programu (systému). Přičemž jak identifikaci osob, tak jejich autentizaci je možné provádět na základě toho čím jsou, co mají, co znají či co umí. V případě autentizace musíme vždy brát v úvahu, že uživatelé mohou autentizační systém testovat a hledat cesty, jak nad ním vyzrát. Nemusím tedy ani připomínat mnohé články popisující například různé metody k podvržení otisků prstů (např. pomocí kopie otisku prstu vytvořené ze žvýkacích medvídků apod.).

Osobní doklady
Termín osobní doklady je hovorovým termínem. Zpravidla se tím míní:

- Cestovní doklady, tj. cestovní pasy a víza.
- Občanské průkazy a průkazy je nahrazující
- Řidičské průkazy
- Průkazy pojištěnce apod.
- …
- Ostatní průkazy, kterými jsou zejména průkazy opravňující ke vstupu do firmy či úřadu.

Osobní doklady rozhodně původně sloužily k identifikaci. S rozvojem elektronických služeb se nám do osobních průkazů postupně dostává čip. Ten slouží převážně k :

- Zdokonalení identifikace
- Umožňuje autentizaci v rámci nadstavbových elektronických služeb.

Klasický osobní doklad zpravidla obsahoval:

- Fotografii držitele, která slouží k ne-elektronické identifikaci držitele, pročež má jiné charakteristiky než fotografie sloužící k elektronické identifikaci/autentizaci držitele (držitel se na ni např. může i usmívat).
- Identifikační údaje (jméno, příjmení, adresa, rodné číslo apod.).
- Ochranné prvky

Otázkou je, jaké údaje obsahuje čip, který se nám postupně vloudil do osobních dokladů. Pomineme skutečnost, že i na čipu zpravidla budou i identifikační údaje vytištěné na dokladu, tak je zajímavé, že v čipu je v každých dokladech něco úplně jiného.

Začněme občanskými průkazy. I když v našich občankách dosud čip není, tak v okolní Evropě se i občanské průkazy začínají vydávat ve tvaru kontaktní „kreditní karty“ dle ISO 7816-1. Některé severské země včetně Estonska s tím začaly. Jejich motivací bylo umožnit občanům elektronický styk se státní správou a samosprávou za využití zákona o elektronickém podpisu. Výsledkem bylo, že na čipu byly dva soukromé klíče a certifikáty jim příslušných veřejných klíčů. Jedna dvojice veřejný/soukromý klíč slouží k elektronickému podpisu a druhá k autentizaci. Přičemž soukromý klíč sloužící k elektronickému podpisu je uložen v takovém adresním prostoru karty, který není dostupný zvenku, tj. je neimportovatelný i neexportovatelný. Jedná se tedy o klasické kontaktní PKI čipové karty.

V poslední době se do osobních dokladů začínají ukládat biometrické údaje držitele. Přičemž španělské občanské průkazy mají údajně už obsahovat i otisky prstů. Využití biometrie přitom nikterak nevylučuje i využití PKI. Naopak specifické PKI je využíváno i pro biometrii.

Jak to tedy s tou biometrii je? V podstatě existují tři typy systémů biometrických údajů v čipu dokladu:

- **přímá** biometrická identifikace čipem, kdy dochází k porovnávání biometrických údajů přímo čipem,
- **nepřímá** biometrická identifikace, kdy k porovnávání biometrických údajů dochází mimo čip,
- **centralizovaný** systém.

Přímá biometrická identifikace čipem
Tuto metodu specifikuje standard ISO 7816-11 (Osobní autentizace pomocí biometrických metod). Při této metodě je vzor biometrických údajů (např. otisk prstu) uložen v čipu tak, aby ho nebylo možné exportovat (obdobně jako soukromý klíč pro elektronický podpis).
Ověření pak probíhá tak, že sejmutý vzorek se zašle do čipu, který provede verifikaci. Pokud čip vzorek ověří s kladným výsledkem, pak otisky patří držiteli čipu. Čip může být např. vložen do čipové karty, na které jsou personalizovány identifikační údaje držitele.

Tento systém bude údajně využit ve španělských občanských průkazech. V komerční praxi se tato metoda používá i v zaměstnaneckých průkazech, kdy se pomocí čipové karty nesoucí vzory otisků prstů můžeme přihlašovat do operačních systémů (např. Microsoft) či vstupovat do budov.

Důležité je, že tento systém (pakliže je správně nastaven) neumožňuje útočníkovi získat vzor otisku prstu.

Nepřímá biometrická identifikace
Biometrické údaje jsou uloženy v datové struktuře (datovém objektu) v čipu. Při ověření se tato datová struktura z čipu překopíruje do aplikace, která provede verifikaci. Čip tedy slouží pouze jako nosič dat. Otázkou je pravost datové struktury se vzorem biometrických údajů. Ta může být stvrzena elektronickým podpisem důvěryhodné strany (např. výrobcem dokladů).

Tento systém má dvě základní nevýhody:

- Datovou strukturu s biometrickými údaji je možné zkopírovat a uložit do databáze či do jiného čipu. Hrozbou je tedy např. v kopírování čipu. Protiopatřením je pak autentizace čipu. Což lze realizovat např. za využití Diffie-Hellmanových čísel. Soukromé číslo se uloží do neadresovatelné části čipu a veřejné do zmiňované elektronicky podepsané struktury s biometrickými údaji. Pomocí DH algoritmu je pak možné ověřit pravost čipu, která je založená na držení soukromého DH čísla.

- Přístup k osobním biometrickým údajům při jejich porovnávání. Aplikace může osobní biometrické údaje nejenom využít k jejich porovnávání, ale i uložit do vlastní databáze, tj. zneužít. Protiopatřením je autentizace čtečky, tj. umožnění přístupu ke zmíněné datové struktuře jen oprávněným aplikacím. Tuto autentizaci je možné provádět např. na bázi specializovaného PKI.

Tento systém je využit v evropských cestovních pasech. Pro komerční praxi je metoda asi příliš komplikovaná a tedy i příliš nákladná.

Centralizovaný systém
Tento systém udržuje biometrické údaje na serveru. Uživatel tedy s sebou teoreticky nemusí nosit ani čip. Stačí přijít a nasnímat své biometrické údaje a systém jej přihlásí, otevře dveře apod. Takové systémy jsou nejlákavější, ale také nejspornější. Jsou vhodné pro identifikaci ale sporné pro autentizaci.

Nasazení těchto systémů pro autentizaci je účelné zejména v případě, kdy cena za přívětivost systému je vyšší než možné hrozby. Jako příklady lze uvést přístupy do garáží a méně chráněných prostor, využívání služeb v zábavných centrech, identifikace pacientů v zdravotnických centrech před vydáním léků či před zdravotnickým zákrokem apod.

Centralizovaný systém může být kombinován s něčím, co uživatel má (čipová karta, letenka apod.). Taková vícesložková autentizace pak může být využita např. pro řízení přístupu do budov (nejenom do garáží), k odbavování na letištích apod.

Centralizovaný systém bude využit pro schengenská víza, tj. pro vízové cizince přijíždějící do EU. Žadatelům budou pro účely víz kromě fotografie snímány také otisky všech deseti prstů. Identifikace na hranicích pak může proběhnout vůči libovolnému prstu.

Ochrana osobních údajů

Velice zajímavá je otázka ochrany osobních údajů. V případě evropských cestovních pasů mohou být biometrické údaje dlouhodobě uloženy jen v čipu. V centrálních systémech mohou být uloženy jen v případě pasů 60 dnů, tj. na dobu výroby a případné reklamace pasu. Obávám se, že to nebude platit např. při vstupu do USA. Tj. mé osobní biometrické údaje budou muset být v Evropě nejpozději do 60 dnů zničeny, ale pokud pojedu do USA, tak si je tam pěkně uloží do databáze a pokud se mi to nebude líbit, tak mi jistě odpoví, že tam přece jezdit nemusím. Určitě to využijí autoři detektivek.

Jenže Evropa se vůči svým vízovým cizincům bude chovat stejně, protože vízoví cizinci budou mít své biometrické údaje uloženy dlouhodobě v Bruselu.

Identifikace a autentizace

Biometrické údaje v osobních dokladech zásadně slouží k identifikaci držitele. Avšak stále více se např. hovoří o bezobslužných odbavovacích pracovištích na letištích apod. Bezobslužná pracoviště ale podle mne znamenají již autentizaci. Docela mne zajímá, jakými dalšími opatřeními budou tato bezobslužná pracoviště disponovat (např. televizní okruhy snímající, čím se vlastně uživatel autentizuje).

Závěr

Následující tabulka obsahuje shrnutí pro jednotlivé osobní doklady v EU:

	Čip	**Biometrie**	**PKI**
Občanský průkaz	V některých zemích	Zpravidla ne, ale údajně např. ve Španělsku se počítá s přímou identifikací	Pokud obsahují čip
Cestovní pasy občanů EU (mimo GB a Irska, kde mají vlastní standardy)	Ano	Nepřímá identifikace	Specializované PKI pro podporu biometrie
Schengenská víza	Ne	Centralizovaný systém	Ne

B. Bezpečnost elektronických pasů, část II.

Zdeněk Říha, Masarykova Univerzita a JRC EC Ispra, (zriha@fi.muni.cz)
Petr Švenda, Masarykova Univerzita, (xsvenda@fi.muni.cz)
Václav Matyáš, Masarykova Univerzita, (matyas@fi.muni.cz)

V prvé části [4] jsme diskutovali vlastnosti elektronických pasů první generace, tedy těch pasů, které jsou vydávány v současné době a které obsahují biometrická data jen ve formě snímků obličeje držitele (uložených v DG2). Biometrické systémy založené na srovnávání obličejů jsou však značně chybové a pro přesvědčivější a přesnější verifikaci (případně identifikaci[1]) osob je nutné využít jiných (silnějších) biometrických technologií. Standardy organizace ICAO v oblasti elektronických pasů podporují ukládání otisků prstů (DG3) a snímků očních duhovek (DG4). Jejich uložení v pasech je zatím na celosvětové úrovni dobrovolné. Evropská komise však ve svém rozhodnutí K(2005) 409 rozhodla, že nejpozději od 28. června 2009 musí členské státy ukládat do elektronických pasů i otisky prstů ve formátu WSQ (ztrátová komprese optimalizovaná pro snímky otisků prstů).

Biometrická data ve formě otisků prstů nebo snímků duhovek jsou považovány za citlivější údaje než snímky obličejů, a to z důvodu jejich podstatně přesnějších identifikačních možností. Standardy ICAO proto doporučují dodatečná ochranná opatření pro přístup k těmto citlivým datům a rozhodnutí Evropské komise, které nařizuje ukládání otisků do elektronických pasů, činí ochranná opatření (tzv. rozšířené řízení přístupu) povinnými. Jak však tato ochranná opatření vypadají? Standardy ICAO jsou v této oblasti značně vágní a detaily nechávají na jednotlivých státech. Jen jako příklad uvádějí šifrování dat nebo rozšířené řízení přístupu pracující na stejném principu jako základní řízení přístupu s tím, že symetrický autentizační klíč je tajný [1]. V některých dokumentech zmiňují dokumenty ICAO i rozšířené řízení přístupu založené na PKI, žádné detaily však nejsou rozpracovány. Prvotní rozhodnutí Evropské komise vyžadující ochranu citlivých dat v pasech (K(2005) 409) žádné bližší detaily o rozšířeném řízení přístupu neuvádí, další rozhodnutí Evropské komise v této oblasti (K(2006) 2909) se jen odkazuje na technickou zprávu německého BSI [3]. Tato technická zpráva od té době doznala několika změn a řada detailů protokolu se stále diskutuje.

Pojďme se nyní podívat na jednotlivé teoretické možnosti ochrany citlivých biometrických dat v elektronických pasech. Nejdříve krátce zmíníme dva fundamentální přístupy k celému problému: on-line a off-line přístup. Principielním rozdílem mezi základním řízením přístupu a dodatečnou ochranou citlivých biometrických dat je okruh autorizovaných subjektů, které mají mít přístup k daným datům. Zatímco u základních dat uložených v elektronických pasech je nutné umožnit přístup pohraničníkům všech zemí včetně těch nepřátelských a klíč tak nemůže být skutečně utajen (a u základního řízení přístupu je autentizační klíč v podstatě vytištěn v pase, viz minulý díl), u ochrany citlivých biometrických údajů je okruh subjektů s přístupem značně omezen a tak je možné přístupové klíče lépe chránit a umožnit přístup právě cílové skupině autorizovaných subjektů. Tuto skupinu navíc definuje právě vydavatel dokumentu. Pro přístup k citlivým biometrickým datům jsou tedy nutná tajná autentizační

[1] Jak státy naloží s biometrickým daty získanými pro uložení do pasu je jejich rozhodnutí, na celoevropské úrovni však žádná centrální databáze nevzniká. Česká republika otisky prstů po jejich uložení v pase po krátké době z ostatních úložišť maže, otisky prstů tak lze využít pouze k verifikaci držitele pasu, identifikace osob není možná.

data a nejrůznější metody ochrany biometrických dat v pasech se vlastně zabývají správou těchto tajných klíčů. V principu existují dvě metody správy tajných klíčů a podle typu přístupu ke klíči se nazývají on-line a off-line metody.

V případě on-line režimu jsou tajné klíče (ať už tajné symetrické nebo soukromé asymetrické) umístěny na centrálním serveru (nebo několika málo serverech). Výhodou je relativně snadná ochrana těchto klíčů, neboť chránit je třeba jen několik takových lokalit a při budování takovýchto centrálních bodů je možné s výhodou využít již existujících zabezpečených lokalit. Nevýhodou je nutnost on-line připojení všech inspekčních systémů. To znamená nejen zvýšené náklady na připojení všech míst, kde se budou pasy kontrolovat (navíc v případě některých vzdálených lokalit to může být až neřešitelný problém (například některé ostrovy)), ale také kompletní závislost na tomto připojení. V případě výpadku připojení inspekčního systému k centrálnímu serveru s klíčem nemá inspekční systém žádnou možnost čtení citlivých biometrických dat z pasů. Je zřejmé, že výpadky připojení mohou být způsobeny i úmyslně a připojení je pak kritickým prvkem celého systému. V případě off-line systémů jsou všechny nutné tajné klíče uloženy v každém inspekčním systému, což znamená nezávislost na centrálním systému, ale problém s ochranou tajných klíčů na velkém množství míst (a zvýšenou možnost kompromitace klíčů). Možné jsou i kombinace obou přístupů, pak se kombinují výhody i nevýhody obou přístupů.

Pojďme se nyní podívat na možné principy ochrany citlivých biometrických dat v pasech.

Symetrické metody

V případě využití symetrických šifrovacích metod můžeme buďto data v pase ukládat nešifrovaně a přístup k nim vázat na autentizační schéma založené na symetrické šifře nebo data šifrovat, ukládat šifrovaně a pak se již nestarat o přístup k nim.

Symetrický klíč musí být jiný pro každý pas, klíče mohou být buďto zcela náhodné nebo odvozené z hlavního klíče pomocí nějakého diversifikačního algoritmu (například zašifrováním čísla dokumentu pomocí hlavního klíče získáme klíč specifický pro tento pas). V každém případě potřebujeme minimálně jeden klíč pro každý stát, pravděpodobněji jeden klíč pro každého vydavatele pasu (např. kraje, ambasády apod.) a klíč by měl být pravidelně (např. měsíčně, ročně) aktualizován (pro aktuálně vydávané pasy). Inspekční systém pak musí mít přístup ke všem klíčům nutným pro přístup ke všem platným pasům (tj. až deset let) řady zemí. U off-line systémů se jedná o velké množství velice citlivých klíčů, které by musely být ukládány v každém inspekčním systému a kompromitace byť i jediného inspekčního systému by znamenala okamžitý i budoucí přístup útočníka k biometrickým údajům všech pasů platných v době krádeže. U on-line systémů jsou klíče dobře fyzicky chráněny, chránit je však nutné i přístup k centrálnímu systému, v případě incidentu s neautorizovaným přístupem k serveru je však zotavení snadné – stačí ukončit možnost neautorizovaného využití sítě.

Výhodou symetrické autentizace nebo šifrování jsou malé nároky na výpočetní sílu čipu v pase. Symetrická autentizace je součástí základního řízení přístupu (BAC), rozšířené řízení přístupu by pak bylo zcela stejné, jen založené na klíči, který je skutečně tajný. V případě ukládání šifrovaných dat nejsou nároky na čip žádné, neboť pro pas jsou šifrovaná data transparentní a přístup k nim nemusí nijak řídit. V případě, kdy jsou tajné klíče udržovány v tajnosti (což však není triviální), je takové řešení bezpečné.

Nevýhodou je velké množství klíčů, které je třeba uchovávat v tajnosti (u off-line řešení dokonce na každém koncovém inspekčním systému). Tajné klíče navíc mají dlouhou dobu platnosti/použitelnosti a není možné je revokovat (neboť se nacházejí ve velkém množství pasů). Získání takových klíčů znamená přístup ke všem dosud vydaným pasům. Bezpečnostní nevýhodou šifrovaně ukládaných dat bez ochrany řízením přístupu je možnost získání šifrovaných dat a provádění off-line útoků (třeba i paralelních), což je samozřejmě podstatně mocnější zbraň než provádění on-line útoků na autentizaci vůči pasu. Při vhodně zvolené délce šifrovacího klíče a šifrovacího algoritmu by to však neměl být problém tak jako tak.

Asymetrické přístupy

Jinou možností je provést autentizaci čtečky pomocí autentizace založené na PKI. Cílem je limitovat počet tajných (soukromých) klíčů na straně čtečky a limitovat možnost zneužití těchto klíčů v případě jejich kompromitace. Ačkoliv možností, jak implementovat rozšířené řízení přístupu pomocí PKI, by mohlo být více, budeme se zde držet návrhu německého BSI [3].

Podle tohoto návrhu (pro tzv. autentizaci terminálu) každá země zřídí CV (Country Verifying) certifikační autoritu, která bude vydáváním certifikátů určovat kdo (které jiné země) bude mít přístup k citlivým biometrickým datům této země. Certifikát této autority je uložen v pase a je počátečním bodem (kořenovým certifikátem) řízení přístupu. Dále země, které budou chtít přistupovat k citlivým biometrickým údajům (ať už ve vlastních pasech nebo pasech jiných zemí), musí zřídit DV (Document Verifier) certifikační autoritu. Ta získá certifikát od všech zemí, které ji dovolí přistupovat k datům v jimi vydávaných pasech. Tato DV CA pak bude vydávat certifikáty koncovým entitám přistupujícím k biometrickým datům (tzv. inspekčním systémům – IS).

V pase je pak uložen CVCA certifikát vydávající země (např. ČR). Pokud čtečka (například italská) chce přesvědčit pas o tom, že je autorizovaná pro přístup k citlivým biometrickým datům, musí ukázat certifikát DV (v našem případě Itálie) podepsaný správnou vydávající CVCA (tedy českou) a svůj IS certifikát (pro toto konkrétní zařízení) podepsaný DV certifikační autoritou (v našem příkladě italskou). Jakmile pas celý tento certifikační řetěz ověří, musí ještě zjistit, zda inspekční systém (čtečka) má k dispozici soukromý klíč, jehož veřejná část je certifikována. To se provede pomocí protokolu výzva-odpověď. Pokud toto vše proběhne v pořádku, může následně čtečka přistupovat k citlivým biometrickým datům (tedy DG3 a/nebo DG4).

Výše uvedený postup je mírně komplikován aktualizacemi CVCA certifikátů, pro které se vydávají tzv. linkovací certifikáty (pokud má pas uložen starý CVCA certifikát, je třeba nejprve předložit (a v pase verifikovat) překlenovací linkovací certifikáty). Kromě autentizace terminálu německý návrh dále zavádí autentizaci čipu, která jednak odstraňuje nevýhodu malé entropie BAC (a tedy dešifrovatelnosti komunikace), neboť výsledkem je nový šifrovaný kanál, a jednak také nahrazuje aktivní autentizaci, neboť při ní je ověřen přístup k čipu k tajné informaci (jejíž veřejná část je uložena v DG14 a je tedy součástí digitálního podpisu dat v pase). Pojďme se nyní podívat na jednotlivé protokoly podrobněji.

Autentizace čipu

Inspekční systém získá z čipu pasu veřejnou část Diffie-Hellman (podporovaný je klasický DH podle PKCS #3 a DH založený na eliptických křivkách podle ISO 15946) klíčového páru spolu s doménovými parametry (uloženo v DG14). Dále inspekční systém vygeneruje svůj dočasný (právě pro jedno sezení platný) DH pár klíčů (se stejnými doménovými parametry jako klíč čipu) a pošle jej čipu (příkazem Manage Security Environment – Set for Computation – Key Agreement Template). Jak čip, tak i inspekční systém nyní na základě údajů, které mají k dispozici, mohou odvodit sdílené tajemství. Toto tajemství se využije ke konstrukci klíče (resp. klíčů – pro šifrování a MAC) sezení, který bude použit pro zabezpečení následné komunikace přes Secure Messaging (a SSC (Send Sequence Counter – čítač zpráv použitý pro zabránění přehrání zpráv) se nyní nuluje). Znalost správného klíče se tedy potvrdí možností následné úspěšné komunikace.

Výsledkem je ustavení nového šifrovacího kanálu (odstraňuje se tak nedostatečnost BAC) a autentizace čipu (nahrazuje se tak aktivní autentizace, pas však přesto může aktivní autentizaci podporovat, aby bylo možné ověřit autenticitu čipu i na systémech, které nejsou kompatibilní s rozšířeným řízením přístupu a podporují pouze protokoly standardizované organizací ICAO).

Autentizace terminálu

Během autentizace terminálu musí čtečka (inspekční systém) přesvědčit čip v pase, že je autorizována pro přístup k citlivým biometrickým datům. Počáteční bod důvěry je certifikát CVCA, který je do pasu nahrán při jeho personalizaci. Při autentizaci terminálu musí čtečka pasu předložit certifikační řetěz, začínající certifikátem CVCA v pase uloženým a končícím certifikátem inspekčního systému (odesílá jej příkazy Manage Security Environment – Set for verification – Digital Signature Template a Perform Security Operation – Verify Certificate). Tento certifikační řetěz může v případě potřeby obsahovat i linkovací certifikáty, v takovém případě pas (po jejich ověření) aktualizuje CVCA certifikát za nový (vzhledem k možnému překrytí časové platnosti CVCA certifikátů mohou v jeden okamžik být platné i dva CVCA certifikáty, v takovém případě jsou jako aktuální uloženy oba). Ostatní certifikáty (tedy certifikát pro DV vydaný CVCA a pro IS vydaný DVCA) jsou po ověření ukládány jen dočasně a slouží pouze k ověření celého certifikačního řetězce. V případě úspěšného ověření řetězce pas získá veřejný klíč inspekčního systému a jeho přístupová práva. Ta jsou v současném návrhu pouze dvě a to přístup k DG3 (otisky prstů) a DG4 (oční duhovka). Výsledná práva se získají jako bitové AND těchto práv v celém certifikační řetězci.

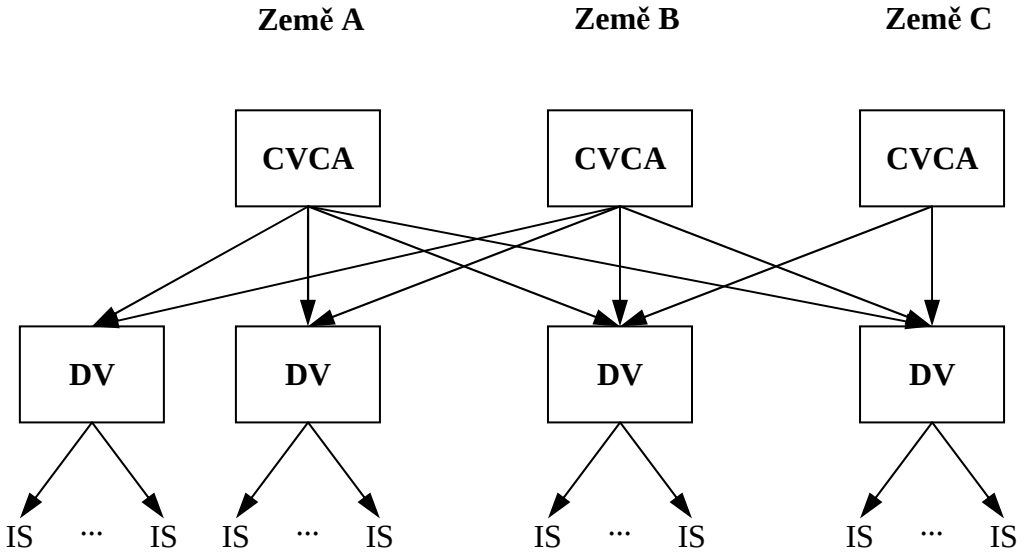
Po získání veřejného klíče inspekčního systému je třeba ověřit, zda inspekční systém má přístup k odpovídajícímu soukromému klíči. To provedeme pomocí protokolu výzva-odpověď. Nejprve inspekční systém získá 8-bajtovou náhodnou výzvu (příkazem GET CHALLENGE), tu digitálně podepíše (podepisuje ve skutečnosti zřetězené číslo pasu, náhodné číslo čipu a haš dočasného DH klíče čtečky (z předchozí autentizace čipu)) a příkazem EXTERNAL AUTHENTICATE posílá čipu k verifikaci. Pokud proběhne verifikace úspěšně, je čtečka autentizována a může přistupovat k DG3 nebo DG4 podle vypočítaných přístupových práv. Předpokladem autentizace terminálu je provedená

autentizace čipu. Autentizace terminálu není povinným prvkem komunikace s pasem. Pokud nezamýšlíme číst z pasu citlivá biometrická data, můžeme autentizaci čtečky vynechat.

Pro autentizaci terminálu jsou podporována následující schémata: RSASSA-PKCS#1_v15 (v kombinaci s SHA-1 a SHA-256), RSASSA-PSS (v kombinaci s SHA-1 a SHA-256) a ECDSA (v kombinaci s SHA-1, SHA-224 a SHA-256). Teoreticky je možné pro jeden pár klíčů vydat certifikáty různých CVCA, DV a tím minimalizovat celkový počet párů klíčů a certifikátů. Různé pasy/CVCA však mohou využívat jiných podpisových schémat a tak teoretický maximální počet klíčů, který může být umístěn na inspekčním systému je dán počtem povolených schémat, tedy 7.

Protože výpočetní síla čipových karet je omezená, jsou místo klasických X.509 certifikátů používány certifikáty zjednodušené, tzv. kartou verifikovatelné (card verifiable – CV) certifikáty. Zajímavé je ověřování časové platnosti certifikátů. Čip totiž nemá vlastní hodiny a tak jediné, co mu zbývá, je využít datum vydání certifikátů. Pokud čip úspěšně ověří platnost certifikátu vydaného určitého dne, ví, že toto datum už jistě nastalo, a může tak aktualizovat svůj časový odhad na tuto hodnotu (tedy pokud je novější, než hodnota dosud uložená). Je zřejmé, že pokud by nějaká CV CA nebo DV CA vydala (ať už omylem, cíleně nebo jako výsledek nějakého útoku) certifikát s datem vydání v budoucnosti, pas by pak odmítal i aktuální certifikáty a byl tak prakticky nepoužitelný. Z důvodu rizika takových útoků se pro aktualizaci interního odhadu data používají pouze CVCA, DV a domácí IS certifikáty.

PKI



Jak již bylo zmíněno, zřizuje každá země CV CA a ta pak určuje, které jiné země budou mít přístup k datům v pasech vydávaných touto zemí. Každá země, která chce přistupovat ke chráněným datům, musí zřídit DV CA a požádat CV CA všech zemí, k jejichž chráněným datům chce přistupovat, o vydání certifikátu touto CV CA pro DV CA. DV CA pak vydává certifikáty jednotlivým inspekčním systémům, kterých mohou být například desítky až tisíce. Pokud se někdo neautorizovaně zmocní inspekčního systému, může pomocí něho číst data z chráněných pasů a to z pasů zemí, pro které daná DV CA získala certifikát od CVCA a po dobu platnosti certifikátu tohoto inspekčního systému (resp. u málo používaných pasů, které

nemají uloženu příliš přesnou aproximaci data i později). Doba, na kterou jsou vydávány certifikáty inspekčním systémům, je tedy jedním z klíčových parametrů bezpečnosti celého systému. Je zřejmé, že čím kratší je tato doba, tím menší užitek bude mít útočník z ukradených či jinak neautorizovaně získaných inspekčních systémů. Konkrétní doba platnosti certifikátů bude záviset na domluvě jednotlivých CA, například doba platnosti certifikátu pro DV CA vydaného CV CA by mohla být roční a doba platnosti IS certifikátů vydávaných DV CA by mohla být měsíční nebo týdenní. Pomocí řešení založeného na on-line přístupu by bylo možné se vyvarovat problémů s ukradenými inspekčními systémy (ať už přesměrováním autentizace nebo aktuálními CRL), toto však nebylo akceptovatelné pro všechny země EU, neboť ne všechna inspekční místa lze vždy spolehlivě propojit on-line s centrem. Z tohoto důvodu je v EU zvažován off-line systém, kde každé inspekční zařízení může mít k dispozici svůj pár klíčů a jemu odpovídajících certifikátů. S CRL se v diskutovaném schématu nijak nepočítá. I přesto je však možné například na úrovni země implementovat on-line režim tak, že inspekční systém má daná země vlastně jen jeden a všechna kontrolní místa s přístupem ke chráněným datům jsou vybavena terminály, které svoje požadavky na autentizaci on-line přesměrují na centrální inspekční systém. Takové řešení pak má klasické výhody a nevýhody centrálního on-line přístupu (tj. snadnější ochrana tajných klíčů, ale závislost na připojení). Vzhledem k faktu, že bezpečnost systému jako celku je dána nejslabším článkem, může být při off-line přístupu problematická například ochrana klíčů na vzdáleném ostrově.

Mezi nevýhody takto definovaného rozšířeného řízení přístupu patří především zneužitelnost ukradeného inspekčního systému (samozřejmě záleží na detailech ochrany klíčů) po dobu platnosti certifikátu pro tento IS (řešení tohoto problému by vyžadovalo kompletní on-line přístup) a značně náročná (jak finančně, tak i organizačně) režie související s použitým PKI.

Celosvětová interoperabilita v oblasti rozšířeného řízení přístupu není nutná, neboť citlivá data by měla být přístupná jen na základě vzájemných dohod států a je na těchto státech, aby se domluvily na technických detailech v rámci mantinelů stanovených standardy ICAO. Lídrem v oblasti EAC je v současné době EU, která navrhla (vlastně německé BSI) protokol pro EAC a diskutuje jeho detaily tak, aby členské země mohly nejpozději od 28. června 2009 začít ukládat otisky prstů do pasů a chránit je pomocí rozšířeného řízení přístupu. Rozhodnutí Evropské komise o povinnosti ukládat otisky prstů, a tyto chránit pomocí EAC, se odkazuje na technickou zprávu BSI, ta však není v některých detailech zcela jednoznačná. Úkol detailněji specifikovat případné problematické body má tzv. Výbor podle článku 6 (Article 6 committee podle čísla článku, kterým byl zřízen – původně ke stanovení společného postupu v oblasti víz) a ten pro svá rozhodnutí využívá doporučení skupiny BIG (Brussels Interoperability Group), která pravidelně zasedá a řeší aktuální otázky v oblasti elektronických pasů. Ve dnech 6. a 7 prosince 2006 proběhl v italské Ispře workshop, jehož součástí byl první test interoperability. Ačkoliv výsledná interoperabilita jednotlivých národních implementací zdaleka ještě nebyla 100%, pomohl test identifikovat problematická místa v implementacích a na ta se dále soustředit (jedná se o formáty jednotlivých polí, chybějící podpora některých kryptografických algoritmů, APDU s rozšířenou délkou pro příkazy verifikace certifikátu, kde velikost certifikátu přesahuje 260 bajtů apod.).

Dá se očekávat, že pokud se tento protokol úspěšně osvědčí v EU, bude použit i v jiných zemích, případně, že se stane základem pro diskuze ohledně možností zápisu dalších dat na čip (víza, záznamy o přechodech hranic a oprávnění k automatickému přechodu hranic).

Interoperabilita ovšem nespočívá jen v technických detailech, ale také v oblastech důvěry, ochrany citlivých klíčových dat a jiných organizačních záležitostech. Aby se usnadnila vzájemná certifikace CV certifikačních autorit a DV certifikačních autorit jednotlivých členských zemí, vzniká na evropské úrovni certifikační politika, která by měla být minimální (ve smyslu, toto je minimální bezpečnost, která je vyžadována), resp. maximální (tj. země by neměly od ostatních vyžadovat více) požadavky na certifikační politiky DV certifikačních autorit.

Pro začátek se předpokládá, že chráněná biometrická data budou přístupná pouze navzájem mezi zeměmi EU. V diskuzích se však objevují i Spojené státy americké, Kanada a Austrálie jako další možné země zapojené do evropského systému rozšířeného řízení přístupu. Při pohledu na strukturu PKI však vidíme, že je na jednotlivých členských zemích, aby rozhodly, které jiné země budou mít přístup k údajům v jimi vydávaných pasech.

Ačkoliv autentizace čipu nahrazuje aktivní autentizaci a zlepšuje bezpečnost i pro Secure Messaging, probíhá autentizace čipu a terminálu protokoly, které zatím nebyly standardizovány organizací ICAO. Proto to jsou protokoly, které budou využity jen v těch kombinacích, kdy pas i inspekční systém dané protokoly podporují. Pokud pas (např. pasy první generace) nebo inspekční systém (např. ne-EU systém, nebo i EU systém na méně významném přechodu) protokol nepodporují, je nutné využít klasické protokoly standardizované v 9303 (tedy přímé čtení, BAC a AA). Je také možné, že některé země (mimo EU) nebudou otisky prstů nebo oční duhovky považovat za citlivá data a datové skupiny DG3 a DG4 tedy v jejich pasech nebudou nijak dodatečně chráněny.

Poznámka

Názory, zde uvedené, jsou soukromé názory autorů a nemohou být považovány za oficiální stanovisko Evropské komise, kde jeden z autorů pracuje ve Společném výzkumném středisku (JRC) v italské Ispře.

Odkazy

[1] ICAO NTWG: PKI for Machine Readable Travel Documents
Offering ICC Read-Only Access V1.1, http://www.icao.int/mrtd/download/technical.cfm .

[2] ICAO NTWG: Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technologies, V 1.7, http://www.icao.int/mrtd/download/technical.cfm .

[3] BSI: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.0, TR-03110,
http://www.befreite-dokumente.de/eingereichte-akten/tr-03110-eac-1.0/.

[4] Říha, Z.: Bezpečnost elektronických pasů, Crypto-World 10/2006, str. 19-26,
http://crypto-world.info/casop8/crypto10_06.pdf

C. XML a bezpečnost
Část I.

RNDr. Dagmar Brechlerová, EUROMISE Ústav informatiky CAS, (Dagmar.Brechlerova@seznam.cz)

Webové služby jsou založeny na standardech W3C, jsou technologicky nezávislé. Jedním z jejich základních problémů je ale neřešení bezpečnosti. Protokol SOAP používaný ve webových službách je ve své podstatě XML dokument, který je přenášen obvykle protokolem HTTP. Pro komerční, ale i jiné aplikace, kde se jedná o přenos citlivých či osobních informací, je tato vlastnost (neřešení bezpečnosti) nepřijatelná.

Během přenosu informací je nutno příslušné informace ochránit před úmyslným i neúmyslným prozrazením a/nebo modifikací, je nutno ověřit identitu podepsaného pracovníka. Je nutno zajistit základní bezpečnostní požadavky (autenticita, integrita dat, nepopíratelnost a utajení, a dostupnost dat). V prostředí Internetu je nutno zjistit identitu původce informace a určit, která data smí který uživatel vidět.
Kromě dostupnosti informací, která se zajišťuje jinými způsoby, se veškeré výše uvedené požadavky dají zajistit přímo přidáním určitých částí do XML. Samotné webové služby v sobě základní bezpečnostní služby nemají, bylo nutno XML rozšířit o část zvanou XML Security. Velmi rychle se vyvíjí standardizace pro bezpečnost webu. V příspěvku bude podán přehled v současné době vyvíjených technologií. Je to XML Signature, XML Encryption, XML Key Management Specification, Secure Assertion Markup Language, XML Access Control Markup Language, WS - security (Web Services Security), EbXML Message Services.

Úvod

Webové služby jsou služby použité v distribuovaných systémech pro volání vzdálených funkcí, které vytvářejí rámec na zabezpečení spolupráce mezi jednotlivými odděleními organizace (např. nemocnice, vysoké školy), prodejcem a zákazníkem, studentem a školou atd. Tvoří technologický základ pro integraci např. obchodních či jiných procesů v rámci organizace a/nebo s dodavateli, zákazníky atd. Obvykle používají Internetu příp. jiný druh sítě. Základem je jednak použití protokolu TCP / IP a jednak jazyka XML.

XML je sice velmi silný nástroj k použití v tzv. „bussines procesech“ vzhledem k možnosti sdílení informací např. mezi jednotlivými odděleními atd., ale na druhou stranu tyto možnosti zvyšují **nebezpečí zneužití informací**. Pokud se sdílejí informace o kreditních kartách, citlivé informace o pacientech, osobní údaje např. studentů, informace o fakturách atd., jsou zde vždy obsažena data, která mohou být zneužita, ať již jde o obchodní informace nebo informace osobní (osobní údaje) nebo případně i citlivé informace (ve zdravotnictví). Navíc některé z těchto informací je nutno chránit v důsledku platných zákonů (Zákon o ochraně osobních údajů aj.) a situace v této oblasti se stále zpřísňuje. Např. při přenosu informací o pacientovi je nutno během přenosu příslušné informace **ochránit před úmyslným či neúmyslným prozrazením** či **modifikací**, je nutno ověřit **identitu** podepsaného pracovníka. Je tedy nutno zajistit **základní bezpečnostní požadavky** (autenticita, integrita dat, nepopiratelnost a utajení a dostupnost dat). V prostředí Internetu je nutno určit **identitu**

původce informace. Je nutno určit, které informace smí který uživatel vidět. Při on-line transakcích musíme určit, **které transakce jsou platné**. Musíme zajistit **utajení citlivých dat** při transferu informací. Dalším požadavkem může např. být možnost, jak případně u soudu dokázat, že někdo měl přístup k určitým informacím. Navíc bezpečnostní požadavky je nutno splnit v každém bodě komunikace. **Kromě dostupnosti informací, která se zajišťuje jinými způsoby, se veškeré výše uvedené požadavky dají zajistit přímo přidáním určitých částí do XML.**

Vzhledem k tomu, že samotné webové služby v sobě základní bezpečnostní služby nemají, bylo nutno XML rozšířit o část zvanou **XML Security**. Tak, jak se XML stává významnou komponentou pro elektronické transakce (obchod, výměna dat atd.), potřebujeme důvěryhodné a bezpečné XML dokumenty, které vytvoří základ zejména (ale nejen) pro obchodní transakce. Bezpečnostní otázky spojené s webovými službami a bezpečností Internetu se zdají velmi obtížné, ale v poslední době jsou již buď řešitelné nebo budou v krátké době, neboť se velmi rychle vyvíjí standardizace pro bezpečnost webu [4], [6]. V následující části je podán stručný přehled v současné době vyvíjených technologií.

XML Security

V posledních letech byla vyvinuta celá řada XML bezpečnostních technologií, které jsou dnes v různé fázi normalizace a vývoje. Je to XML Signature (XML-DSIG nebo také XML-SIG nebo XS), XML Encryption (XE), XML Key Management Specification (XKMS), Secure Assertion Markup Language (SAML), XML Access Control Markup Language (XACML), WS - security (Web Services Security), EbXML Messege Services. Dále se jedná o Liberty Alliance Project.

Následující tabulka ukazuje, kdo je hlavním tvůrcem a v jaké fázi vývoje je daná technologie

XML DSIG	*W3C Recommendation*
XML Encryption	*W3C Recommendation*
WS – Security	*OASIS Committee Draft*
SAML	*OASIS Standard*
XKMS	*W3C Working Draft*
XACML	*OASIS Standard*
EbXML	*OASIS Standard*

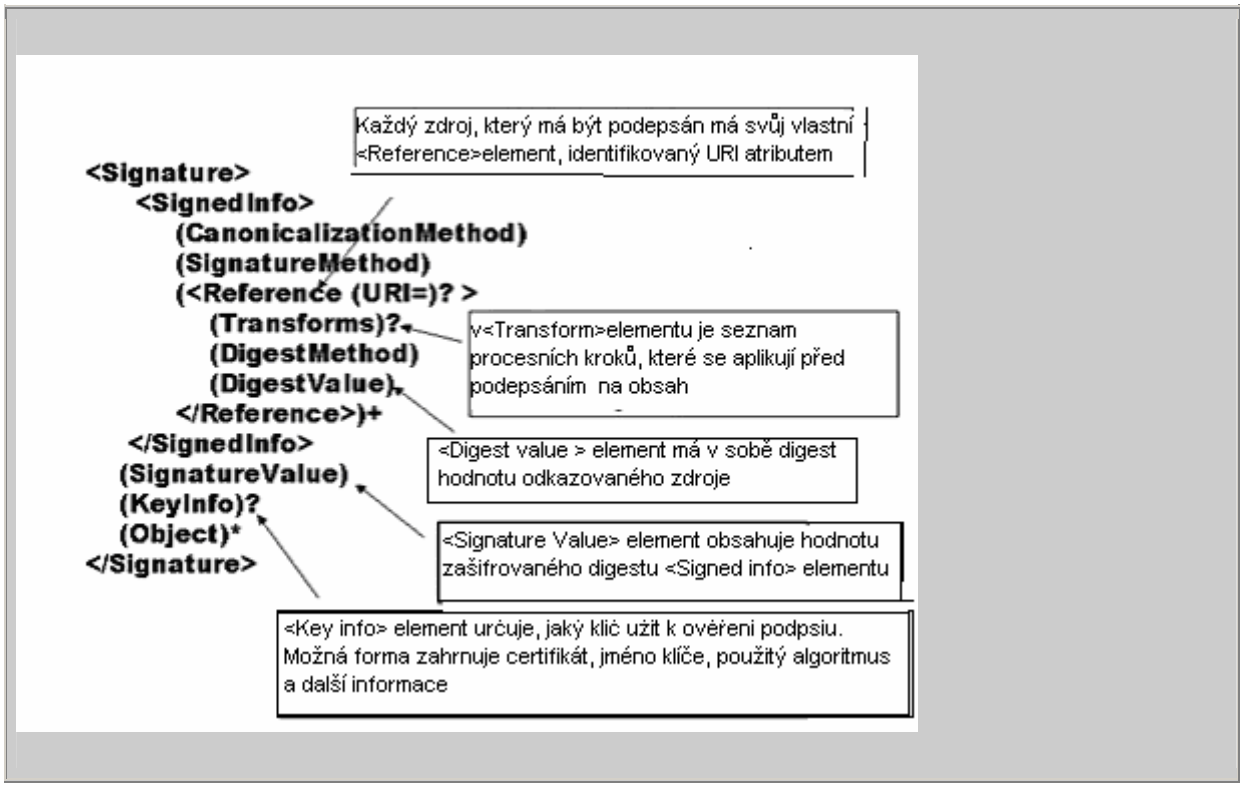
XML Digitální podpis (XS)

XML podpisy jsou digitální podpisy vyvinuté **pro užití v XML transakcích**. XML Signature je rozvíjející se standard pro digitální podpisy, který zahrnuje speciální požadavky a problémy, které XML prezentují pro podepisovací operace a užívá XML syntaxi pro vyjádření výsledku (což zjednodušuje integraci do XML aplikace.)
Standard [2] definuje schéma pro uložení výsledku operace digitálního podpisu aplikované na libovolná (ale nejčastěji XML) data. Stejně tak jako digitální podpisy, které neodpovídají specifikaci XML (např. PKCS podpis), tak i XML podpis poskytuje autentizaci, kontrolu integrity dat a podporu pro neopakování (non repundation). Navíc na rozdíl od „ne XML“ digitálního podpisu je XML podpis technologie, která se snaží **spojit výhody Internetu i XML**. Základním rysem XML podpisu je **schopnost podepsat pouze část XML stromu** (tree) spíše než celý kompletní dokument. To je velmi významné, když máme dokument,

který má dlouhou historii, ve které jsou různé části dokumentu vytvořeny v různých časech různými autory, a každá má být podepsána pouze tím, kdo je pro danou část relevantní. Tato flexibilita je důležitá, když je nutné zajistit integritu určité části XML dokumentu, zatímco jiné části dokumentu je nutné nechat otevřené pro možnost změn. Předpokládejme například, že je uživatelovi doručen určitý formulář k dovyplnění. (zdravotní karta, informace o studentovi atd.). Jestliže by podpis byl podpisem celého XML dokumentu, každá změna uživatele v původních hodnotách dokumentu by vedla k tomu, že by původní podpis porušila. **Tato možnost podepisovat pouze části dokumentu činí XML podpis mimořádně silným prostředkem.**
XML podpisem je možno podepisovat více druhů zdrojů**. Např. jeden XML podpis může pokrýt HTML data, JPG data, XML data a specifickou část XML dat.**
Ověření podpisu vyžaduje, aby datový objekt, který byl podepsán, byl přístupný. Samotný XML podpis obecně určuje umístění originálního podepisovaného objektu. Tento odkaz může být:

1. odkazován pomocí URI uvnitř XML podpisu
2. být umístěn ve stejném zdroji jako XML podpis (podpis je sourozenec)
3. být zakotven v XML podpisu (podpis je rodič)
4. mít podpis zakotven v sobě (podpis je dítě)

Následující obrázek ukazuje, jak se podpis postupně skládá z komponent. Jednotlivé kroky jsou dále zhruba popsány.



Jak vytvořit XML podpis

Následuje krátký úvod do vytvoření XML podpisu, úplná specifikace je XML Signature specification. [2]

1. Určíme, jakého druhu bude zdroj, který má být podepsán
Zdroj je identifikován svým URI (Uniform Resource Identifier).

"http://www.abccompany.com/index.html" odkazuje na HTML stránku na Webu
"http://www.abccompany.com/logo.gif" odkazuje na GIF obrázek na Webu
"http://www.abccompany.com/xml/po.xml" odkazuje na XML sobor na Webu
"http://www.abccompany.com/xml/po.xml#sender1" odkazuje na specifický element XML souboru na Webu

2. Z každého zdroje je spočítán digest
V XML podpisu je každý odkazovaný element specifikován skrze <Reference> element a každý jeho digest (spočítaný ze specifikovaného zdroje, nikoliv z elementu samého!!!) je umístěn v dětském (child) elementu <DigestValue> jako např.

```
<Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
 <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
</Reference>
<Reference
 URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-example.xml">
 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
 <DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue>
</Reference>
```

<DigestMethod> element identifikuje algoritmus použitý na spočítání digestu. Tedy v tuto chvíli pouze počítám jednotlivé digesty a vždy k odkazu na podpisovaný zdroj připojím algoritmus (DigestMethod) a příslušný digest. (DigestValue).

3. Spojení, spočítání Reference elementů
Spojí se <Reference> elementy (spolu s jejich přičleněnými digesty) do <SignedInfo> elementu jako např.

```
<SignedInfo Id="foobar">
 <CanonicalizationMethod
  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
 <Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
 </Reference>
 <Reference
   URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-example.xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue>
 </Reference></SignedInfo>
```

Dalším přidaným prvkem je tzv. **kanonizační metoda.**

<CanonicalizationMethod> element udává, že byl použit **kanonizační algoritmus** na <SignedInfo> element. Různé datové proudy se stejnou XML informací mohou totiž dát různé textové reprezentace, např. se mohou lišit ve white spaces, v prázdných tazích, vložených řádcích, komentářích, oddělovačích atd. Proto, abychom zabránili rozdílným výsledkům při ověřování podpisu, je nutno, aby XML informace byly nejdříve před podepisovacím procesem kanonizovány. Aby byl podpis jednoznačný, **musí se podepisovat a ověřovat zcela identický proud bitů (bytů).** Sebemenší změna ve vzkazu (message), ze kterého se počítá digest, má za následek změnu tohoto digestu. To je jedním ze základních kritérií pro kvalitní hash funkce. Ovšem pro použití v souvislosti s XML to přináší zásadní problémy. **Ačkoliv jsou 2 XML dokumenty logicky stejné, mohou se lišit textově**. To vše nemá vliv na logickou strukturu, ovšem hash je pak jiný. Kanonizace přesně popisuje a normuje, jak vyrobit tzv. kanonizační formu (přesně definovaná fyzická struktura dokumentu).

<SignatureMethod> element indikuje, který z **podepisovacích algoritmů** byl použit pro podpis. Jde tedy o to, který algoritmus byl použit pro převedení kanonizovaného elementu <SignedInfo> na hodnotu <SignatureValue>.

4. Podepsání
Spočítá se digest <SignedInfo> elementu, podepíše se digest a hodnota podpisu se dá do <SignatureValue> elementu. Tedy se vlastně **může podepisovat několik digestů najednou**, které byly předtím nakumulovány do jednoho <SignedInfo> elementu.

```
<SignatureValue>MC0E LE=</SignatureValue>
```

5. Přidání informací o klíči
Pokud se přidávají **informace o klíči**, tak se umístí do <KeyInfo> elementu. Zde uvedený příklad např. obsahuje **X.509 certifikát** odesílatele a tento certifikát obsahuje veřejný klíč nutný pro ověření podpisu. Tento element je volitelný, neboť podepisující nemusí mít vždy zájem prozrazovat svůj veřejný klíč všem stranám.

```
<KeyInfo>
 <X509Data>
  <X509SubjectName>CN=Ed
Simon,O=XMLSecinc.,ST=OTTAWA,C=CA</X509SubjectName>
  <X509Certificate>MIID5jCCA0+gA...lVN</X509Certificate>
 </X509Data>
</KeyInfo>
```

6. Složení do Signature elementu
A teď to celé poskládáme dohromady.
Umístí se <SignedInfo>, <SignatureValue>, a <KeyInfo> elementy do <Signature> elementu . <Signature> element zahrnuje XML signature.

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo Id="foobar">
<CanonicalizationMethod
```

```
  Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod
  Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
<Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
</Reference>
<Reference
  URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-example.xml">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MC0E~LE=</SignatureValue>
<KeyInfo>
<X509Data>
<X509SubjectName>CN=Ed Simon,O=XMLSec
Inc.,ST=OTTAWA,C=CA</X509SubjectName>
<X509Certificate>
MIID5jCCA0+gA...lVN
</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
```

7. Ověření XML podpisu
Jak se XML podpis ověří?

a. **Ověří se podpis <SignedInfo> elementu.** Abychom to provedli, tak se znovu spočte digest <SignedInfo> elementu (použije se digest algoritmus specifikovaný v <SignatureMethod> elementu) a použije se veřejný ověřovací klíč, abychom ověřili, že hodnota <SignatureValue> elementu je korektní digest <SignedInfo> elementu.

b. Jestliže tento krok proběhne, **spočte se digest z referencí** obsažených uvnitř <SignedInfo> elementu a porovná se to s digest hodnotami vyjádřenými v každém <Reference> elementu odpovídající <DigestValue> elementu.

XS je tedy **schéma XML pro uplatnění digitálního podpisu v XML**, kde digitální podpis zaručuje integritu (resp. zjištění porušení integrity), nepopíratelnost (nemožnost popřít odeslání) a autenticitu. Je možno podepsat jak celý XML dokument, části dokumentu nebo externí datové objekty, na které XML odkazuje. **XML podpisem je možno podepisovat více druhů zdrojů**. Např. jeden XML podpis může pokrýt HTML data, JPG data, XML dat a specifickou část XML dat. V předcházející části byly ukázány základní rysy XML podpisu tak, aby bylo možno prezentovat použití v praxi.

Práce na tomto schématu jsou nyní nejdále. XML Signature je rozvíjející se standard pro digitální podpisy, který zahrnuje speciální požadavky a problémy, které XML prezentují pro podepisovací operace a užívá XML syntaxi pro vyjádření výsledku (což zjednodušuje

integraci do XML aplikace.) Standard [2] definuje schéma pro uložení výsledku operace digitálního podpisu aplikované na libovolná (ale nejčastěji XML) data**.**

Na XML Signature spolupracovalo **W3C konsorcium a IETF**. Cílem bylo vyvinout syntaxi takové části jazyka XML, která umožňuje podpisy webových zdrojů, dále jsou definovány procedury pro počítání a ověřování podpisů a je definována tzv. kanonizace. Hlavní výhodou je **možnost podepisovat pouze určité části dokumentu**, nemožnost této akce byla dříve hlavním problémem použití digitálního podpisu v reálné praxi. Za nevýhodu je považováno to, že jsou pro podpis nutné zdroje ze sítě. Poskytování autentizačních služeb by časem mohlo vést až k monopolu určitého výrobce SW.

XML Encryption - XML šifrování

Předpokládejme, že chceme poslat XML soubor (příklad 1) společnosti, která publikuje knihy. Tento soubor obsahuje detaily o knize, kterou chceme koupit. Navíc obsahuje informace o kreditní kartě zákazníka. Pro komunikaci o takto soukromých údajích chceme samozřejmě použít bezpečnou komunikaci. XML dokument, stejně tak jako jiné dokumenty, může být zašifrován vcelku např. SSL a poslán jednomu nebo více příjemcům.
Mnohem zajímavější ale je, jak řešit situaci, kdy různé části stejného dokumentu potřebují různé zacházení. Možností je XML šifrování. XML šifrování není alternativou SSL/TLS. Pokud aplikace vyžaduje zabezpečit celou komunikaci, je lepší SSL. Na druhé straně XML šifrování je nejlepší možností, pokud aplikace vyžaduje kombinaci bezpečné a nebezpečné komunikace. Tj. část bude vyměňována zabezpečeně a část nezabezpečeně. Navíc ovšem SSL nezajišťuje trvalou ochranu tj. při uložení na disku. Cílem vyvíjeného standardu je také schopnost rozlišit, zda je podpis aplikován na zašifrované části nebo naopak.

Příklad 1 – XML, které budeme šifrovat

```
<purchaseOrder>
        <Order>
                <Item>book</Item>
                <Id>123-958-74598</Id>
                <Quantity>12</Quantity>
        </Order>
        <Payment>
                <CardId>123654-8988889-9996874</CardId>
                <CardName>visa</CardName>
                <ValidDate>12-10-2004</ValidDate>
        </Payment>
</purchaseOrder>
```

Tento XML soubor je velmi jednoduchý, tak, aby na něm mohly být ukázány rysy vztahující se k šifrování. Skutečný XML soubor ve spolupráci s webovými službami bude mít podobnou strukturu, ale bude mnohem komplikovanější. Např. WSDL (Web Services Definition Language) a SOAP (Simple Object Access Protocol) jsou jazyky založené na XML, které

jsou často užívané v B2B integraci. Jak WSDL tak i SOAP také mohou použít XML šifrování.

XML Encryption poskytuje široké možnosti. Příklady 2, 3 a 4 ukazují různé výsledky a navíc na nich bude popsán postup zašifrování.

Příklad 2. Zašifrování celého souboru

```
<?xml version='1.0' ?>
<EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
                    Type='http://www.isi.edu/in-notes/iana/assignments/media-
types/text/xml'>
        <CipherData>
                <CipherValue>A23B45C56</CipherValue>
        </CipherData>
</EncryptedData>
```

Příklad 2 ukazuje, jak vypadá zašifrovaný soubor v případě, že zašifrujeme dokument v příkladu 1.

Důležité jsou <CipherData> a <CipherValue> tagy. Zašifrovaná data jsou obsahem <CipherValue> tagu. Kompletní CipherData element se objevuje v EncryptedData elementu. EncryptedData element obsahuje XML jmenný prostor použitý pro šifrovaní. Např. originální data před zašifrováním byla XML, tak, jak je oficiální definice (Internet Assigned Numbers Authority (IANA) - pro XML je http://www.isi.edu/in-notes/iana/assignments/media-types/text/xml). Zde je to hodnota typu atributu XML Encryption, používá typovou definici IANA pro různé oblíbené formáty jako je RTF, PDF a JPG. Pokud máme nějaké speciální datové formáty (např. naše vlastní DTD nebo XSD), tak je můžeme specifikovat v Type atributu v EncryptedData elementu. Xmlns, specifikuje XML Encryption jmenný prostor, který budeme používat pro šifrování. Encrypted Data obsahuje text kódovaný ve formátu Base64.

Zašifrování jednotlivého elementu pomocí XML šifrování

Z nějakého důvodu můžeme chtít zašifrovat pouze jeden element z příkladu 1, např. element Payment . V tomto případě je výsledek ilustrován příkladem 3. Srovnáním příkladů 2 a 3 docházíme k následujícím rozdílům

1. Příklad 2 obsahuje pouze šifrovanou část, zatímco příklad 3 obsahuje šifrovanou část stejně tak jako nešifrovaný element. Šifrovaná část je zakotvena uvnitř souboru XML.

2. Příklad 3 má také typový atribut v <EncryptedData>, ale jeho hodnota je nyní http://www.w3.org/2001/04/xmlenc#Element. Zde není dále používán typ IANA; místo toho je používán typ specifikovaný XML šifrováním (normou).

3. Fragment #Element znamená, že jde o šifrování jednoho elementu.

Příklad 3 – zašifrování pouze elementu <Payment>

```
<?xml version='1.0' ?>
<PurchaseOrder>
        <Order>
                <Item>book</Item>
                <Id>123-958-74598</Id>
                <Quantity>12</Quantity>
        </Order>
        <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'

        xmlns='http://www.w3.org/2001/04/xmlenc#'>
                <CipherData>
                        <CipherValue>A23B45C564587</CipherValue>
                </CipherData>
        </EncryptedData>
</PurchaseOrder>
```

Zašifrování obsahu dokumentu

Obrázek 4 ukazuje výsledek, pokud chceme šifrovat pouze obsah elementu, zde se jedná o obsah elementu CardId. Zde je použit http://www.w3.org/2001/04/xmlenc#Content jako hodnota atributu typu. Tato hodnota bude použita, pokud se jedná pouze o obsah elementu.

Příklad 4. Zašifrování pouze obsahu CardId elementu

```
<?xml version='1.0' ?>
<PurchaseOrder>
        <Order>
                <Item>book</Item>
                <Id>123-958-74598</Id>
                <Quantity>12</Quantity>
        </Order>
        <Payment>
                <CardId>
                        <EncryptedData
Type='http://www.w3.org/2001/04/xmlenc#Content'

        xmlns='http://www.w3.org/2001/04/xmlenc#'>
                                <CipherData>

        <CipherValue>A23B45C564587</CipherValue>
                                </CipherData>
                        </EncryptedData></CardId>
                <CardName>visa</CardName>
                <ValidDate>12-10-2004</CardName>
        </Payment>
</PurchaseOrder>
```

Zašifrování dat, která nejsou XML

Na příkladu 5 je ukázáno, jak se zašifruje JPEG soubor pomocí XML šifrování. Celý zašifrovaný JPEG soubor je frekvence bytů, která je zde obsahem elementu CipherValue. Mezi příkladem 2 (zašifrovaní XML souboru jako celku) a příkladem 5 je pouze jediný rozdíl: Atribut Type elementu EncryptedData. Příklad 5 obsahuje IANA typ pro JPEG formát. Obdobně i jiné formáty můžeme zašifrovat pomocí IANA (viz IANA Web site, Resources).

Příklad 5. Šifrování libovolných ne XML dat

```
<?xml version='1.0' ?>
<EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
                                Type='http://www.isi.edu/in-notes/iana/assignments/media-
types/jpeg' >
        <CipherData>
                <CipherValue>A23B45C56</CipherValue>
        </CipherData>
</EncryptedData>
```

XE je schéma pro šifrování dat. Je možno šifrovat celý XML dokument, část nebo externí datové objekty, na které XML odkazuje. XE tedy umožňuje selektivní šifrování. Dále vyvíjený standard [5] by měl umožnit rozlišit části, které byly podepsány před zašifrováním a po zašifrování, a tedy se s nimi musí zacházet rozdílnými způsoby. XE je koordinováno konsorciem W3C. Za hlavní nevýhody je nutno považovat to, že zašifrováním včetně tagů se ztrácí určité informační vlastnosti XML.

Kombinace XML podpisu a XML šifrování - některé obecné problémy pro použití bezpečnostních metod v XML

XML dokument, stejně tak jako jiné dokumenty, může být zašifrován vcelku a poslán jednomu nebo více příjemcům. To je situace např. s SSL a TLS. Ale mnohem zajímavější je, jak řešit situaci, kdy různé části stejného dokumentu potřebují různé zacházení. Výhodou XML je to, že XML dokument může být poslán jako celek, ale pak se s ním dá zacházet po částech, čímž se omezuje síťový provoz. Ale to pak stejně navozuje otázku, jak řídit autorizovaný náhled na rozdílné skupiny elementů. Obchodník potřebuje znát jméno a adresu zákazníka, ale nikoliv nějaké detaily o jeho kreditní kartě (ani to není žádoucí), naopak banka nepotřebuje vědět informace o zboží, které zákazník kupoval. Vědec by neměl vědět osobní informace ze zdravotní karty (měly by mu stačit anonymizované údaje), naopak administrátor nemocnice by měl vědět osobní informace a ne medicínskou historii. Lékař nebo sestra naopak potřebují medicínské detaily, ale ne úplné personální detaily. V oblasti universitního informačního systému, pokud bude XML dokument použit jako záznam o studentovi, nepotřebuje pedagog znát informace např. o zdravotním stavu studenta, naopak je nežádoucí, aby měl k takovým informacím přístup. Naopak by měl vidět některé jiné informace. Pedagog by měl samozřejmě podepisovat pouze části dokumentu, které se ho týkají. Stejně tak lékař nebo sestra.

Kryptografie nyní slouží nejen k ukrývání informací. Digest potvrdí integritu textu, digitální podpis podporuje autentizaci odesílatele a s tím spojené mechanismy jsou užívány k tomu, aby zajistily, že provedená transakce nebyla později odmítnuta jinou stranou.

Z obecného hlediska není problém s podepsáním XML dokumentu jako celku. Problém nastává, pokud části dokumentu je nutno podepsat, navíc různými lidmi a tato potřeba je společně dohromady se selektivním šifrováním. Může být totiž těžké nebo i nemožné určit zašifrování částí určenými lidmi v určitém pořadí. Další problém nastává tehdy, pokud je nutno nějakou část podepsat, ale ta je zašifrována někým jiným. Není totiž samozřejmě rozumné podepisovat něco zašifrovaného. Navíc data, která jsou již zašifrována, mohou být dále zašifrována jako součást větší množiny (části). Čím komplikovanější formulář bude a čím bude procházet více aplikacemi (např. workflow) a přes více uživatelů, tím to bude celé složitější.

Další problém je zakotven v samotném XML, pokud budeme šifrovat vše včetně tagů, ztrácí se schopnost vyhledávat v XML podle tagů, tedy vlastně vypovídací schopnost XML. Navíc pokud zašifrujeme celé tagy, je to vhodný materiál pro prolomení (známe strukturu, co jsme zašifrovali). Jako ukázka, o jak komplikované rozhodování se může jednat, je dále uveden příklad šifrování dokumentu.

Následující příklad ukazuje možné postupy při zašifrování stejného dokumentu, ukazuje, jak rozdílné výsledky jednotlivé způsoby dávají a jaké množství informace poskytují nebo naopak skrývají.

Příklad 6 - nezašifrovaná informace o zákazníkovi, obsahuje jméno, příjmení, číslo kreditní karty, limit atd...

```
<?xml version='1.0'?>
  <PaymentInfo xmlns='http://example.org/paymentv2'>
     <Name>John Smith<Name/>
     <CreditCard Limit='5,000' Currency='USD'>
       <Number>4019 2445 0277 5567</Number>
       <Issuer>Bank of the Internet</Issuer>
       <Expiration>04/02</Expiration>
     </CreditCard>
   </PaymentInfo>
```

Předpokládejme, že pro nějaké účely je nutno zašifrovat veškeré informace týkající se platební karty, potom výsledek vypadá následovně.

Příklad 7

```
<?xml version='1.0'?>
      <PaymentInfo xmlns='http://example.org/paymentv2'>
        <Name>John Smith<Name/>
        <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
         xmlns='http://www.w3.org/2001/04/xmlenc#'>
            <CipherData><CipherValue>A23B45C56</CipherValue></CipherData>
        </EncryptedData>
      </PaymentInfo>
```

Jsou zašifrovány veškeré informace týkající se platební karty. Je tedy jasné, že nyní není přístupná informace, podle které je možno vyhledávat určité karty atd. Dá se říci, že informační možnosti jsou značně omezeny.

Další možností je, že budou zašifrovány pouze některé důvěrné informace týkající se kreditní karty, tj. číslo karty. Limit, banka a expirace je ponechán čitelný. Jsou ponechány názvy tagů elementu, jen obsah je zašifrován.

Příklad 8

```
<?xml version='1.0'?>
     <PaymentInfo xmlns='http://example.org/paymentv2'>
       <Name>John Smith<Name/>
       <CreditCard Limit='5,000' Currency='USD'>
         <Number>
           <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
            Type='http://www.w3.org/2001/04/xmlenc#Content'>
              <CipherData><CipherValue>A23B45C56</CipherValue>
              </CipherData>
           </EncryptedData>
         </Number>
         <Issuer>Bank of the Internet</Issuer>
         <Expiration>04/02</Expiration>
       </CreditCard>
     </PaymentInfo>
```

Také někdy může být nutnost zašifrovat prostě všechny informace v dokumentu.

Příklad 9

```
<?xml version='1.0'?>
    <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
     Type='http://www.isi.edu/in-notes/iana/assignments/media-types/text/xml'>
          <CipherData><CipherValue>A23B45C56</CipherValue></CipherData>
    </EncryptedData>
```

Ačkoliv původní zdroj je stejný, po zašifrování každý výsledek poskytuje jiné informace. Každý je vhodný (nevhodný) pro jiné použití, každý určitým způsobem omezuje původní plnou informaci a je tedy věcí důkladné analýzy, jak postupovat. Nyní si ovšem musíme představit, že některé části XML dokumentu budou navíc podepsány. Zde se skutečně můžeme dostat do velice těžko řešitelných situací.

WS Security

WS security je obecný mechanismus, který je stavebním kamenem pro spojení a využití jiných bezpečnostních řešení jako např. XML podpisu a XML šifrování. Definuje, jak vložit zašifrovaná data atd. do zprávy protokolu SOAP. WS Security byl vyvinut v roce 2002 společně Microsoftem, IBM a firmou VeriSign. Umožňuje zlepšení protokolu SOAP tak, aby poskytoval integritu, utajení a autentizaci vzkazu. Kombinuje SOAP s XML Encryption a XML Signature a je připraven i pro jiné bezpečnostní modely a jiné technologie.

XKMS

XML Key Management Specification (XKMS) je dokument W3C, byl vyvinut společně W3C a IETF, je zde specifikován protokol pro klíčové hospodářství tj. registraci a distribuci veřejných klíčů. Tedy XKMS je určeno pro spojení s XML podpisem a XML šifrováním (XML Signature and XML Encryption). Definuje důvěryhodné služby pro management kryptografických klíčů.

XKMS má 3 části :

XML Key Information Service Specification (X- KISS) a **XML Key Registration Service** Specification (X – KRSS).
X KISS podporuje služby pro používání kryptografických klíčů.
X KRSS podporuje služby užívané držitelem kryptografických klíčů (registrace, obnova klíče atd.)

Bulk Key Regisration (X- Bulk) je rozšíření X-KRSS pro hromadnou registraci
Tyto protokoly mohou být použity dohromady se SOAP pro bezpečnou distribuci klíčů a nalezení informací o klíčích.

Tato práce vznikla za podpory projektu 1ET200300413 AV ČR - Informační technologie pro rozvoj kontinuální sdílené péče o zdraví.

D. Elektronická fakturace

RNDr. Libor Dostálek, Siemens, (libor.dostalek@siemens.com)
Mgr. Michal Hojsík, Siemens, (michal.hojsík@siemens.com)

V poslední době se stále více hovoří o elektronické fakturaci. Avšak dojem z toho máme takový, že se o tom jen hovoří. Na počátku je třeba stručně popsat, jak faktura vlastně funguje:

1. Dodavatel vyrobí zboží/službu na základě objednávky odběratele nebo na základě předem sjednané obchodní smlouvy.
2. Dodavatel dodá zboží, službu apod. K dodávanému zboží dodavatel přiloží předávací protokol (v případě služeb se může jednat o akceptační protokol apod.).
3. Dodavatel vystaví fakturu, kterou rovněž zašle odběrateli. Faktura je velice často zasílána jinou cestou než zboží (např. poštou).
4. Odběratel fakturu likviduje. Likvidace nejčastěji probíhá tak, že se k faktuře se přiloží další formulář – „košilka“. Faktura je ve své podstatě přílohou tohoto formuláře. Formulář s fakturou pak obíhají organizací odběratele. Odpovědné osoby odběratele na formulář postupně stvrzují, že zboží bylo dodáno (např. na základě dodacího listu) a nakonec, že faktura má být proplacena.
5. Odběratel proplatí fakturu např. bankovním příkazem.
6. Dodavatel např. na základě výpisu z bankovního účtu zjistí, že zboží bylo zaplaceno.

Po proběhnutí tohoto procesu pak samotná faktura slouží jako indicie toho, že proces proběhl správně podle platných zákonů. Zákon nám předepisuje, že se faktura musí značnou dobu archivovat. Konkrétně v Česku se jedná o nejméně 10 let. Nad správností tohoto procesu bdí nejenom auditoři, ale zejména místně příslušný finanční úřad (tj. správce daně) podle sídla firmy.

Možná, že jste nad tím mávli rukou, těch pár faktur se strčí do krabice, která se někde nechá ty léta ležet. Jenže pro takový hypermarket na okraji města se za ta léta nemusí jednat o krabice faktur, ale o vagony nebo dokonce celé vlaky faktur. A jen pronájem místa na uložení tolika písemností rozhodně není lacinou záležitostí.

Podíváme-li se na zmíněný proces podrobněji, pak vidíme, že z listinné do elektronické formy lze převést vše:

- Objednávky zboží i sjednávání obchodních smluv (tzv. e-ordering, kterému se dnes nevěnujeme).
- Faktury včetně „košilek“.
- Komunikaci s bankami (bankovní příkazy, zpracování výpisů z účtů apod.)

Elektronickou komunikaci s bankami dnes považujeme za naprostou samozřejmost. Je to však důsledek toho, že banky samy investovali do elektronického bankovnictví nemalé částky. Svým klientům pak za výhodných podmínek poskytly programové vybavení, které se často snadno přímo napojuje i na informační systémy klientů.

Velcí vystavovatelé/příjemci faktur bohužel zatím takovou cestou nešly, a tak se faktury stále tisknou a tisknou k radosti výrobců tiskový/scanovacích linek a pošty. Je to rozhodně dáno také tím, že na rozdíl od bank netvoří nějakou komunitu se vzájemnou konkurencí.

Kdo jsou to ti velcí vystavovatelé/příjemci faktur? Klasickými velkými vystavovateli faktur jsou „utility“, tj. telekomunikační operátoři, dodavatelé elektřiny, plynu, vody apod. Klasickým velkým příjemcem faktur je např. „retailer“, tj. např. hypermarket. Retaileři přitom díky velké konkurenci tlačí na snižování cen. Mne vcelku překvapuje, že podle vzoru bank neinvestují do programového vybavení na elektronickou fakturaci, které by poskytovali svým dodavatelům. Přitom by si mohli klást jako podmínku odběru zboží tuto elektronickou fakturaci. Evropská unie přitom odhaduje, že přechodem na elektronickou fakturaci se ušetří přibližně 30-50 Kč na každou fakturu (na vlak faktur to už přece musí být zajímavé!). Není přitom ani podstatné, zda-li k úspoře dochází na straně dodavatele nebo odběratele, protože dodavatel si případné náklady promítne do ceny. Proč tedy není elektronická fakturace používaná? V čem je zakopán pes?

Nejprve byl problém v legislativě. Dnes ale již existuje velké množství právních úprav, které se touto oblastí zabývají. Na úrovni práva Evropských společenství to jsou hlavně:
Směrnice Rady 2001/115/ES z 20.12.2001, Doporučení Komise 1994/820/ES z 19.10.1994 a Směrnice 1999/93/ES Evropského parlamentu a Rady z 13.12. 1999.

Na úrovni práva České republiky jsou to především:
zákon o elektronickém podpisu č. 227/2000 Sb. v platném znění, zákon o dani z přidané hodnoty č. 235/2004 Sb. a jeho novela zákon č. 377/2005 Sb. a zákon o účetnictví č. 563/1991 v platném znění.

Dnes se tedy jeví jako největší problém výměna dat mezi informačními systémy odběratele a dodavatele. Doposud tak převládá výměna dat na papíře.

Řešením přitom rozhodně není, mnohými firmami tak inzerované scanování faktur. Co takové řešení totiž nabízí:

- Dodavatel fakturu vytiskne, tj. má náklady na tisk a obálku.
- Dodavatel fakturu odešle např. poštou, tj. má náklady na porto.
- Odběratel fakturu nascanuje a převede obraz do textového tvaru, tj. má náklady na scanování.

Díky předávání dat na papíře nám zde žije celé průmyslové odvětví zabývající se touto problematikou. Na první pohled je tak vidět, kolik má elektronická fakturace nepřátel.

Electronic Data Interchange (EDI)

EDI je systém pro výměnu strukturovaných dat mezi počítači (přesněji mezi aplikacemi běžícími na těchto počítačích) jehož cílem je minimalizace lidského zásahu do výměny dat.

EDI vzniklo před více jak dvaceti lety, tj. v době, kdy Internet byl jen jednou z mnoha budoucích možností komunikace. V té době se objevila koncepce tzv. *Value Added Networks* (VAN), kdy specializovaný poskytovatel zajišťuje nejenom prostou výměnu dat, jak ji známe u poskytovatelů Internetu, ale slouží jako mezilehlý uzel, přes který se strukturovaná data vyměňují. Nezávislý operátor VAN tak do jisté míry může sloužit jako smluvní svědek skutečnosti, že strukturovaná data skrze něj prošla. VAN operátora bychom s trochou nadsázky mohli přirovnat k provozovateli poštovních serverů, přes které se rovněž vyměňují dávky dat – nikoliv však jen maily, ale prostě jiné strukturované zprávy. Důležité je, že se

jedná o „strukturovaná data“, tj. je známo jaký typ dat (typ zpráv) se přenáší (např. elektronické faktury).

EDI často chápeme jako sadu mezinárodních a národních standardů. Tyto standardy lze přibližně rozdělit na dvě skupiny:

- Standardy zabývající se transportem EDI zpráv. Díky mnohaleté historii EDI už asi nemá cenu uvádět komunikaci po synchronních linkách o rychlostech 2800 b/s apod. Vše převálcoval Internet. Postupně se přešlo na zapouzdření EDI zpráv do MIME hlaviček. Výsledek pak může být zabezpečen např. S/MIME a transportován elektronickou poštou nebo skrze populární protokol HTTP (blíže viz RFC-3335 a RFC-4130).
- Standardy specifikují strukturu vlastních strukturovaných zpráv (EDI zpráv). Asi nejrozšířenějším je standard *United Nations/Electronic Data Interchange For Administration, Commerce, and Transport* (UN/EDIFACT) vyvinutý pod hlavičkou OSN a převzatý též jako ISO 9735.

A tak pro naše národní prostřední máme např. k dispozici standard ČSN 97 3080 – Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) – Zpráva Faktura.

Dnes mnoho lidí vidí VAN operátory jako nákladný mezičlánek. Avšak asi nikdo jim neupírá úsilí, které věnovali na analýzu datových struktur přenášených dat. A pokud využijeme přímou komunikaci mezi dodavatelem a odběratelem, pak tyto formáty mohou být velice užitečné.

XML

Syntaxe zpráv EDI pamětníkům připomene strukturu dat děrovaných do děrných štítků. Takový formát se ale dnes příliš nenosí. Dnes světem hýbe jazyk XML, který je údajně pro člověka lépe čitelný. Pakliže EDI nám např. vypracovalo formát strukturované zprávy pro fakturu, pak je vcelku snadné transformovat tuto strukturu do špičatých závorek XML. Konverzí EDIFACTových zpráv do XML se zabývá zejména RosettaNet a EDIFICE (viz http://www.edifice.org).

Faktura není jen faktura

Faktura je u nás zároveň i daňovým dokladem pro plátce daně z přidané hodnoty (DPH). Tj. plátce faktury (odběratel) si zaplacenou částku může odečíst z odváděné DPH. A to je právě důvod, proč jsou faktury tak bedlivě sledovány finančními úřady. Na druhou stranu pokud odběratel není plátcem DPH, pak ostříží sledování finančními úřady odpadá. V takovém případě k jiné než elektronické formě faktury není důvod, pokud si to odběratel výslovně nepřeje. Jenže tisk faktur je u nás tak zažitý zvyk, že např. můj poskytovatel Internetu mi každý měsíc posílá fakturu nejenom elektronicky, ale i poštou s přetiskem, abych nic neplatil, protože vše je elektronicky zajištěno. Každý měsíc mi proto vždy vrtá hlavou, proč vynakládá tyto náklady.

Legislativa o DPH

Jelikož jsme součástí společného evropského trhu, tak faktury jsou platné v rámci celé EU. Tj. faktura/daňový doklad vystavená např. v Portugalsku musí být u nás přijata obdobně jako faktura/daňový doklad vystavená u nás v Čechách. Finanční úřad může nanejvýš vyžadovat

překlad takové faktury do češtiny. Jen v obchodním styku mimo EU faktura neslouží jako daňový doklad (tam se používají celní deklarace).

Faktura je v rámci EU upravena Směrnicí Rady 2001/115/ES, kde se mj. uvádí:

„Faktury vydané na základě písmena a) lze zasílat buď na papíře, nebo elektronicky, pokud s tím zákazník souhlasí.

Faktury zaslané elektronicky členské státy přijímají pod podmínkou, že věrohodnost původu a neporušenost obsahu jsou zaručeny:

- zaručeným elektronickým podpisem ve smyslu čl. 2 odst. 2 směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy; členské státy však mohou požadovat, aby se zaručený elektronický podpis zakládal na kvalifikovaném osvědčení a byl vytvořen prostředky pro bezpečné vytváření podpisů ve smyslu čl. 2 odst. 6 a 10 uvedené směrnice,

- nebo prostřednictvím elektronické výměny dat (EDI) vymezené v článku 2 doporučení Komise 1994/820/ES ze dne 19. října 1994 o právních aspektech elektronické výměny dat, jestliže dohoda o výměně stanoví užití postupů zaručujících věrohodnost původu a neporušenost dat; členské státy však mohou za podmínek, které stanoví, požadovat doplňkový souhrnný dokument na papíře.“

Česká republika tuto směrnici promítla do zákonu o DPH. Zákon č. 235/2004 Sb., o dani z přidané hodnoty doslova praví:

„Daňový doklad může být vystaven se souhlasem osoby, pro kterou se uskutečňuje zdanitelné plnění nebo plnění osvobozené od daně s nárokem na odpočet daně, i v elektronické podobě, pokud jej plátce nebo osoba uvedená v odstavci 3 opatřila zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo elektronickou značkou založenou na kvalifikovaném systémovém certifikátu podle zvláštního právního předpisu (odkaz na zákon o elektronickém podpisu) nebo pokud je zaručena věrohodnost původu a neporušitelnost obsahu daňového dokladu elektronickou výměnou informací (EDI).“

Legislativa jakoby dávala do protikladu elektronické faktury, jejichž věrohodnost původu je založena na elektronickém podpisu s těmi, které jsou vyměňovány pomocí EDI. V praxi je ale situace podstatně jednodušší. Ti, kteří investovali nemalé peníze do EDI, mohou pokračovat ve výměně přes EDI klidně dále. Ti, kteří nechtějí uzavírat smlouvy s VAN operátory, pak mohou jít cestou elektronického podpisu. Směrnice nehovoří o formátu dat, ale o tom, jak zajistit věrohodnost původu faktury (buď smluvně, nebo elektronickým podpisem).

Jaká je váha elektronického podpisu v elektronické faktuře?

Historicky jsme zvyklí, že listinná faktura musí mít podpis a razítko. Zákon nám nic takového přitom nepředepisuje. Velcí vystavovatelé faktur faktury tisknou na tiskových linkách a představa, že na konci linky sedí v posledním modulu tiskové linky úředník s razítkem a perem je přinejmenším úsměvná. Navíc v takové Velké Británii vůbec nikomu nevysvětlíte, že by faktura měla nějaké razítko obsahovat a britské faktury se u nás běžně přijímají.

U elektronických faktur je situace jiná. Pokud nejsou vyměňovány přes EDI, pak musí být opatřeny elektronickým podpisem. Vzhledem k požadavku na následnou archivaci by elektronický podpis měl být doplněn o nepodepisovaný atribut nesoucí časové razítko z elektronického podpisu např. dle [2]. Časové razítko nám sice žádný zákon přímo neukládá, ale nevíme, co na nás během těch deseti let zákonodárci připraví. Já být na jejich místě to časové razítko vyžadoval.

Co je ale podle našeho názoru důležité, je váha elektronického podpisu pod fakturou. My vidíme v elektronickém podpisu nezpochybnitelný důkaz pravosti dokumentu. A první, co bychom na faktuře kontrolovali, je elektronický podpis.

Jenže o věrohodnosti faktury rozhoduje správce daně, tj. úředník finančního úřadu. A ten, světe div se, se pravděpodobně zaměří na elektronický podpis až jako na úplně poslední část elektronické faktury. Daňový úředník bude totiž kontrolovat celý cyklus od dodavatele k odběrateli a zpět (on má totiž přístup k oběma stranám). Běžně je totiž velice obtížné zakamuflovat podvrženou/upravenou fakturu současně na straně dodavatele i odběratele. Teprve až podezřelou fakturu najde, pak možná (když se nešťastník pod tíhou důkazů nepřizná), přijde na řadu elektronický podpis.

Formát faktury
Vlastní formát faktury bude vycházet z EDI nebo jeho transformace do XML. Dnes možná i transformace do formátu PDF/A. To přitom platí i o elektronických fakturách nevyměňovaných přes EDI.

Formát elektronického podpisu faktury
Horší je to s formátem elektronického podpisu. EDI má vlastní formáty pro certifikát veřejného klíče, pro elektronickou obálku i pro elektronický podpis. Jenže to je spíše technická zajímavost. V případě EDI totiž žádný elektronický podpis vyžadován není.

RFC-3335 doporučuje pro případ elektronické výměny obchodních dat využívat PGP/MIME nebo S/MIME. Na PGP/MIME příliš nevěříme (alespoň v našich zeměpisných šířkách). Zdá se, že zbývá S/MIME, tj. CMS formát elektronického podpisu, nebo chcete-li PKCS#7 . Nevýhodou formátu CMS je skutečnost, že elektronický podpis zapouzdří podepisovanou zprávu. V případě CMS nelze při likvidaci faktury připsat nějakou poznámku a připojit další elektronický podpis z původního textu a připsané poznámky.

My sice patříme k příznivcům CMS, ale pokud bychom použili XML formát faktury, pak se nám přímo ideálním jeví formát XMLSignature. Proč? Protože dodavatel by mohl vystavit fakturu v XML formátu a podepsat ji pomocí standardu XMLSignature. Při likvidaci faktury by první úředník připsal své vyjádření a pomoci XPath by vyznačil, kterou část podepíše svým podpisem. Podobně by postupoval další úředník. Výsledkem tedy je, že v případě CMS při likvidaci faktury vznikne řada verzí faktury, kdežto v případě XMLSignature vystačíme s jedním souborem.

Jinými slovy: nesmíme zapomínat na košilku faktury (formulář přiložený k faktuře při její likvidaci). Košilka sice může mít firemní tvar (nevyměňuje se mezi firmami), ale podle našeho názoru by právě na ní rovněž měly být elektronické podpisy osob, které rozhodly o proplacení faktury. Na tyto podpisy se totiž bude zaměřovat správce daně v případě pochybností. Tyto podpisy pak mohou být použity jako důkazy v případném řízení před soudem. Navíc pro majitele firmy mohou sloužit jako důkaz při vymáhání škody na konkrétním pracovníkovi.

Archivace elektronických dokumentů
Stále čteme o tom, jaké skvělé výhody mají elektronické dokumenty oproti listinným, ale v případě dlouhodobější archivace elektronických dokumentů máme nemalé problémy a v případě elektronicky podepsaných dokumentů to platí dvojnásob. Hledání dokonalých

archivačních metod pro dlouhodobou archivaci elektronických dokumentů tak připomíná hledání svatého grálu.

Součástí archivace elektronických dokumentů je rovněž udržování platnosti indicií pravosti dokumentu. Takovou indicií je např. elektronický podpis dokumentu nebo jeho časové razítko. Problém elektronických podpisů a časových razítek je v jejich podpisu, který se ověřuje certifikátem veřejného klíče. A tento certifikát má omezenou dobu platnosti.

Filosoficky existují dva pohledy na nutnost udržování indicií pravosti dokumentů:

1. Předpokládáme, že sám archiv dokumentů je důvěryhodný. Pokud vložíme pravý dokument do takového archivu, pak dokument při jeho vyzvednutí z archivu musí být rovněž pravý. A to i v případě, že by důvěryhodný archiv neprováděl žádnou údržbu např. elektronických podpisů. V oblasti elektronické fakturace víceméně touto cestou jde EDI.
2. Zajišťujeme dokumenty bez ohledu na to v jakém archivu jsou uloženy. V takovém případě se hledají různé kryptografické nástroje jak udržovat platnost indicií. V oblasti elektronické fakturace touto cestou jdou faktury využívající zaručený elektronický podpis.

Je ale třeba poznamenat, že mnohé „důvěryhodné archivy“ svoji důvěryhodnost podepírají právě těmi kryptografickým algoritmy zmíněnými ve druhém bodě.

Délka archivace elektronických dokumentů

Z hlediska archivace elektronických dokumentů je třeba nejprve vyřešit otázku, po jakou dobu bude třeba konkrétní elektronický dokument archivovat. Doby archivace dokumentů jsou zpravidla předepsány archivačními a skartačními řády firem a organizací. Hovoří se o krátkodobé, střednědobé, dlouhodobé a dokonce i trvalé archivaci dokumentů. Jak rozlišíme, kdy se jedná například o střednědobou či dlouhodobou archivaci, není přesně stanoveno – střednědobá archivace může být v řádu let, dlouhodobá archivace v řádu desítek let.

Podle našeho názoru je tyto doby nejlépe posuzovat podle životnosti informačního systému, který dokument spravuje, např. na:

- Krátkodobou archivaci, pokud dokument běžně obíhá. Nejpozději při první krátkodobé archivaci by dokument měl být doplněn o časové razítko jako důkaz existence dokumentu v čase. V případě elektronického podpisu se vytváří časové razítko z elektronického podpisu viz [1].
- Střednědobou archivací, po kterou máme k dispozici původní informační systém, ve kterém dokument vznikl nebo do kterého byl vložen, proto v rámci střednědobé archivace nemáme problémy se zobrazováním dokumentu. Střednědobý archiv musí v případě elektronických dokumentů udržovat indicie o původu a pravosti dokumentů. Takovou indicií je zejména elektronický podpis. U střednědobých archivů je vhodné doplňovat elektronické podpisy o archivační časová razítka. Tj. před archivací doplnit elektronický podpis o nepodepisované atributy dle [2] nebo [3] tak, že vznikne tzv. dlouhodobý elektronický podpis. Střednědobý horizont archivace se nezmění ani pokud dojde během této doby k jedné změně informačního systému. Je totiž pravidlem, že nový IS umí importovat dokumenty předchozího (ale často už nikoliv o dvě generace vzad).
- Dlouhodobou archivací pak rozumíme archivaci po takovou dobu, kdy je pravděpodobné, že původní informační systém již nebude k dispozici. Dlouhodobé archivy musí mít k dispozici prostředky jak zobrazovat a ověřovat archivované dokumenty. Dlouhodobé

archivy rovněž musí mít k dispozici prostředky k údržbě indicií o původu dokumentů. Archiválie musí být připraveny k importu do nových archivů a zejména do trvalých archivů. Pro dlouhodobou archivaci je dlouhodobý elektronický podpis příliš neohrabaný. V tomto případě se dokument již nedoplňuje o klasická časová razítka, ale o provázané otisky [6]. Provázané otisky pak vytváří tzv. „důkazní záznam“ (angl. *Evidence Record*) o pravosti dokumentu, viz [4] a [5].

- Trvalá archivace již vyžaduje, aby dokumenty byly v takovém stavu, aby byly na informačním systému původce nezávislé a zpracovatelné archivem. Při trvalé archivaci se původní indicie o pravosti dokumentu vytvořené původcem dokumentu (tj. rozšířené elektronické podpisy a důkazní záznamy) zpravidla ponechají a trvalý archiv vytvoří svou novou řadu důkazních záznamů.

Archivace elektronických faktur

Vzhledem k desetiletému požadavku na archivaci elektronických faktur můžeme jejich archivaci považovat za střednědobou archivaci. Po tuto dobu totiž musíme mít k dispozici možnost zobrazit fakturu správci daně.

Pro střednědobou archivaci elektronicky podepsaných dokumentů je pak vhodný dlouhodobý elektronický podpis dle [2] nebo [3].

V zákoně o DPH (235/2004 Sb.) je ještě jedna zajímavost týkající se archivace naskenovaných faktur:

„Daňový doklad v písemné formě lze převést do elektronické podoby a uchovávat pouze v této podobě, pokud metoda použitá pro převod a uchování zaručuje věrohodnost původu, neporušitelnost obsahu daňového dokladu a jeho čitelnost a pokud je daňový doklad převedený do elektronické podoby opatřen zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu nebo označen elektronickou značkou založenou na kvalifikovaném systémovém certifikátu osoby odpovědné za jeho převod.“

Tj. neskenované faktury jsou též elektronickými fakturami a obsahují elektronický podpis obdobně jako „původně“ elektronické faktury. Je zde ale jeden úplně nový fenomén. Ve jménu úspor na vytváření elektronického podpisu přišli řešitelé s trikem: nebudou podepisovat každou neskenovanou fakturu, ale:

1. Neskenují celou dávku faktur.
2. Z každé faktury spočtou otisk
3. Vytvoří nový „umělý“ dokument, který pro každý neskenovaný dokument bude obsahovat: jeho identifikaci a jeho otisk.
4. Elektronicky podepíší či elektronicky označkují až tento nový dokument. Tento podpis pak upraví do formátu dlouhodobého elektronického podpisu viz [9].

Tento trik má jednu nevýhodu, která spočívá v síle algoritmu pro výpočet otisku. Zatímco u obnovování časových razítek nebo provázaných otisků se může snadno přejít na nový algoritmus, tak otisky v umělém dokumentu zůstávají.

Závěr

Z teoretického pohledu má tak podle našeho názoru největší budoucnost formát XML, který vznikl jako transformace formátu EDIFACT do XML. A jako formát podpisu pak XMLSignature.

Vidíme tedy, že ačkoliv cesta k běžnému užívání elektronické fakturace není dlouhá, obsahuje ještě tajemná zákoutí. Hledá se tedy odvážlivec, který ji projde jako první. Ostatní se pak jistě rádi přidají.

Literatura

[1] C. Adams, P. Cain, D. Pinkas, R. Zuccherato, 2001: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 3161. IETF.

[2] European Telecommunication Standard Institute, 2006: Electronic signature formats for long term electronic signatures, ETSI TS 101 733 V1.6.3 (2005-09). ETSI.

[3] European Telecommunication Standard Institute, 2002: XML Advanced Electronic Signatures (XAdES), ETSI TS 101 903. ETSI.

[4] R. Brandner, U. Pordesch, T. Gondrom, 2006: Evidence Record Syntax (ERS), Internet draft, draft-ietf-ltans-ers-05.txt. IETF.

[5] A. Jerman-Blazic, P. Sylvester, C. Wallace, 2005: Long-term Archive Protocol (LTAP), draft-ietf-ltans-ltap-00.txt. IETF.

[6] R. Merkle, 1980: Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), pages 122-134.

[7] C. Wallace, U. Pordesch, R. Brandner, 2005: Long-Term Archive Service Requirements, Internet draft, draft-ietf-ltans-reqs-05.txt. IETF.

[8] A. Jerman-Blazic, 2006: Long Term Trusted Archive Services - Trusted archive service based on long-ter archive protocol and evidence record syntax. aljosa@setcce.org

[9] M. Vohnoutová a kol., 2005-2006: Dlouhodobá archivace dokumentů I - III, DSM 5/2005, 6/2005 a 1/2006

[10] L. Dostálek a M. Vohnoutová, 2006: Velký průvodce infrastrukturou PKI a elektronickým podpisem

E. O čem jsme psali v lednu 2000 – 2006

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje 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 (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/