# Crypto-World

**Informační sešit GCUCMP**

**Ročník 7, číslo 1/2005** **15. leden 2005**


# 1/2005

**Připravil: Mgr. Pavel Vondruška**
**Sešit je přednostně distribuován registrovaným čtenářům.**
**Starší sešity jsou dostupné na adrese**
**http://crypto-world.info**
**(785 registrovaných odběratelů)**


## Obsah :



**Příloha :**
Speciál 2004 - přehled článků a prezentací členů redakce Crypto-World za rok 2004 (http://crypto-world.info/casop6/prehled_2004.pdf )

# A. Předávání dat na Portál veřejné správy

**Ing. Jan Klimeš - ORTEX, spol. s r.o. (jan.klimes@ortex.cz)**

# 1. Úvod

Následujícím článkem bych rád popsal některé slasti a strasti aplikačního programátora (se skromnými kryptografickými znalostmi) postaveného před problém, jak do informačního systému zakomponovat kryptografické rozhraní.

Naše společnost vyvíjí ERP produkt IS Orsoft včetně skupiny úloh Mzdy a personalistika. S účinností od 1.1.2004 existuje zákon 424/2003 Sb., který vyžaduje, aby byly za všechny zaměstnance odevzdávány evidenční listy důchodového pojištění jednou ročně (do 30.4. následujícího roku). Pokud by to bylo jako doposud řešeno „papírově“, ČSSZ by se potýkala s 600 metrů vysokým stohem papírů každý rok. ČSSZ se tedy odvážně pustilo do projektu **elektronického předávání evidenčních listů důchodového pojištění přes Portál veřejné správy**.

Předejmu, že se nám jako prvním v ČR podařilo odevzdat elektronický evidenční list na ČSSZ.

# 2. Kryptografické jádro

Celý IS Orsoft je napsán v jazyce COBOL. To dává programátorům výhody nezávislosti na platformě (funguje na HP-UX, Linux, Windows, SCO Open Server, IBM AIX, …), snadnou hromadnou manipulaci s daty a mnoho dalších výhod. Bohužel je jazyk COBOL naprosto nepoznamenán jakýmikoli kryptografickými algoritmy a velmi těžko bych psal celé kryptografické rozhraní. Moje snaha zde skončila u implementace hashovací funkce SHA-1, jejíž zdrojový kód v COBOLu je cca 5x delší než v jazyce C.

Naším cílem bylo napsat multiplatformní řešení, což vyloučilo kryptografické knihovny CryptoAPI MS Windows a CAPICOM (což by bylo pro nás programátory a koneckonců i uživatele mnohem jednodušší).

Rozhodli jsme se tedy, že z COBOLu budou volány kryptografické a komunikační funkce napsané v jazyce JAVA. Využíváme JRE ve verzi 1.4.2, která je na všech námi podporovaných platformách. Druhou volbou mohlo být OpenSSL, ale to jsme hned zpočátku zavrhli kvůli špatným zkušenostem s portací programů v jazyce C na všech platformách.

Pro kryptografické funkce využíváme projekt BouncyCastle. Pro uložení klíčů jsme zvolili typ UBER. Celý keystore je zašifrován pomocí Password Based Encryption s hashovaní funkcí SHA-1 a šifrou TwoFish v módu CBC (Cipher Block Chaining). Každý klíč sám o sobě je pak šifrován 3-DES (EDE).

# 3. Cíl snažení

Celé řešení elektronického předávání dat na transakční část Portálu veřejné správy (dále jen PVS) je založeno na technologiích GovTalk. Autorem protokolu GovTalk je společnost Microsoft a také celou transakční část PVS vybudovala společnost Microsoft (využívá skupinu MS BizTalk serverů a MS SQL Server 2000). Implementaci DIS (tedy konečného místa zpracování dat ELDP) na ČSSZ má na starosti společnost Siemens Business Services.

Mzdová data (evidenční listy) jsou vytvořena mzdovým systémem ve formátu XML v dané struktuře (předepsáno ČSSZ).

*Zjednodušený postup předání dat na PVS:*

A. Vytvoření GovTalk zprávy SUBMISSION (úvodní požadavek na zpracování dat)
   a. Podepsání dat ELDP (PKCS#7 - SignedData)

b. Zašifrování dat (PKCS#7 – EnvelopedData)
c. Složení GovTalk zprávy (doplnění identifikátorů pro PVS) v XML
d. Navázání HTTPS spojení se serverem `bezpecne.podani.gov.cz`
e. Odeslání GovTalk zprávy metodou POST (HTTP 1.1)
f. Zpracování odpovědi (XML) - např. odesláno na DIS nebo chyby na PVS (pokud je vše z hlediska PVS v pořádku, je transakci přiřazeno jednoznačné ID – Correlation ID).

B. Opakované vytvoření a zaslání dotazu na stav transakce (podobné XML zaslané přes HTTPS POST). Součástí tohoto dotazu je Correlation ID, na které se dotazujeme.
C. Po obdržení výsledku transakce (pozitivní nebo negativní) musíme provést „výmaz“ požadavku na zpracování z PVS.

Jak je vidět ze zjednodušeného průběhu transakce, tak zde probíhá několik kryptografických operací. Je zajímavé, že bezpečnost je řešena dvoustupňově – podepsání a následné zašifrování – mohl být použit typ SignedAndEnveloped data. Na dotaz, zda má nějakou hlubší myšlenku, proč SignedData a EnvelopedData, mi bylo řečeno: „by design“ – tedy prostě to tak je navrhnuto (a konec). Zajímavou a dobře použitelnou technologií mohlo být využití W3C standardu XML Signature a XML Encryption. Bohužel v době vzniku GovTalk protokolu byly tyto standardy teprve ve fázi vývoje (draft).

```
<?xml version="1.0" encoding="UTF-8"?>
<GovTalkMessage xmlns="http://www.govtalk.gov.uk/CM/envelope">
  <EnvelopeVersion>2.0</EnvelopeVersion>
  <Header>
    <MessageDetails>
      <Class>CSSZ_RELDP</Class>
      <Qualifier>request</Qualifier>
      <Function>submit</Function>
      <Transformation>XML</Transformation>
      <GatewayTest>0</GatewayTest>
    </MessageDetails>
    <SenderDetails>
      <IDAuthentication>
        <SenderID>725SUNIC7XHA</SenderID>
        <Authentication>
          <Method>clear</Method>
          <Value>HESLO_NA_PVS</Value>
        </Authentication>
      </IDAuthentication>
    </SenderDetails>
  </Header>
  <GovTalkDetails>
    <Keys>
      <Key Type="vars">99999999</Key>
    </Keys>
  </GovTalkDetails>
  <Body>
    <RELDPMessage xmlns="http://www.cssz.cz/XMLSchema/reldp/envelope">
      <EnvelopeVersion>1.0</EnvelopeVersion>
      <Header>
        <Encryption version="1.0" />
        <Signature xmlns:dt="urn:schemas-microsoft-com:datatypes" version="1.0">
DIGITÁLNÍ PODPIS PKCS#7 v BASE64
        </Signature>
        <Vendor productName="ORSOFT" version="8" />
      </Header>
      <Body xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="bin.base64">
ZAŠIFROVANÁ DATA PKCS#7 v BASE64
      </Body>
    </RELDPMessage>
  </Body>
</GovTalkMessage>
```

Na obrázku je ukázaný celý XML soubor (GovTalk obálka) SUBMISSION REQUEST, která zasílá požadavek na zpracování dat, která jsou podepsána a zašifrována.

## 3.1 Podepsání dat

Vstupem pro podepsání dat je XML soubor s evidenčními listy vygenerovaný mzdovým systémem. ČSSZ uznává podpisy s kvalifikovaným certifikátem (tedy toho času pouze I.CA) nebo tzv. „Podpisové klíče ČSSZ".

Pokud jsou data podepsána klíči s kvalifikovaným certifikátem, pak není potřeba nic víc dělat. Pokud využiji k podpisu „podpisový klíč ČSSZ", mám jako odesílající organizace povinnost do 3 dnů od elektronického odeslání dat doručit na OSSZ **papírový formulář, kde se upíši, že jsem poslal elektronicky data na ČSSZ.**

Proč podpisové klíče ČSSZ? Důvod je jednoduchý, ČSSZ má strach, že si všechny organizace nebudou chtít pořídit kvalifikovaný certifikát jen kvůli odesílání ELDP. Jelikož se však nejedná o kvalifikovaný certifikát vydaný akreditovanou certifikační autoritou, musí existovat ještě „papírové" potvrzení o předání dat s ručním podpisem. Využili tedy svou certifikační autoritu (CN=CSSZ EMP CA) vydávající certifikáty, kterým říkají „podpisové klíče ČSSZ"[1]. Tyto certifikáty jsou na 3 roky a zdarma. Je to velmi zajímavá varianta pro firmy, které chtějí „ušetřit každou korunu" (záměrně v uvozovkách) za cenu mírného papírování. Zde je třeba také podotknout, že I.CA vydává kvalifikované certifikáty osobám, které budou odesílat data na PVS, za sníženou cenu 370,- bez DPH 19%.

Pro podepsání fungují jak algoritmy RSA tak DSA o síle klíče 1024 bitů s hashovací funkcí SHA-1.

***PROBLÉM: ČSSZ neumí ověřit podpisy nad daty, jejichž délka je LICHÉ ČÍSLO!***

**Řešení:** Pravděpodobně proto, že k ověřování na straně ČSSZ slouží CAPICOM, který už z principu COM bere na vstupu 16-bitová UNICODE data. CAPICOM vnímám jako černou skříňku, ze které nelze získat téměř žádné další informace (kromě ověřeno, neověřeno).

Protože na straně ČSSZ dlouho nebyli schopni s tímto problémem nic udělat (použít jiné kryptografické knihovny,…), přistoupil jsem k něčemu, za což bych se měl jako programátor stydět (ale funguje to) – doplňuji vstupní XML s evidenčními listy před podepsáním a zašifrováním o mezeru (0x20) na konci, pokud je délka lichá!

Je také možné, že problém vzniká již při rozšifrování dat (která jsou následně ověřována). Umím si představit situaci, že v 16-bitovém řetězci jsou osmibitová data po dvou v každém „znaku" a tudíž zarovnána na sudý počet bytů.

***PROBLÉM: Dvojí žádost o certifikát.***

Již při vygenerování dvojice klíčů (soukromý a veřejný) dochází k vytvoření *self-signed* certifikátu, který nese identifikaci vlastníka klíče. Bohužel jsem se dostal do situace, kdy ČSSZ a I.CA vyžadují jiné položky *rozlišitelného jména (DN – Distinguished Name)* v žádosti o certifikát.

V prvotní žádosti o kvalifikovaný certifikát NESMÍ být položka *obecné jméno (CN - Common Name)*. Naopak vyžadovány jsou *Name* (příp. *Surname* a *GivenName* nebo *Pseudonym*). Naopak pro CA ČSSZ (která je založena na Microsoft Certfication Services) je položka CN nutná.

Proto tvořím 2 druhy žádosti o certifikát – jednou vyplňuji položku *jméno (N - Name - OID= 2.5.4.41)* pro I.CA nebo *obecné jméno (CN – Common Name – OID= 2.5.4.3)* pro CA ČSSZ.

[1] Dle vyjádření ČSSZ je to jen dočasné řešení, v budoucnu počítají pouze s kvalifikovanými certifikáty.

***Lidský faktor na RA certifikačních autorit***

Několik našich uživatelů se setkalo se situací, že na RA (OSSZ) nechtěli přijmout žádost o certifikát, když neměla příponu .req (což je standardní přípona pro žádosti v prostředí MS Windows). My vytváříme žádosti s příponou .csr (a ani to měnit nehodláme ;-).

Druhý zajímavý případ – I.CA. Uživatel měl v žádosti o certifikát adresu Hradec Králové a kraj vyplněn jako Královehradecký kraj[2]. Jelikož kraj není uveden na občanském průkazu ani v jiném osobním dokladu, nechtěli takový certifikát vydat. Žadatel by prý musel mít písemné potvrzení, že jeho adresa se nachází v Královehradeckém kraji (po delší debatě byl Hradec Králové uznán jako součást Královehradeckého kraje). Z toho vyplynulo doporučení pro naše uživatele, aby k identifikaci klíče nevyplňovali kraj.

## 3.2 Šifrování dat

Data evidenčních listů je třeba před vložením do XML obálky zašifrovat. Zašifrování probíhá dle standardu PKCS#7 (EnvelopedData). Dle ČSSZ jsou podporovány následující algoritmy[3]:

| | |
|---|---|
| *Symetrické šifry:* | RC2, RC4, DES, 3DES, AES |
| *Asymetrické šifry:* | RSA, DSS |
| *HASH funkce:* | MD2, MD4, MD5, SHA-1 |

Prakticky se mi podařilo poslat pouze data 3DES (EDE v módu CBC) a RC2 (mód CBC). Zkoušel jsem ještě AES 128, 196 a 256 s negativním výsledkem (spíš jen ze zájmu jsem zkusil i CAST5 a IDEA opět s negativním výsledkem). Šifrovací certifikát obsahuje veřejný klíč RSA o síle 512 bitů.

## 3.3 HTTPS

Jak jsem již napsal, jsou XML data (GovTalk) zasílána přes port 443 – HTTPS metodou POST (HTTP 1.1). Abychom nemuseli ukládat certifikáty pro https do úložiště klíčů `$JAVA_HOME$/lib/security/cacerts`, které je součástí JRE, nasazujeme následující javové systémové vlastnosti na hodnoty uživatelských úložišť. Tímto zajišťujeme to, že uživatel je nucen pracovat pouze s jedním úložištěm klíčů.

```
System.setProperty("javax.net.ssl.trustStore", keystore);
System.setProperty("javax.net.ssl.trustStorePassword", storepass);
System.setProperty("javax.net.ssl.trustStoreType", "UBER");
```

V souvislosti s HTTPS jsme byli nuceni řešit jednu nekompatibilitu mezi operačními systémy. V JRE pro Tru64 (výrobce HP – 1.4.2-3) je chyba v implementaci protokolu TLS, tak si vynucujeme SSL verze 3 tímto příkazem:

```
SSLSocket socket = (SSLSocket) fac.createSocket(PVSServer, PVSPort);
socket.setEnabledProtocols(new String[] {"SSLv3"});
```

Mnoho uživatelů také z bezpečnostních důvodů mají intranet oddělený od Internetu pomocí proxy serveru. Řešení jsme našli ve vytvoření nové třídy SSLTunnelSocketFactory (potomek SSLSocketFactory), která navazuje nejdříve spojení s proxy serverem (včetně případné autentikace) a dále posílá POST na proxy server[4].

---

[2] Kraj je nepovinná položka žádosti o certifikát viz Certifikační politika pro vydávání kvalifikovaných certifikátů verze 1.03 – kapitola 3.1.2.10 – strana 27

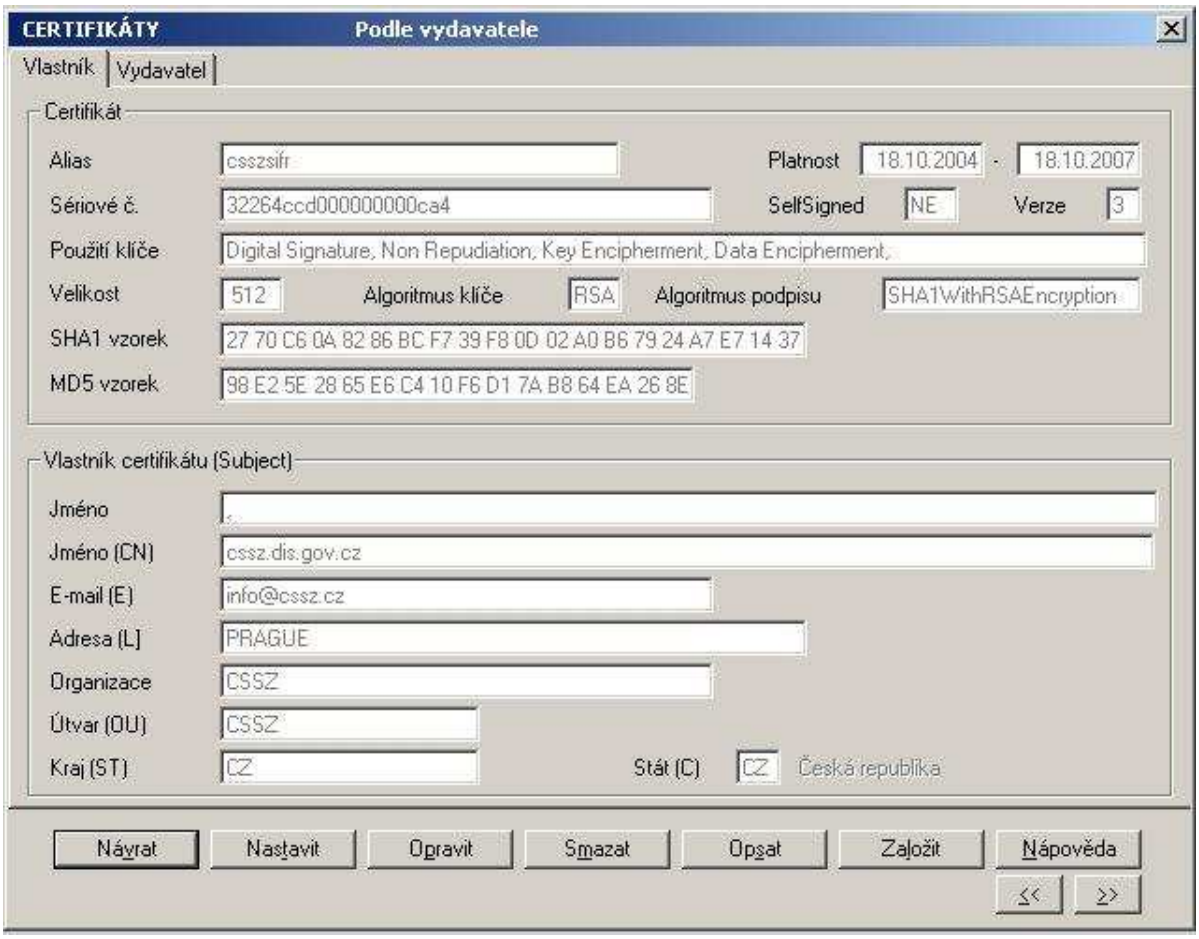
[3] Dle http://www.cssz.cz/tiskopisy/ELDP_2004/sifrovani_dat.asp

[4] Postup jak udělat HTTPS tunneling je na: http://www.javaworld.com/javaworld/javatips/jw-javatip111.html od Pua Yeow Cheonga

# 4. Závěr

Tímto článkem jsem chtěl poukázat na „veselý“ život programátora, jež se snaží využít nových technologií. Při ladění klientské části pro podání dat na PVS se našlo také mnoho chyb na straně přijímající. Zarážející je proto rétorika ČSSZ, kde již v červnu mluvili o plně fungujícím systému. Jsme zatím jediní, kdo je schopen zaslat data na PVS z jiných operačních systémů než MS Windows.

Výsledek našeho snažení se dostavil v prvním odeslaném evidenčním listu na Portál veřejné správy dne 20.10.2004 z operačního systému Linux RedHat 6.4.




**Použité zkratky:**

| | |
|---|---|
| COM | Component Object Model – objektové rozhraní pro volání komponent v prostředí Microsoft Windows. |
| CAPICOM | CryptoAPI přes COM. Objektové rozhraní kryptografických funkcí Microsoft Windows. |
| ČSSZ | Česká správa sociálního zabezpečení |
| DIS | Department Interface Server – počítač na určitém úřadě přijímající data od PVS |
| ELDP | Evidenční list důchodového pojištění |
| JRE | Java Runtime Environment – běhové prostředí pro programovací jazyk JAVA |
| OSSZ | Okresní správa sociálního zabezpečení |
| PKCS | Public Key Cryptography Standards – kryptografické standardy definované společností RSA. |
| PVS | Portál veřejné správy – http://portal.gov.cz |

# B. Praktická ukážka využitia kolízií MD5

**Ondrej Mikle , MFF UK ,** (ondrej.mikle@gmail.com )

Publikácia páru vektorov [2], ktoré spôsobujú kolíziu MD5, vyvolala v auguste celkom slušný rozruch. Odvtedy je stále pomerne rušno, ale zatiaľ nikto nezverejnil postup, ako sa dajú kolízie MD5 počítať pre ľubovolný inicializačný vektor v rozumnom čase. Na túto tému mal svoju prednášku pán Klíma [1], kde dal výzvu na praktické predvedenie dopadu kolízií. Každý vie, že schopnosť (v rozumnom čase) nájsť správu N k danej správe M tak, že ich haše sa rovnajú, znamená prelomenie hašovacej funkcie. To je tzv. kolízia druhého rádu alebo preimage attack. Čínski krytológovia predviedli ale kolíziu prvého rádu, tj. že je možné v zmysluplnom čase nájsť dve správy M, N s rovnakým hašom, čo je trocha slabšie.

Výzva ma zaujala, tak som nad tým začal rozmýšľať. Na začiatku decembra vyšla za asistencie pána Klímu moja práca [3], kde ukazujeme, že len za využitia dvoch známych kolidujúcich vektorov z [2] je možné vytvárať kolidujúce správy vybrané útočníkom. Následne o pár dní vyšla podobná práca [4]. Tu stručne popíšem podstatu, viac podrobností sa dá nájsť priamo v [3].

Myšlienka je založená na konštrukcii MD5. Pri počítaní MD5 hašu správy M sa správa najprv zarovná Damgard-Merklovým zosilením, aby jej dlžka bola násobkom 512 bitov. Postupne sa berú 512-bitové bloky správy a po spracovaní každého bloku sa zatiaľ vypočítaná hodnota H (tzv. hašový kontext) použije ako inicializačný vektor pre počítanie MD5 nasledujúceho bloku (pre prvý blok je inicializačný vektor daný algoritmom MD5). Po spracovaní všetkých blokov sa hašový kontext po spracovaní posledného bloku prehlási za výsledný haš. V nejakom momente počítania teda haš správy závisí len na predchádzajúcom hašovom kontexte a ďalších, ešte nespracovaných blokoch.

To znamená, že ak poznáme dve správy M1, M2 s rovnakým MD5 hašom (zarovnané na násobok dĺžky bloku), po pripojení ľubovolnej správy N budú mať obe rovnaký MD5 haš: MD5(M1||N) = MD5(M2||N). Takéto dve správy M1, M2 máme práve z [2].

Teraz môžme vytvoriť pár samorozbaľulúcich archívov, každý z nich bude zložený z dvoch súborov tak, že platí:

MD5(self_extract.exe_z_prvého_archívu) = MD5(self_extract.exe_z_druhého_archívu)
MD5(data.pak_z_prvého_archívu) = MD5(data.pak_z_druhého_archívu)

pričom spustenie každého z archívov rozbalí súbor contract.pdf, čo sú dve zmluvy odlišné v zmysle podľa útočníkovej vôle:

contract.pdf_z_prvého archívu != contract.pdf_z_druhého_archívu

Ako je taký archív vytvorený? Najprv vyvtoríme dátový súbor data.pak:

| Veľkosť | Dáta |
|---|---|
| 1024 bitov | blok spôsobujúci kolíziu MD5 |
| 1 bajt | dĺžka názvu súboru - *fnamelen* |
| fnamelen bajtov | názov súboru, ktorý sa má rozbaliť |
| 4 bajty | veľkosť prvého vloženého súboru – *filesize1* |
| 4 bajty | veľkosť druhého vloženého súboru – *filesize2* |
| filesize1 bajtov | dáta prvého vloženého súboru |
| filesize2 bajtov | dáta druhého vloženého súboru |

Súbor data.pak prvého archívu bude obsahovať jeden kolidujúci blok (M1) na začiatku, data.pak z druhého archívu bude obsahovať druhý kolidujúci blok (M2). Zbytok oboch súborov je identický, preto budú mať aj rovnaký MD5 haš. Vieme, že M1 a M2 sa musia líšiť aspoň v jednom bite. Samotný spustiteľný súbor preto pozrie na tento konkrétny bit a podľa neho rozhodne, ktorý súbor rozbaliť. Samozrejme je možné vytvoriť ľubovolný program, ktorý sa na základe jedného bitu rozhodne spraviť jednu akciu alebo druhú. Je možné spraviť ľubovolné rozhodnutie a netreba to dokonca robiť ani takto nápadne. Zdrojové kódy a predkompilované binárky funkčného príkladu je možné stiahnuť na stránke [3]. Okrem toho sú tam nástroje na vytváranie archívov obsahujúcich ľubovolné súbory.

Neskôr sa objavili pochybnosti o praktickosti a využiteľnosti útokov využitím kolízií MD5 - či kolízia môže vylepšiť útok alebo nie. Skeptici tvrdili, že kód namiesto rozhodovacieho bitu v kolidujúcom vektore môže napr. použiť sériové číslo dosky, ping nejakého serveru alebo podobnú "bulharskú konštantu" a teda použitie kolízie neprináša žiadne vylepšenie. Pritom ale prehliadli jeden zásadný fakt: kým použitie pingu je možné, v kóde je odhaliteľné, že sa tak deje. Pri použití kolidujúceho vektora je naopak (v jednom prípade) dokázateľné, že kód je bezpečný. Pri použití pingu je vidieť, že rozhodnutie nie je "absolútne", ale závisí od vonkajšieho vplyvu. Použitím kolidujúceho vektora človek prezerajúci kód naopak vidí, že rozhodnutie je absolútne. Kolízia MD5 maskuje práve tento vonkajší zásah. Obecne kolízia MD5 poskytuje takýto druh útoku:

Eva vytvorí nejaký software. Bob, známy kryptoanalytik, prezrie zdrojový kód software a usúdi, že software je bezpečný a niekde zverejní svoj posudok, hovoriaci: "Verzia x.y software, ktorého zdrojové kódy majú nasledovné MD5 haše, je bezpečná." Potom Eva vymení práve jednu časť kódu, ktorá spôsobí kolíziu u MD5 a vnáša do software bezpečnostnú chybu. Alica, ktorá verí Bobovi a nemožnosti zneužitia MD5 kolízií, si stiahne Evin software, skontroluje MD5 haše a tie sedia. V mylnom domnení, že používa bezpečný software, si vniesla k sebe zadné vrátka.

Dajú sa takto napadnúť napr. schémy, ktoré sú bezpečné za použitia parametrov s určitými vlastnosťami, kde parameter bez požadovaných vlastností naruší bezpečnosť celej schémy. John Kelsey uvádza v diskusii o využiteľnosti týchto útokov [5] príklad vyslovene orientovaný na kryptografické schéma. Tu vidíme, čo možno predchádzajúci príklad so samorozbaľovacími archívmi neukazuje dosť jasne – že netreba priamo rozhodnutie štýlu if-then-else, ale vznik bezpečnostnej diery môže napr. z matematického hľadiska závisieť na určitom parametri:

Eva vytvorí implementáciu Diffie-Hellmana, kde je použitý určitý prvočíselný modulus, ktorý je zabudovaný priamo do kódu ako osobitný súbor. Bob prezrie kód, dalej

potvrdí, že modulus je prvočíslo a má všetky žiadané vlastnosti a teda je implementácia bezpečná. Zdrojový kód s MD5 hašmi pre každý súbor je niekde zverejnený. Eva potom vymení modulus za číslo rovnakej dĺžky (rádu) s rovnakým MD5 hašom, ktoré je ale zložené a dovoľuje pomerne jednoduchý útok na Diffie-Hellmana. Konkrétny príklad kolidujúcich modulov:

D131DD02C5E6EEC4693D9A0698AFF95C2FCAB58712467EAB4004583EB8FB7F8955A
D340609F4B30283E488832571415A085125E8F7CDC99FD91DBDF280373C5BD8823E31
56348F5BAE6DACD436C919C6DD53E2B487DA03FD02396306D248CDA0E99F33420F5
77EE8CE54B67080A80D1EC69821BCB6A8839396F9652B6FF72A7000000000000000000
00000000000001B
je prvočíslo

D131DD02C5E6EEC4693D9A0698AFF95C2FCAB50712467EAB4004583EB8FB7F8955A
D340609F4B30283E4888325F1415A085125E8F7CDC99FD91DBD7280373C5BD8823E31
56348F5BAE6DACD436C919C6DD53E23487DA03FD02396306D248CDA0E99F33420F5
77EE8CE54B67080280D1EC69821BCB6A8839396F965AB6FF72A7000000000000000000
00000000000001B
je zložené číslo

Oba majú rovnaký MD5 haš b4b12dc7ec1b9422f6596d2a863d7900 (čísla sú uložené v binárnej podobe). Príklad využíva v zásade rovnaký trik s dvoma verziami programov našitý na Diffie-Hellmana.

Prelomených hašovacích funkcií je viacero - okrem MD5 ešte RIPEMD a HAVAL-128. MD5 je z nich ale najrozšírenejšia. Používa sa dodnes celkom bežne napríklad na overenie integrity pri distribúcii software. Akonáhle ale bude známy algoritmus na výpočet kolízií MD5, prakticky všetky známe formáty používané pri distribúcii software budú zraniteľné na útok kolíziou MD5 - samoinštalačné balíky, komprimované formáty tar.gz, tar.bz2, zip a pravdepodobne každý formát umožňuje určitým spôsobom vložiť "zmysluplne" kolidujúci blok. Dnes to ide pre inštalačné balíky rozdelené do viacerých súborov alebo CD-ROM formátu (ISO image), pretože ISO image prvých 16 blokov (32 kB) nepoužíva a je tam možné vložiť kolidujúci blok. Viac detailov opäť v [3].

Odkazy:

[1] Klíma, V.: Hašovací funkce, MD5 a čínský útok, prednáška na seminári bezpečnosť IS v praxi, MFF UK, 22. novembra 2004, http://cryptography.hyperlink.cz/2004/Hasovaci_funkce_a_cinsky_utok_MFFUK_2004.pdf
[2] X. Wang, D. Feng, X. Lai, H. Yu, "Collisions for Hash Functions MD4, MD5, HAVAL128 and RIPEMD", rump session, CRYPTO 2004, Cryptology ePrint Archive, Report 2004/199, http://eprint.iacr.org/2004/199
[3] Mikle, O.: Practical Attacks on Digital Signatures Using MD5 Sums, 2. december 2004, http://cryptography.hyperlink.cz/2004/collisions.htm
[4] Kaminsky, D.: MD5 to Be Considered Harmful Someday, 6. december 2004, http://doxpara.com
[5] mailinglist thread http://www.mail-archive.com/cryptography@metzdowd.com/msg03170.html

# C. Kryptografie a normy
# Formáty elektronických podpisů - část 2.
## (dokument ETSI TS 101 7733 - Electronic Signature Formats)

**Jaroslav Pinkava, PVT a.s**. (jaroslav.pinkava@pvt.cz )

## 1. Úvod

V první části článku byly popsány základní formáty elektronického podpisu tak, jak je definuje dokument ETSI [1] TS 101 733. Jednalo se o následující formáty:
- základní elektronický podpis - BES;
- elektronický podpis s explicitní politikou - EPES;
- elektronický podpis s časovým razítkem - ES-T;
- elektronický podpis s úplnými odkazy pro ověřování - ES-C

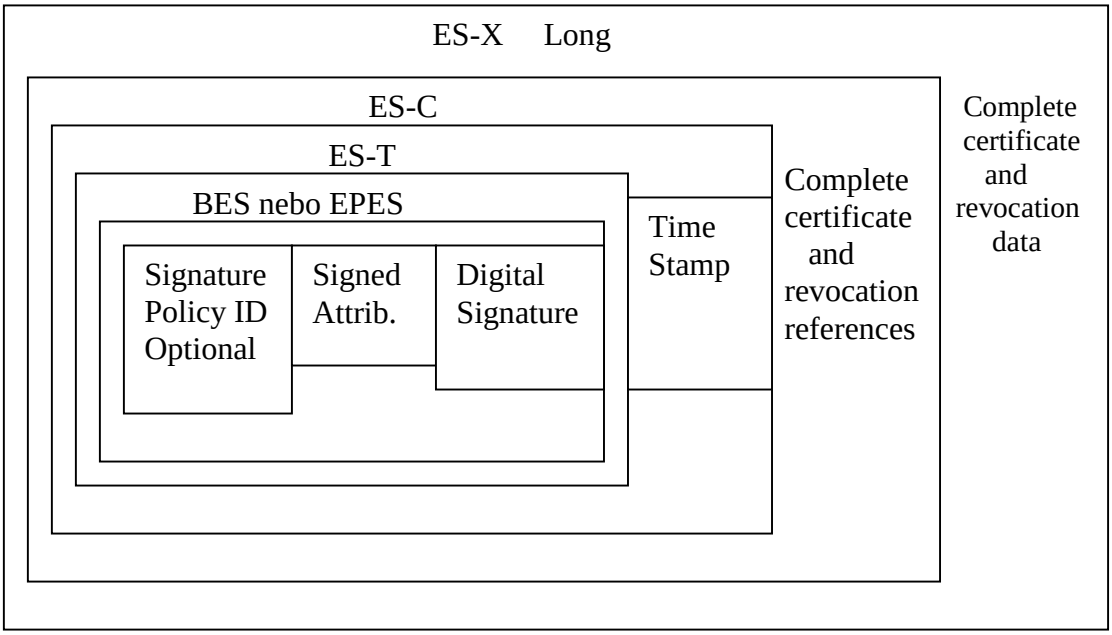
V tomto pokračování budou popsány tzv. rozšířené formáty elektronických podpisů a v návaznosti na to také archivační formát elektronického podpisu.

## 2. Rozšířené formáty elektronických podpisů

Formát ES-C (úplné odkazy) lze ještě rozšířit přidáním dalších (nepodepsaných) atributů. Dokument ETSI definuje několik takovýchto atributů, které lze využít pro verifikace po uplynutí dlouhého časového období resp. s cílem prevence některých situací při haváriích.

## 3. Rozšířený dlouhý elektronický podpis - ES-X Long

Tento formát (ES-X Long) přidává k formátu ES-C atributy: certificate-values a revocation-values. První z těchto atributů obsahuje celou certifikační cestu, která je požadována pro ověření podpisu. Druhý pak obsahuje CRL a odpovědi OCSP požadované pro validaci podpisu.



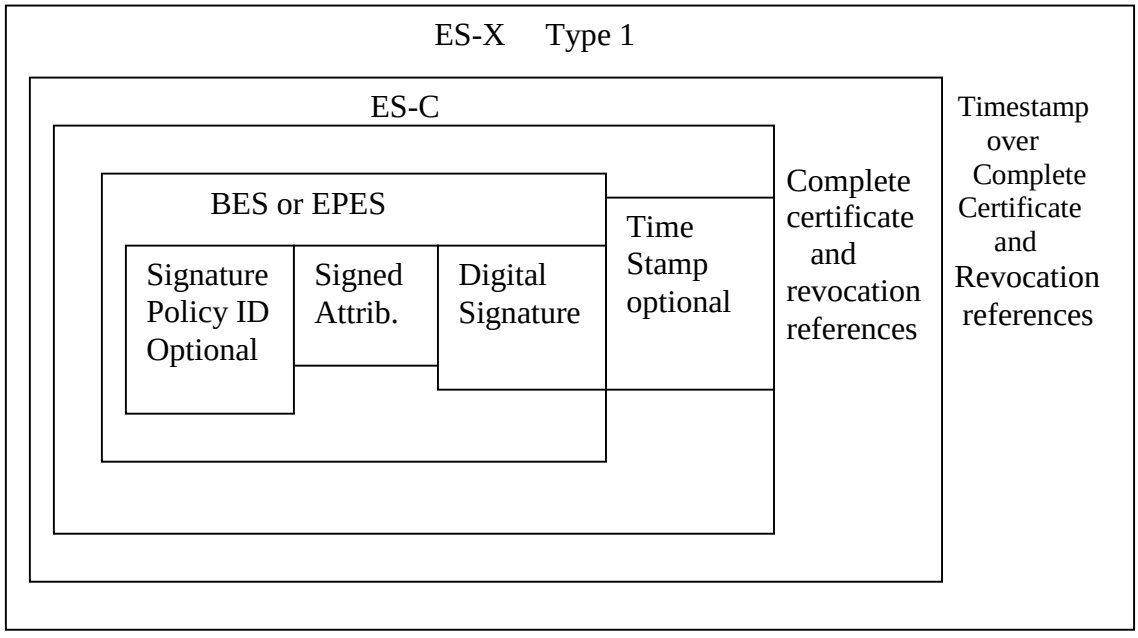

Atribut certificate-values je nepodepsaný atribut. V elektronickém podpisu se může vyskytovat nejvýše jednou. Obsahuje hodnoty certifikátů, na které je odkazováno v atributu

complete-certificate-references. Následující identifikátor objektu identifikuje atribut certificate-values:
id-aa-ets-certValues OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 23}
Atribut certificate-values má následující ASN.1 syntaxi:
CertificateValues ::= SEQUENCE OF Certificate

Atribut revocation-values je rovněž nepodepsaný atribut a může se v elektronickém podpisu vyskytovat pouze jedenkrát. Obsahuje hodnoty CRL a OCPS, na které je odkazováno v atributu complete-revocation-references. Následující identifikátor objektu identifikuje atribut certificate-values:
id-aa-ets-revocationValues OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 24}
Atribut revocation-values má následující ASN.1 syntaxi:
RevocationValues ::= SEQUENCE {
crlVals [0] SEQUENCE OF CertificateList OPTIONAL,
ocspVals [1] SEQUENCE OF BasicOCSPResponse OPTIONAL,
otherRevVals [2] OtherRevVals OPTIONAL}
OtherRevVals ::= SEQUENCE {
otherRevValType OtherRevValType,
otherRevVals ANY DEFINED BY OtherRevValType
}
OtherRevValType ::= OBJECT IDENTIFIER

## 4. Rozšířený elektronický podpis s časem, typ 1. - ES-X Type 1

Tento formát (typu 1) přidává k formátu ES-C atribut ES-C-time-stamp, jehož obsahem je časové razítko přes samotný ES-C. Toto poskytuje formátu integritu a důvěryhodnou ochranu v čase a to všech prvků a odkazů. Může tak ochránit certifikáty, CRL a odpovědi OCSP v případě pozdější kompromitace klíče CA (či klíče pro podepisování CRL resp. odpovědí OCSP).



Atribut ES-C-timestamp je nepodepsaný atribut. V elektronickém podpisu se může vyskytovat vícekrát (od různých TSA - autorit časových razítek). Je to časové razítko přes hash elektronického podpisu a úplných ověřovacích dat (ES-C). Následující identifikátor objektu identifikuje atribut ES-C-timestamp:

id-aa-ets-escTimeStamp OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 25}

Atribut ES-C-timestamp má následující ASN.1 syntaxi:

ESCTimeStampToken ::= TimeStampToken

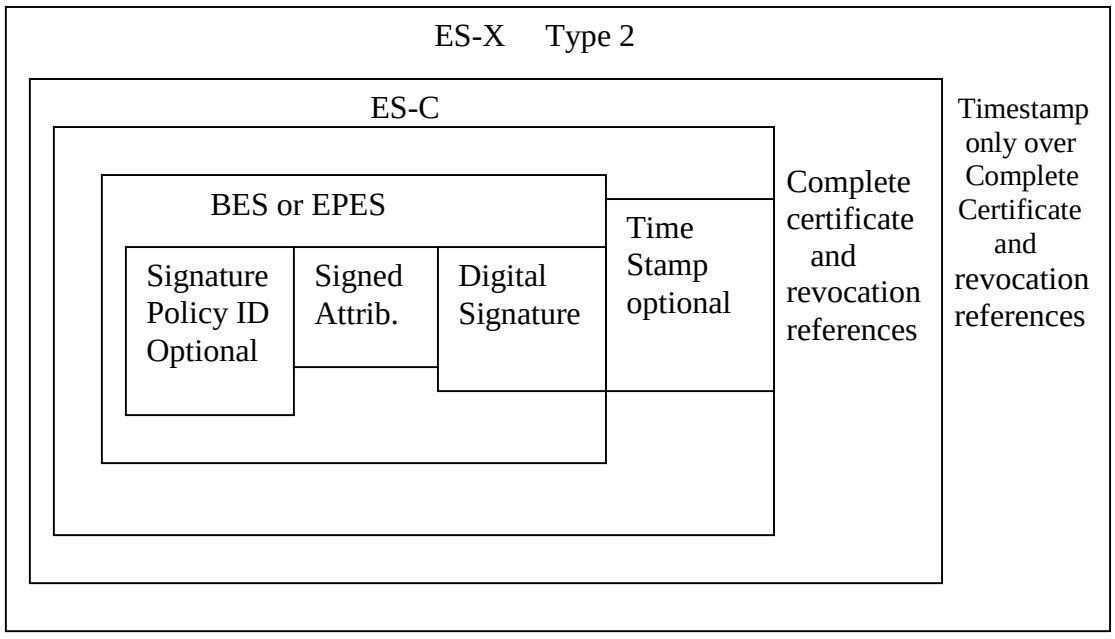
CertificateValues ::= SEQUENCE OF Certificate

Obsahem pole messageImprint pro TimeStampToken je hash spojených (konkatenace) hodnot následujících datových objektů:

- OCTETSTRING of the SignatureValue field within SignerInfo;
- signature-time-stamp;
- complete-certificate-references s attribute;
- complete-revocation-references attribute

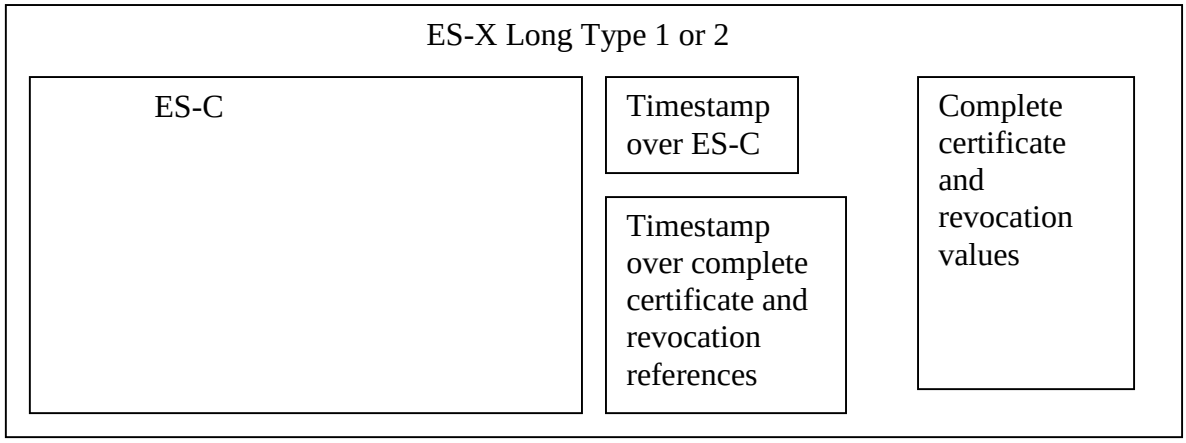
## 5. Rozšířený elektronický podpis s časem, typ 2. - ES-X Type 2

Tento formát (typu 1) přidává k formátu ES-C atribut ES-C-time-stamped-certs-crls-references, jehož obsahem je časové razítko přes certifikační cestu a odkazy na příslušné informace o revokacích. Toto poskytuje formátu integritu a důvěryhodnou ochranu v čase těchto odkazů. Může tak ochránit certifikáty, CRL a odpovědi OCSP v případě pozdější kompromitace klíče CA (či klíče pro podepisování CRL či odpovědí OCSP). Oba dva typy podpisů (ES-X Type 1 a ES-X Type 2) směřují k ochraně proti týmž hrozbám a který z těchto dvou typů bude použit, závisí na konkrétním prostředí.



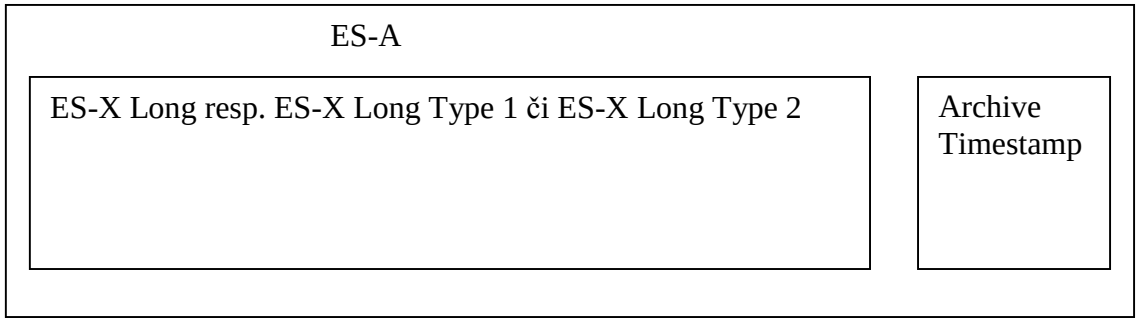
## 6. Rozšířený dlouhý elektronický podpis s časem - - ES-X Long Type 1 a 2

Tento formát je podle specifikace v dokumentu [1] kombinací formátu ES-X Long a jednoho z formátů ES-X Type 1 + ES-X Type 2.




## 7. Archivační elektronický podpis, ES-A

Tento formát ES-A přidává k formátům ES-X Long resp. ES-X Long Type 1 či ES-X Long Type 2 jeden nebo více atributů typu archive-time-stamp. Formát je používán pro archivaci podpisů s dlouhodobou platností. Následná časová razítka ochraňují celý materiál jak proti oslabením hashovacích funkcí, tak i proti oslabením kryptografických funkcí či algoritmů.




V příloze B jsou popsány detaily rozšířených formátů, požadované nepodepsané atributy pro každý typ a také jak mohou tyto atributy být využity při ověřování elektronického podpisu. K této příloze a také k dalším definicím některých atributů zase v příštím pokračování.

## 8. Literatura

[1] ETSI TS 101 733, V.1.5.1, Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
[2] RFC 3126, Electronic Signature Formats for long term electronic signatures

# D. Test elektronickej svojprávnosti

**Ing. Andrej Olejník, ASSET Soft a.s., (**andrej.olejnik@assetsoft.sk **)**
**Mgr. Ivan Pullman, ASSET Soft a.s., (**ivan.pullman@assetsoft.sk **)**

Elektronický podpis, digitálny podpis, certifikačná autorita – takto by sa dalo pokračovať vo vymenúvaní pojmov spojených s dnešnou dobou. To, že k dnešnej dobe patria, svedčia čoraz častejšie sa vyskytujúce články v médiách venované tejto problematike. Nakoľko rozumiete týmto pojmom si môžete otestovať v nasledujúcom teste. Skôr, ako sa doň pustíte, dovolím si uviesť pár viet prečo tento test vznikol.

V prípade vlastnoručného podpisu človek intuitívne rozumie podstate takto vytvoreného podpisu. Elektronický podpis sa však od vlastnoručného výrazne odlišuje v postupoch ako vzniká a ako sa overuje. Ak máme začať používať elektronický podpis masovo, mali by sme vedieť na akých princípoch je založený a aké povinnosti vyplývajú pre používateľov. Neznalosť zákona neospravedlňuje, rovnako aj nepochopenie obchodných podmienok (certifikačných autorít, uzavretých PKI riešení).

Dnes neexistuje základné vzdelávanie v oblasti používania elektronických podpisov. Rovnako ani postupy ako overiť, či príslušná osoba ovláda základy používania elektronického podpisu. Veľa článkov v neodbornej tlači a na internete obsahuje zavádzajúce informácie a potvrdzuje neznalosť autorov a nepochopenie základných princípov elektronického podpisu. Z tohto dôvodu vznikol tento test. Doposiaľ nikto nezaviedol pojem ako elektronická svojprávnosť. Ak je človek svojprávny automaticky sa predpokladá, že bude schopný používať aj elektronické prostriedky, ktoré nahrádzajú vlastnoručný podpis. Či je tento predpoklad správny si môžete ľahko overiť. Stačí ak tento test dáte vyplniť pár ľuďom z oblasti IT. Pravdepodobne budete nemilo prekvapení.

Test nie je kompletný z hľadiska reálneho používania (zaručeného) elektronického podpisu. Pre kompletnosť by si vyžadoval aj overenie vedomostí pri používaní softvéru a hardvéru, ktorý sa používa pre vytváranie a overovanie (zaručeného) elektronického podpisu. Test neprešiel kvalifikovanou oponentúrou a nebol nikým schválený. Je to len prvý pokus ako si overiť vedomosti ohľadne elektronického podpisu. V teste sú skryté aj základné chyby, ktoré sa najčastejšie vyskytujú v článkoch novinárov a na webových stránkach (ďakujem p. Vondruškovi za jeho obľúbené slovné spojenia).

Upozorňujem na rozdielnosť odpovedí v poslednej časti spôsobenú nejednotnosťou legislatívy. Na Slovensku, v Českej republike a v EÚ máme nekompatibilnú legislatívu v oblasti zaručeného elektronického podpisu. Preto je posledná IV. časť venovaná zaručenému elektronickému podpisu problematická a správne odpovede sa v rôznych štátoch môžu líšiť. Niektoré odpovede môžu byť diskutabilné, často sa môžu vyskytnúť rôzne „ale“, ktoré môžu viesť k zmene odpovede. Cieľom nie je vyriešiť test na jednotku, ale overiť si základné vedomosti.

Ak odpoviete na väčšinu otázok správne, môžete používať elektronický podpis a zaručený elektronický podpis bez obáv. Ak nie, je vhodné si svoje vedomosti doplniť tak, aby nenastali pochybnosti o tom, či elektronické podpisy realizujete a overujete na základe správnych vedomostí.

Správne odpovede a vyhodnotenie nájdete na konci testu. Pre každú otázku je možné vybrať jednu odpoveď. Za každú správnu odpoveď získavate jeden bod.

# Test elektronickej svojprávnosti

## I. časť - Certifikát (certifikáty verejného kľúča)

### 1. Certifikáty vydáva

a) certifikačná organizácia
b) certifikačná autorita
c) certifikačná spoločnosť, ktorá je oprávnená certifikovať

### 2. Aká je platnosť certifikátu?

a) je neobmedzená rovnako ako u vlastnoručného podpisu
b) je obmedzená na jeden kalendárny rok a začína vždy 1. januára
c) je uvedená v certifikáte
d) certifikát nemá určenú platnosť

### 3. Môžem mať vydaných viac certifikátov?

a) áno
b) nie, rovnako ako mám len jeden vlastnoručný podpis
c) áno, ale maximálny počet je obmedzený na 3 certifikáty
d) od každej certifikačnej autority môžem mať vydaný len jeden certifikát

### 4. Čo musím urobiť ak stratím svoj certifikát?

a) nemusím robiť nič, certifikát získam z certifikačnej autority
b) musím okamžite hlásiť stratu certifikačnej autorite
c) musím okamžite hlásiť stratu certifikačnej autorite a všetkým partnerom

### 5. Kto vydáva kvalifikované certifikáty?

a) každý poskytovateľ certifikačných služieb
b) zaručený poskytovateľ autorizačných služieb
c) akreditovaná certifikačná autorita
d) kvalifikovaný registrátor

### 6. Ako si overím platnosť certifikátu?

a) pozriem sa kedy platí a kto ho vydal, ak poznám vydavateľa a je dôveryhodný tak je certifikát platný
b) telefonicky kontaktujem majiteľa a overím si, či je certifikát platný
c) overím si, či certifikát nie je na zozname zrušených certifikátov u certifikačnej autority, ktorá certifikát vydala alebo použijem aplikáciu, ktorá zabezpečí overenie platnosti certifikátu u vydavateľa certifikátu
d) certifikát vydala certifikačná autorita a tá je dôveryhodná, preto nepotrebujem overovať či je certifikát platný

**7. Ako sa mení certifikát vydaný k môjmu verejnému kľúču?**

a) certifikát sa nemení
b) certifikát sa aktualizuje vždy po podpise, v certifikáte sa mení dátum vystavenia posledného elektronického podpisu
c) certifikát sa aktualizuje iba pri zmene letného času na zimný a naopak

**8. Čo musím chrániť ako oko v hlave?**

a) môj certifikát
b) môj súkromný kľúč
c) môj verejný kľúč
d) môj súkromný kľúč a verejný kľúč
e) môj súkromný kľúč, verejný kľúč a môj certifikát

## II. časť - Súkromný kľúč

**9. Ako mi je doručený súkromný kľúč?**

a) súkromný kľúč generuje certifikačná autorita a dodáva ho spolu s certifikátom
b) súkromný kľúč je uložený v certifikáte
c) súkromný kľúč mi nikto nedoručuje

**10. Je potrebná ochrana môjho súkromného kľúča?**

a) nie je potrebná ochrana, je bezpečne uložený v certifikačnej autorite
b) áno, musím ho chrániť, tak aby ho nikto nemohol zneužiť
c) nie je potrebná ochrana, je potrebný len na vygenerovanie certifikátu

**11. Čo musím urobiť, ak stratím môj súkromný kľúč alebo mám podozrenie na zneužitie môjho súkromného kľúča?**

a) musím to hneď nahlásiť verifikačnej autorite a požiadať o zrušenie platnosti súkromného kľúča
b) musím to hneď nahlásiť certifikačnej autorite a požiadať o zrušenie certifikátu
c) nemusím urobiť nič, moje elektronické podpisy nie sú ohrozené
d) nemusím urobiť nič, certifikáty nie sú ohrozené

**12. Ak niekto zneužije môj súkromný kľúč, dá sa to zistiť z elektronického podpisu?**

a) áno, tak ako u vlastnoručného podpisu to dokáže zistiť grafológ, u elektronického podpisu to dokáže zistiť kryptológ
b) áno, musím však mať certifikát
c) nie, nie je to možné

## III. časť - Elektronický podpis

### 13. Čo je to elektronický podpis?

a) je to naskenovaný vlastnoručný podpis
b) dáta v elektronickej podobe, ktoré sú pripojené k iným elektronickým dátam a sú s nimi logicky spojené, rovnako aj s osobou, ktorá podpis vystavila
c) je to vlastnoručný podpis prevedený do elektronickej podoby a pripájaný k dátam ako obrázok vlastnoručného podpisu

### 14. Je elektronický podpis pre človeka rovnako čitateľný ako vlastnoručný podpis?

a) áno, rovnako ako vlastnoručný podpis, aj keď ten je niekedy ťažšie čitateľný
b) áno, ale na prečítanie je potrebný krátky tréning
c) nie, sú to dáta v elektronickej podobe

### 15. Zabezpečuje elektronický podpis aj šifrovanie dokumentu?

a) áno
b) závisí to od aplikácie
c) nie

### 16. Môžem elektronicky podpísať ľubovoľný elektronický dokument?

a) áno
b) áno, obrázky a iné multimediálne súbory však nie
c) nie, iba textové dokumenty

### 17. Kto overuje platnosť elektronického podpisu dokumentu?

a) certifikačná autorita
b) registračná autorita
c) platnosť overuje príjemca alebo hocikto, kto má k dispozícii certifikát a aktuálny zoznam zrušených certifikátov
d) iba kvalifikovaný kryptológ

### 18. Ako rýchlo dokáže odhaliť kvalifikovaný kryptológ elektronický podpis, ktorý bol vytvorený ukradnutým súkromným kľúčom?

a) závisí to od okolností a odborných znalostí kryptológa
b) takýto elektronický podpis sa nedá odlíšiť od iných elektronických podpisov a nie je možné zistiť, či bol realizovaný ukradnutým súkromným kľúčom
c) závisí to od dĺžky kľúča a použitého šifrovacieho algoritmu

### 19. Kde si môžem kúpiť elektronický podpis?

a) v certifikačnej autorite
b) v registračnej autorite
c) v akreditovanej certifikačnej autorite
d) v certifikačnej autorite, každoročne vám vydajú nový elektronický podpis
e) elektronické podpisy sa nepredávajú

**20. Koľko stojí vyhotovenie elektronického podpisu?**

a) cenu určuje certifikačná autorita
b) cenu nie je možné priamo vyčísliť
c) cenu určuje zákon
d) cenu určuje registračná autorita

**21. Kde je uložený môj elektronický podpis?**

a) je uložený na tokene alebo diskete (disku) spolu s certifikátom
b) je pripojený alebo logicky spojený s podpísaným dokumentom, môže byť uložený s podpísaným dokumentom alebo samostatne
c) je uložený v certifikačnej autorite tak, aby ho bolo možné použiť na overenie v prípade sporov
d) je uložený v certifikačnej autorite tak, aby ho bolo možné použiť na overenie v prípade sporov a aby certifikačná autorita mohla potvrdzovať pravosť môjho podpisu

**22. Je elektronický podpis pre rôzne dokumenty stále rovnaký?**

a) áno, podobne ako vlastnoručný podpis
b) áno, jeho základná podoba je daná certifikátom vygenerovaným v certifikačnej autorite
c) nie, vždy je iný

## IV. časť - Zaručený elektronický podpis

**23. Akú právnu hodnotu má zaručený elektronický podpis spojený s kvalifikovaným certifikátom vydaným akreditovanou certifikačnou autoritou?**

a) je rovnocenný s vlastnoručným podpisom
b) je rovnocenný s elektronickým podpisom
c) je rovnocenný s elektronickým podpisom a zároveň rovnocenný s vlastnoručným podpisom
d) ani jedno predchádzajúce tvrdenie nie je správne

**24. Môžem elektronicky podpísať zaručeným elektronickým podpisom ľubovoľný elektronický dokument určený pre účely administratívneho styku?**

a) áno
b) áno, ale iba textové dokumenty
c) nie, iba schválené formáty dokumentov

**25. Môžem elektronicky podpísať zaručeným elektronickým podpisom dokument vo formáte MS Word (prípona DOC) a použiť ho pre účely administratívneho styku?**

a) áno
b) áno, ale iba bez obrázkov
c) áno, ale nesmie to byť farebný dokument
d) nie

**Správne odpovede**

**Pre Slovensko:**
1b, 2c, 3a, 4a, 5c, 6c, 7a, 8b, 9c, 10b, 11b, 12c, 13b, 14c, 15c, 16a, 17c, 18b, 19e, 20b, 21b, 22c, 23a, 24c, 25d

**Pre Českú republiku:**
1b, 2c, 3a, 4a, 5c, 6c, 7a, 8b, 9c, 10b, 11b, 12c, 13b, 14c, 15c, 16a, 17c, 18b, 19e, 20b, 21b, 22c, 23d, 24a, 25a
*pozn.: správne odpovede pre Českú republiku (otázky 23,24 a 25) navrhol p. Vondruška.*


**Vyhodnotenie**

Za každú správnu odpoveď si môžete dať bod. Potom je vaše celkové hodnotenie nasledovné:

**1-10 bodov** - študovať, študovať, študovať, ste nesvojprávny pre používanie elektronického podpisu (neberte to doslovne)
**11-15 bodov** - potrebujete sa vzdelávať, veľa vašich povinností a fungovanie elektronického podpisu vám nie je jasné
**16-19 bodov** - po krátkom vzdelávaní dosiahnu vaše vedomosti potrebnú úroveň
**20-25 bodov** - vaše vedomosti sú na výbornej úrovni

---

[1] Zákon o elektronickom podpise a o zmene a doplnení niektorých zákonov 215/2002 Z.z. http://www.nbusr.sk/NBU_SEP/215.html

[2] Úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu),jak vyplývá ze změn provedených zákonem č. 226/2002 Sb., zákonem č. 517/2002 Sb.a zákonem č. 440/2004 Sb.
http://www.micr.cz/files/1540/UZ-227_2000.pdf

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/esignatures_en.pdf

# E. VOJNIČŮV RUKOPIS - výzva

**Jan B. Hurych** (hurychj@tnt21.com)

*Možná, že jste už četli v novinách o nedávném výzkumu Angličana Gordona Rugga, který prohlásil, že tento rukopis (tj. VM), označovaný podle jeho nálezce, antikváře Vojniče (autor je neznámý), je zřejmě hoax, čili podvrh, a že neobsahuje nic jiného než zakódovaný text beze smyslu (viz např. článek v loňském Crypto-Worldu 1/2004, Voynichův rukopis). A ještě dodává, že autorem je patrně alchymista a šarlatán Kelley - celá známá historie rukopisu se totiž točí kolem Prahy a první historicky prokázaná osoba s rukopisem spojená je Jakub Horčický, jehož jméno je dokonce v samotném rukopise, ale bylo později částečně vymazáno a Vojnič je uviděl až pod ultrafialovým světlem. Část je mimochodem vidět i dnes, kdy University of Yale pořídila nádherné barevné skany celého rukopisu).*

O rukopise jsem se prvně dozvěděl asi před deseti lety ze světoznámé knihy nestora kryptografů, Davida Kahna, *The Codebreakers.* Co uchvátilo mou pozornost, nebylo jen to, že rukopis je napsán neznámým písmem v neznámem jazyce nebo že je nazýván "nejzáhadnějším rukopisem na světě", ale i to, že byl v jedné době též ve vlastnictví rektora Karlovy univerzity, mojí Alma Mater, jehož dopis přiložený k rukopisu se též zachoval. Studoval jsem rukopis delší dobu, než jsem se odvážil napsat článek do mého netového časopisu Hurontaria, zprvu jen anglicky. Článek si ale získal pozornost, přidal jsem tedy jeho českou verzi, založil dvoujazyčnou stránku o časopise a později napsal i celou knihu "Záhadný rukopis", tj. v češtině a to v elektronické verzi.

Nejsou to jen dějiny rukopisu, které jsou tak zajímavé, ale hlavně to, že téměř čtyři sta let se lidé pokouší rozluštit tuto záhadu, rukopis, který ač byl vytvořen pravděpodobně jen jedním autorem, dosud vzdoruje velkému počtu vědců i nejmodernější technologii, hlavně tedy počítačům. Po čase jsem se stal členem mezinárodní konference, kde na Internetu diskutujeme současné objevy a pokrok ve světovém výzkumu VM a založil jsem i českou *Skupinu SVM*, kde máme několik odborníků na historii, lingvistiku, botaniku, astronomii a podobně. Jde totiž o to, že mezinárodnímu výzkumu chybí hlavně data z Čech, ale bohužel zájem dosud není takový, jak by se dalo očekávat. Co nám chybí, jsou odborníci na kryptografii - a to je důvod, proč píši tento článek, který váš webmaster laskavě souhlasil zde zveřejnit.

Nejde nám ovšem jen o to dokázat, zda má Mr. Rugg pravdu či ne - už ostatně na svém důkazu pilně pracuje - ale o celkový výzkum rukopisu vůbec. Ať už je to podvrh nebo ne, je to vědecky i umělecky zajímavý objekt a nakonec i část českých dějin (první tři majitelé byli Češi). A zatímco cizina už pokročila ve výzkumu dost daleko, česká složka má co dohánět. Nedávno jsme sice umožnili v Praze pobyt panu René Zandbergenovi z Holandska, který navštívil strahovskou knihovnu, kde objevil jiný rukopis, také z Horčického majetku a dokonce i místo narození druhého majitele, Bareše. Nám jde ale hlavně o to, abychom získali více našich, českých, objevů či poznatků.

Snad jen stručně o rukopisu samém: má kolem 204 stránek, je psán abecedou, která je na světě zcela unikátní a jinak zcela neznámá. Jeho rozložení "slov" je takové, že mu chybí delší slova, jeho "gramatika" taková, že se zatím její obdoba u jiných jazyků nenašla. To vše naznačuje, že jde spíše o zakódování než otevřený text. Navíc obsahuje kresby bylin, které se

nepodobají skutečným rostlinám a i jiné obrázky, které mohou mít skrytý význam. Není divu, že první, co člověka napadne, je domněnka, že to vše nedává smysl, ale dlouholeté studium už nalezlo v rukopisu mnoho zajímavých souvislostí dokazujících, že se jedná o značně promyšlené dílo a rukopis bude ještě dlouho inspirovat ty, kteří mají zájem o záhady a jejich řešení.

Tak například písmo: autor zřejmě sestavil svou abecedu ze segmentů, jejichž kombinace lze seřadit do čtvercové tabulky a navíc je samotné písmo vcelku velmi elegantní. Jedna evropská skupina sestavila už celý *transkript* pomocí své abecedy EVA a snaží se rozluštit text. Podobně frekvenční charakteristiky písmen a slov ukazují charakteristiky přirozeného (tedy ne umělého) jazyka a i studie entropie druhého řádu je zajímavá, nemluvě už o aplikaci Zipfových zákonů. Nejzajímavější je ovšem možný způsob zakódování. V té době (řekněme šestnácté století, původ se odhaduje někde mezi koncem čtrnáctého a koncem šestnáctého století, ale odhady se liší) už znali transpoziční i substituční šifru (i s více abecedami), Cardanovu mřížku či matricovou šifru a dokonce i *steganografii* (viz Baconova šifra, používající už to, co dnes nazýváme binárním počtem) a nevylučuje se ani nějaký kód v obrázcích.

Naše skupina už dosáhla určitých úspěchů - nalezli jsme například pravý podpis Horčického v archivu mělnického zámku (kde byl Horčický hejtmanem, než byl zajat, vyměněn za Jana Jesenia a poslán do exilu), nová fakta o Barešovi a Tadeášovi Hájkovi, dokonce jsme nalezli v rukopise i přemalovaná čísla, která by mohla nějak vést k vyluštění. Co nám hlavně chybí, jsou ale odborníci na šifry - proto se zde obracím na studenty tohoto oboru - a také lidé s chutí objevovat. Pochopitelně nikomu nedáváme úkoly či instrukce co a jak dělat (nevylučujeme ani výzkum podél linií pana Rugga), jen žádáme, aby se členové podíleli se svými zkušenostmi s ostatními ve skupině. Tím se dosáhne nejen jisté koordinace, ale zároveň to pomůže i ostatním, kteří se tak doví, že to, co dělají, už někdo jiný někdy zkoušel anebo ne.

Také dáváme členům naší skupiny možnost publikovat své výsledky na Netu, na naší stránce, ta je na http://hurontaria.baf.cz/VM/ kde je popsána historie rukopisu, nejdůležitější poznatky, historie řešení, reference a kopie některých dokumentů přeložených do češtiny. Také tam vedeme zajímavé diskuse a popisujeme všechny nové objevy. Stránka je dvoujazyčná a je běžně navštěvována odborníky z ciziny. Každý člen/členka má možnost si stáhnout zdarma z Netu knihu "Záhadný rukopis" a využívat možnost konzultací s kýmkoliv z našeho klubu. Členství je pochopitelně také zdarma a je to i příležitost k osobnímu prosazení, tak např. naše redaktorka udělala úspěšné interview s už jmenovaným panem Zandbergenem a zveřejnila jej v českém tisku. Já sám jsem byl vyzván k interview pro *Prager Tagblatt* a jak je vidět, zájem o VM neutichá.

Co dodat? Máte-li zájem, podívejte se na naši stránku a chcete-li se státi členy nebo i jinak nám pomáhat, napište mi na adresu níže. Vítáme i ty, kteří si sami netroufají na samotný výzkum, ale rádi by se dovídali novinky z výzkumu a případně pomáhali jako dobrovolníci.

Jan B. Hurych,
hurychj@tnt21.com
předseda české SVM

# F. O čem jsme psali v lednu 2000 – 2004

**Crypto-World 1/2000**



**Crypto-World 1/2001**



Příloha:
trustcert.pdf (upoutávka na služby Certifikační Autority TrustCert)

**Crypto-World 1/2002**



**Crypto-World 1/2003**



Příloha : Crypto_p1.pdf
CEN Workshop Agreements (dokumenty vztahující se k elektronickému podpisu)

**Crypto-World 1/2004**

# G. 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@pvt.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/ |