Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 11, číslo 4/2009 **15.duben 2009**

4/2009

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1315 registrovaných odběratelů)

Obsah :

Příloha: april.htm (ukázka aprílového žertíku s využitím XSS zranitelnosti)

A. Apríl (který se však až tak úplně nekonal)

Těsně před prvním dubnem mne kontaktoval Roman Kümmel, ze serveru http://soom.cz/ a požádal mne, zda bych se nechtěl připojit k aprílovému žertu, který připravují. Přesněji, zda bych v Security-News na našem serveru (http://crypto-world.info/news/index.php) nezveřejnil dne 1.4 následující příspěvek.

Nebezpečný počítačový virus napadá uživatele PC

Po Internetu se rychle šíří nebezpečný počítačový virus, který zatím jako jediný dokáže infikovat i samotné uživatele počítače. Virus má na svědomí již několik prvních obětí, a protože je vývoj protilátky stále v začátcích, očekává se brzké vypuknutí epidemie. Proti viru se dá úspěšně bránit prověřeným firewallem a zkrácením času stráveného u počítače. Jako první o tom dnes informovala televize NOVA v této reportáži na tv.nova.cz.

Pokud čtenář klikl na klíčové slovo "*v této reportáži*", tak se aktivoval odkaz [2], který díky XSS zranitelnosti stránky TV NOVA měl vyvolat dojem, že následující obrazová reportáž se přehrává z originální stránky této televize. Je fakt, že obsah reportáže již určitě nikoho nenechal na pochybách, že se jedná o povedený aprílový žertík.

Odmítl jsem tuto spolupráci, neboť ne všichni mají pochopení pro tento druh humoru a jistě by se našla řada různých komentářů o šíření poplašné zprávy, nedovoleném porušování copyrightu TV NOVA, nezákonné napadení stránky této televize, neseriózności našeho serveru a propůjčení se nízké zábavě…

Na druhou stranu mne to opravdu pobavilo a myšlenka uvedeného žertíku s ukázkou využití XSS zranitelnosti se mi velmi líbila. Nejprve jsem jej rozeslal svým známým, a když jsem uviděl, jaký měl u nich kladný ohlas, rozhodl jsem se o něm podělit touto cestou i s vámi - čtenáři Crypto-Worldu.

Poznámka na závěr, připravený pěkný aprílový žertík zveřejnil 1. 4. 2009 server soom.cz na své stránce [1]. Tentokrát se sice jednalo o aprílový žertík, ale stojí za zamyšlení, co by podobná chyba mohla způsobit, pokud by byla zneužita s jiným záměrem.

[1] http://www.soom.cz/
[2]
http://tv.nova.cz/hledat?search=Nebezpecny%20virus.....
.....
.....
.....
.....%3C%2F%73%63%72%69%70%74%3E%3C%64%69%76%20%61%6C%69%67%6E%3D%63%65%6E%74%65%72%3E%3C%69%66%72%61%6D%65%20%73%72%63%3D%68%74%74%70%3A%2F%2F%77%77%77%2E%73%6F%6F%6D%2E%63%7A%2F%64%61%74%61%2F%72%65%70%6F%72%74%61%7A%2E%68%74%6D%6C%20%77%69%64%74%68%3D%35%34%30%20%68%65%69%67%68%74%3D%33%32%34%3E%3C%2F%69%66%72%61%6D%65%3E%3C%2F%64%69%76%3E%3C%62%72%3E%3C%62%72%3E%3C%73%63%72%69%70%74%3E

B. Popis a principy EDON-R

Vlastimil Klíma, nezávislý konzultant - kryptolog, Praha,
(http://cryptography.hyperlink.cz, v.klima@volny.cz)

Úvod

O SHA-3 se v Crypto-Worldu píše přímo i nepřímo už od začátku tohoto roku, nicméně podrobné informace může čtenář nalézt na spoustě míst na internetu, například na [1 - 11]. EDON-R je velmi zajímavým kandidátem na nový hašovací standard v rámci soutěže SHA-3, protože je ze všech nejrychlejší. V současné době jsem spoluautorem návrhu EDON-R, i když můj vztah k algoritmu prodělal různé změny. Nejprve jsem byl o algoritmu kolegiálně zpraven jeho duchovním otcem Danilem Gligoroskim v době, kdy jsme společně pracovali na Blue Midnight Wish (BMW), ale až do okamžiku jeho publikace jsem ve skutečnosti o něm nic nevěděl. Seznámil jsem se s ním jako s největším konkurentem BMW po zveřejnění všech kandidátů. Nejprve jsem byl jeho kritikem, což vyústilo v kryptoanalýzu [15], poukazující na jednu nevýhodnou vlastnost. Poté jsme s Danilem přirozeně začali diskutovat o možnostech zlepšení. Bylo to náročné a trvalo to velmi dlouho a dosud trvá, protože to vyžaduje novou kryptoanalýzu. To pak vyústilo v Danilovo rozhodnutí, že jsem se de facto stal spoluautorem, proto mě zařadil při první oficiální příležitosti do týmu. To nastalo v lednu 2009 před první konferencí kandidátů, kdy předkladatelé mohli zaslat drobné opravy dokumentace (překlepy, oprava nepřesností v SW, apod.) [12]. Na první konferenci kandidátů SHA-3 [13] byli pak představeni všichni spoluautoři EDON-R a jejich úloha v týmu ([13]). Velice mě to potěšilo, na druhé straně je to velká zodpovědnost a ohromná dobrovolná pracovní zátěž. Mít v takové soutěži dva nejrychlejší kandidáty znamená nejen čest, ale občas i vražedné pracovní nasazení. Nevěřili byste, jaké ohromné množství práce se za jednotlivými návrhy skrývá a co práce a prostředků NIST ušetří, když si nechá zdarma vytvořit standard v mezinárodní soutěži. Člověk si myslí, že se nic neděje a mezitím na analýze a prolamování kandidátů velmi tvrdě pracuje mnoho desítek špičkových kryptologů, které by NIST jen tak nezaplatil. Samozřejmě, že je pro autory bolestné, když někdo najde v jejich funkci chybu. Jejich odhalování je ale přímo náplní soutěže a povinností všech účastníků, i vzhledem ke svým algoritmům! S velmi klidným svědomím můžu prohlásit, že kdybych našel nějakou chybu v BMW nebo EDON-R, tak bych ji publikoval. A předpokládám, že drtivá většina ostatních účastníků by to u svých algoritmů udělala také.

Vznik EDON-R

Vznik EDON-R je poměrně dlouhý, první návrh této funkce pochází z roku 2006 na konferenci [17], kde byla představena jen teoretická východiska, ale nikoli konkrétní náplň. Základním stavebním prvkem jsou kvazigrupy. Právě možnost jejich rychlé implementace posunula EDON-R na první místo v rychlosti. Jsou kritikové, kteří by rádi EDON-R diskvalifikovali a odsunuli do prolomených algoritmů (viz například stránka Nielse Fergusona z Microsoftu, spoluautora algoritmu Skein [11]) nebo poukázali na jeho nevýhody (kvazigrupy se jim zdají neprobádanou oblastí). Nebudeme rozvíjet diskuse na tato témata, i když je to moc zajímavé, jenom si řekněme, že podobných výtek bude přibývat a přitvrdí se. V současné době je jisté, že EDON-R tak jak je, je prakticky odolný proti kryptoanalýze podle představy NIST o bezpečnosti, prezentované na první konferenci SHA-3 (přednáška M. Nandiho z NIST, [7]). Zároveň jsme s Danilem oznámili, že pracujeme na drobné změně (tzv. tweak), která bude NISTem povolena u všech kandidátů, kteří postoupí do druhého kola. Tento tweak je nutný pro to, aby EDON-R mohl být vítězným kandidátem. Vítěz by měl odolat i teoretickým útokům, které byly prezentovány v [18 - 21]. Takovou opravu není jednoduché navrhnout, protože by neměla narušit (změnit) existující kryptoanalýzu a

nesnižovat rychlost. Navíc by měla být malá, aby neměnila zásadní konstrukci algoritmu, ale zároveň velká silou obrany.

Společné rysy EDON-R, BMW a SHA-2

Připomeňme si v krátkosti, co mají EDON-R, BMW a SHA-2 společné. Jsou založeny na iterativním principu a kompresní funkci. Zpráva, která se má hašovat, se doplní definovaným způsobem tzv. paddingem a počtem zpracovávaných bitů původní zprávy a zarovná se na nejbližší násobek délky bloku buď 512/1024 bitů podle toho, zda se jedná o EDON-R256/512 nebo SHA256/SHA512. Potom se tyto funkce shodují v tom, že používají iterativní výpočet s použitím tzv. kompresní funkce (budeme používat označení R z dokumentace EDON-R) a průběžné hašovací hodnoty. Průběžná hašovací hodnota se nastaví na počátku na hodnotu tzv. inicializačního vektoru. Potom se v N krocích vždy ze staré průběžné hašovací hodnoty a daného bloku zprávy pomocí kompresní funkce vytvoří nová hodnota průběžné haše. Poslední průběžná hodnota haše (nebo její část) je pak prohlášena za skutečnou hodnotu haše. Hašování tedy probíhá u EDON-R i SHA-2 podle stejného následujícího scénáře. Poznamenejme, že SHA-2 používá klasické označení H pro průběžnou hašovací hodnotu, zatímco u EDON-R je to označení P (pumpa).

Algorithm: EDON-$\mathcal{R}$

Input: Message M of length l bits, and the message digest size n.

Output: A message digest $Hash$, that is long n bits.

1. Preprocessing
   (a) Pad the message M.
   (b) Parse the padded message into N, m-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
   (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation
   For $i = 1$ to N
   $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
3. $Hash$ =Take_n_Least_Significant_Bits$(P^{(N)})$.

1. Předzpracování

(a) Doplň zprávu M jednoznačným definovaným způsobem o délku zprávy v bitech a doplněk
(b) Rozděl zprávu na celistvý násobek (N) m-bitových bloků $M^{(1)}$, ..., $M^{(N)}$.
(c) Nastav počáteční hodnotu průběžné haše $P^{(0)}$ = IV.

2. Výpočet haše

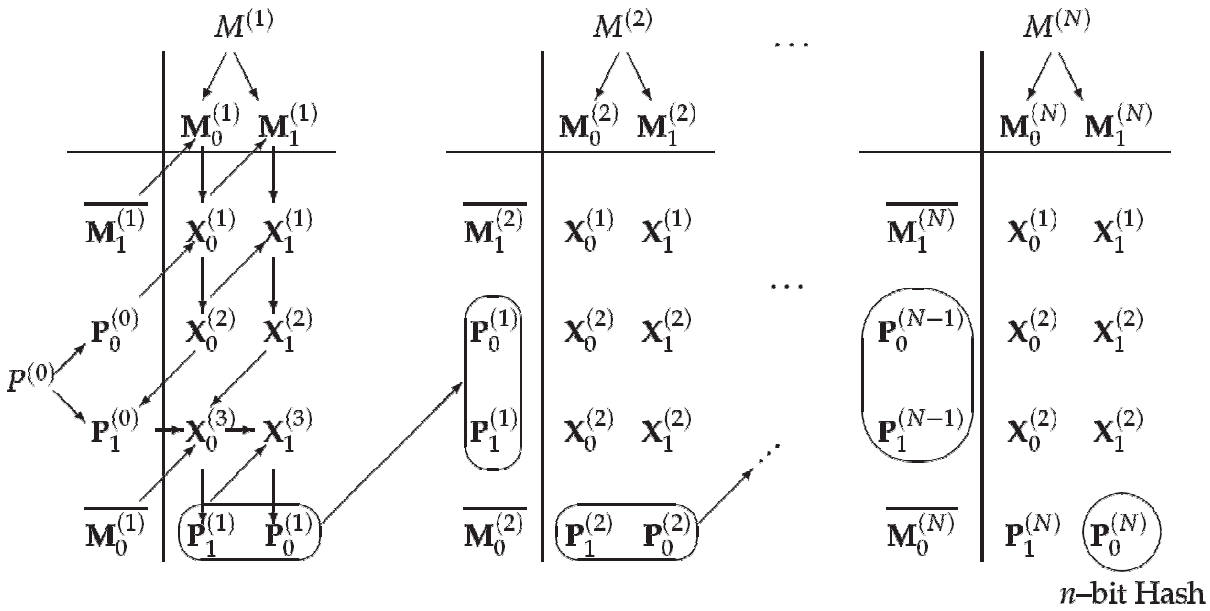
For i = 1 to N
{ $P^{(i)} = R(M^{(i)}, P^{(i-1)})$ }

3. Závěr

H(M) = definovaných n bitů z hodnoty $P^{(N)}$.

Dvojnásobná pumpa

EDON-R používá stejně jako BMW dvojnásobnou pumpu, tedy průběžnou hašovací hodnotu P o délce 2n bitů, kde n je délka haše [16]. To zabraňuje útoku prodloužením zprávy a posouvá složitost Jouxova útoku [14] do nereálna. Kompresní funkce zpracovává také bloky 2n bitů najednou. Obě základní verze EDON-R256/512 používají bloky (P i M) o délce 16 slov, ale liší se délkou použitého slova (w = 32/64 = n/8 bitů), jinak všechny funkce a transformace vypadají až na konstanty stejně. Zpracování zprávy pak probíhá podle následujícího schématu, kde je také vidět závěrečná n-bitová hash.



V jednoduchosti je krása

Celé hašování lze právě zobrazit jen tímto obrázkem. K tomu malý komentář. Na obrázku je vždy dolním indexem 0 nebo 1 označena dolní nebo horní polovina proměnné (tj. 8 w-bitových slov). Proměnné $X^{1,2,3}$ uvnitř mají také dvě poloviny (s dolním indexem 0, 1) a označují průběžné meziproměnné - výsledky kvazigrupové operace Q. Kvazigupová operace Q má dva operandy o 8 slovech (A a B) a výsledkem je také 8 slov C = Q(A, B). Na obrázku je první operand (A) vždy ten odkud vychází *šikmá* šipka, která směřuje do operandu B, a z operandu B jde *vodorovná* nebo *svislá* šipka do výsledku C. Poznamenejme, že rozdělení pumpy P a zprávy M na dvě poloviny $P_{0,1}$ a $M_{0,1}$ je značeno také šikmou šipkou, ale tentokrát to neznamená kvazigrupovou operaci, nýbrž prosté rozdělení na dvě poloviny. Čára nad proměnnou (například nad M_0) znamená obrácení pořadí osmi slov této proměnné. Například první operace, která proběhne je $X_0^1 = Q(M_1^{(1)}$ s čarou, $M_0^{(1)})$.

Kvazigrupová operace

Operace je definována pomocí rychlých a dostupných operací ve všech procesorech: sčítání, xor a bitové rotace.

Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$

where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

1.
$$
\begin{aligned}
T_0 &\leftarrow ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);\\
T_1 &\leftarrow ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);\\
T_2 &\leftarrow ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);\\
T_3 &\leftarrow ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);\\
T_4 &\leftarrow ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);\\
T_5 &\leftarrow ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);\\
T_6 &\leftarrow ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);\\
T_7 &\leftarrow ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);
\end{aligned}
$$

2.
$$
\begin{aligned}
T_8 &\leftarrow T_3 \oplus T_5 \oplus T_6;\\
T_9 &\leftarrow T_2 \oplus T_5 \oplus T_6;\\
T_{10} &\leftarrow T_2 \oplus T_3 \oplus T_5;\\
T_{11} &\leftarrow T_0 \oplus T_1 \oplus T_4;\\
T_{12} &\leftarrow T_0 \oplus T_4 \oplus T_7;\\
T_{13} &\leftarrow T_1 \oplus T_6 \oplus T_7;\\
T_{14} &\leftarrow T_2 \oplus T_5 \oplus T_4;\\
T_{15} &\leftarrow T_0 \oplus T_1 \oplus T_7;
\end{aligned}
$$

3.
$$
\begin{aligned}
T_0 &\leftarrow ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);\\
T_1 &\leftarrow ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);\\
T_2 &\leftarrow ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);\\
T_3 &\leftarrow ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);\\
T_4 &\leftarrow ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);\\
T_5 &\leftarrow ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);\\
T_6 &\leftarrow ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);\\
T_7 &\leftarrow ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);
\end{aligned}
$$

4.
$$
\begin{aligned}
Z_5 &\leftarrow T_8 + (T_3 \oplus T_4 \oplus T_6);\\
Z_6 &\leftarrow T_9 + (T_2 \oplus T_5 \oplus T_7);\\
Z_7 &\leftarrow T_{10} + (T_4 \oplus T_6 \oplus T_7);\\
Z_0 &\leftarrow T_{11} + (T_0 \oplus T_1 \oplus T_5);\\
Z_1 &\leftarrow T_{12} + (T_2 \oplus T_6 \oplus T_7);\\
Z_2 &\leftarrow T_{13} + (T_0 \oplus T_1 \oplus T_3);\\
Z_3 &\leftarrow T_{14} + (T_0 \oplus T_3 \oplus T_4);\\
Z_4 &\leftarrow T_{15} + (T_1 \oplus T_2 \oplus T_5);
\end{aligned}
$$

Jak je vidět, na 8 slov prvního operandu Q(X, Y) je v prvním kroku aplikována nejprve aritmetická bijektivní transformace, a to převod dílčích slov na jejich součty po pěticích. Dále je vždy každé výsledné slovo rotováno a v druhém kroku je na výsledek aplikována tentokrát lineární transformace, a to vždy tři binární součty (xor) dílčích slov. V druhém kroku vzniká operace, kterou označujeme také π_2 a výsledkem je $\pi_2(X)$, bijektivní obraz X. Podobně druhý argument Y je pomocí podobné ale odlišné transformace π_3 převeden na obraz $\pi_3(Y)$. Oba dva obrazy jsou sečteny a slova výsledku mírně permutována permutací označovanou π_1 (permutaci vidíte v kroku 4, kde pořadí slov proměnné Z je posunuto oproti 0,.., 7). Máme tak alternativní zápis pro $Q(X, Y) = \pi_1(\pi_2(X) + \pi_3(Y))$.Jak je vidět, není tady nic neobvyklého, avšak za návrhem stojí velmi hezká teorie Latinských čtverců. Dále tato volba kvazigrupové operace umožňuje odhadnout diferenciální charakteristiky celé kompresní funkce R a tím kvantitativně dokázat odolnost proti diferenciální kryptoanalýze. Pochopitelně složitost kryptoanalýzy je založena podobně jako u BMW na neschopnosti řešit složité nelineární

soustavy booleovských rovnic o mnoha neznámých, což je známý NP-úplný problém. Navíc je zde problém řešení soustavy kvazigrupových rovnic.

Výkonové charakteristiky
Rychlostní charakteristiky jsou nejlepší ze všech algoritmů, měří se v počtech cyklů procesoru, nutných na zpracování jednoho bajtu (vypočítaný poměrně z počtu cyklů nutných pro zpracování dlouhých zpráv). Spotřeba paměti je trochu vyšší než u některých konkurentů, ale rozdíl ani absolutní hodnoty nejsou velké. Charakteristiky ukazuje slajd z přednášky [13].

Software performances of the optimized C implementation on the NIST reference platform

Intel C++ v11.0.66, in 64-bit mode
EDON-R 224/256 achieves **4.54 cycles/byte**

Intel C++ v11.0.66, in 64-bit mode
EDON-R 384/512 achieves **2.29 cycles/byte**

Memory requirements

EDON-R 224/256 needs **256 bytes**

EDON-R 384/512 needs **512 bytes**

HW – gate count

EDON-R 224/256, ~13,000 gates

EDON-R 384/512, ~25,000 gates

8-bit MCU (ATmega16, ATmega406)

EDON-R 224/256, compiled C code produces ~6KB of machine instructions, speed 616 cycles/bytes

EDON-R 384/512, compiled C code produces ~38KB of machine instructions, speed 1857 cycles/bytes

Kritika
Samotná kvazigrupová operace není jednocestná, ale R jako celek je jednocestná v případě, že neznáme zprávu M. Tedy ze znalosti nové i staré hodnoty pumpy nelze určit M. Avšak při znalosti nové hodnoty pumpy a M lze dojít k předchozí hodnotě pumpy. Tato vlastnost se nezdála být na počátku nebezpečná, ale ukázalo se, že je nevhodná, i když nepřinesla žádný *přímý* útok. Proto bude vhodné navrhnout opravu tak, aby funkce R byla jednocestná i v tomto druhém případě. Podrobnější popis, analýzu a průběžné novinky je možné sledovat na internetu (např. [2]).

Závěr
V tomto článku jsme uvedli základní popis a některé vlastnosti hašovací funkce EDON-R, nejrychlejšího kandidáta na SHA-3. Čtenářům se omlouváme za tak drastické zkrácení popisu a vlastností. Skutečně šlo jen o základní seznámení a poukaz na to, jak je tato funkce elegantní. Podrobnější popis, analýzu a průběžné novinky je možné sledovat na internetu (např. [2]).

Varování ministra fair-play: *jediné nezávislé stránky v následujícím seznamu jsou stránky NIST. Ostatní internetové stránky produkují skupiny a lidé, kteří mají své zájmy v soutěži. Většina těchto stránek to skrývá, nelze je považovat za nezávislé, i když se o to všemožně snaží, a často to tak působí.*

Literatura

[1] (nezávislá) oficiální domácí stránka NIST k projektu SHA-3: http://csrc.nist.gov/groups/ST/hash/index.html
[2] stránka autora s novinkami k projektu SHA-3 a algoritmům BMW a EDON-R: http://cryptography.hyperlink.cz/BMW/BMW_CZ.html (naleznete tam rozcestník a všechny zde uvedené linky)
[3] Stránka kandidátů, kteří postoupili do prvního kola (NIST): http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html
[4] Stránka SHA-3 na wiki: http://en.wikipedia.org/wiki/SHA-3
[5] Stránka SHA-3 projektu ECRYPT: http://ehash.iaik.tugraz.at/index.php/The_SHA-3_Zoo
[6] Seznam všech autorů všech kandidátů: http://ehash.iaik.tugraz.at/wiki/SHA-3_submitters
[7] Stránka NIST, věnovaná první konferenci kandidátů SHA-3: http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/Feb2009/program.html
[8] Stránka o SW výkonnosti algoritmů eBash: http://bench.cr.yp.to/results-hash.html
[9] Stránka (ECRYPT) o HW výkonnosti algoritmů : http://ehash.iaik.tugraz.at/wiki/SHA-3_Hardware_Implementations
[10] Srovnávací stránka Fleischmann-Forler-Gorski: http://www.uni-weimar.de/cms/fileadmin/medien/medsicherheit/Research/SHA3/Classification_of_the_SHA-3_Candidates.pdf
[11] Srovnávací stránka (Niels Ferguson): http://www.skein-hash.info/sha3-engineering
[12] Danilo Gligoroski, Rune Steinsmo Odegard, Marija Mihova, Svein Johan Knapskog, Ljupco Kocarev, Aleš Drápal, Vlastimil Klima: Cryptographic Hash Function EDON-R, homepage of EDON-R (http://www.item.ntnu.no/people/personalpages/fac/danilog/edon-r), the whole submission package (Accepted by NIST, Jan 12, 2009, http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/Edon-RUpdate.zip)
[13] EDON-R presentation at the First SHA-3 Candidate Conference on February 25-28, 2009, http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/Feb2009/documents/Edon-R-Presentation-04-pdf-friendly.pdf
[14] A. Joux: Multicollisions in iterated hash functions. Application to cascaded constructions. Proceedings of Crypto 2004, LNCS 3152, pages 306-316.
[15] Vlastimil Klima: Multicollisions of EDON-R hash function and other observations, November 2008, preliminary analysis, http://cryptography.hyperlink.cz/BMW/EDONR_analysis_vk.pdf
[16] Stefan Lucks. Design principles for iterated hash functions. Cryptology ePrint Archive, Report 2004/253, 2004, http://eprint.iacr.org/2004/253.pdf
[17] SECOND CRYPTOGRAPHIC HASH WORKSHOP, USA, August 24-25, 2006, http://csrc.nist.gov/groups/ST/hash/second_workshop.html
[18] Gaëtan Leurent: Key Recovery Attack against Secret-prefix Edon-R, Cryptology ePrint Archive: Report 2009/135, http://eprint.iacr.org/2009/135.pdf,
[19] Dmitry Khovratovich, Ivica Nikolić, Ralf-Philipp Weinmann: Cryptanalysis of Edon-R, 2008, http://ehash.iaik.tugraz.at/uploads/7/74/Edon.pdf,
[20] Danilo Gligoroski, Rune Steinsmo Ødegård - On the Complexity of Khovratovich et. al's Preimage Attack on EDON-R, http://eprint.iacr.org/2009/120.pdf,
[21] Vlastimil Klima: Multicollisions of EDON-R hash function and other observations, November 2008, http://cryptography.hyperlink.cz/BMW/EDONR_analysis_vk.pdf .

C. Aplikace e-notáře a vícenásobného elektronického podpisu v rámci zavádění ISDS ?

(RNDr. J. Hrubý, CSc., hruby@fzu.cz)

Úvod

V současnosti se v ČR zavádí informační systém datových schránek (ISDS), který by měl zajišťovat bezpečnou a průkaznou elektronickou komunikaci mezi Orgány veřejné moci (dále jen OVM) na straně jedné a fyzickými či právnickými osobami na straně druhé, jakož i mezi OVM navzájem.

Zároveň se k realizaci nabízí uskutečnit projekt aplikace vícenásobného elektronického podpisu společně s důvěryhodným e-archivem, tj. vytvoření služby tzv.„e-notáře“, a to k praktickému využití pro zákazníky mobilních operátorů, zákazníky přímého bankovnictví a státní správu (např. podpisu pro elektronické referátníky), se zastřešením projektu vytvoření důvěryhodného e-archivu s využitím mobilního přístupu, přístupu přes webovské stránky a ostatního telekomunikačního přístupu pro co nejširší okruh zákazníků. Zatím tomu tak není.

Proč tomu tak není, proč není využito např. výzvy Czechinvestu v rámci rozvoje strategie ICT u nás, proč toto neřeší tzv. egoverment, spadající pod MV ČR, zůstává pro mnohé specialisty v oboru otázkou?

Cílem tohoto příspěvku je vyzvat kompetentní pracovníky, aby se nad problémem zamysleli a požadovali nabídku této aplikace, která je ve světě zvládnuta a i u nás byla předmětem výzkumu a vývoje v rámci grantů.

Co by měla nabídka projektu aplikace a-notáře a vícenásobného e-podpisu obsahovat?

Obsahem projektu by měla být realizace aplikace vícenásobného elektronického podpisu dokumentů, vytvoření důvěryhodného elektronického podpisu a aplikace „elektronického notáře“ ve smyslu naplnění legislativy ČR pro informační systémy veřejné správy, bankovnictví a telekomunikačního sektoru, a také s cílem široké využitelnosti jednotlivými zákazníky, těchto sektorů, potřebujících využívat tuto aplikace i jednotlivými občany.
Vícenásobným elektronickým podpisem zde rozumíme vícenásobné podepsání e-dokumentu skupinou občanů, a to dle legislativy ČR.

Elektronickým notářem zde pak rozumíme aplikaci důvěryhodného archivu pro ukládání a archivaci „notářsky“ ověřených elektronických dat široké občanské veřejnosti, a to právně průkazným systémem ve smyslu legislativy ČR. V této fázi nejde o simulování plnohodnotné notářské služby. Jde však o rozšíření služby připravené aplikace ISDS.

Novela zákona č.365/2000 Sb. umožňuje každému občanovi ČR dodání datové zprávy orgánu veřejné moci prostřednictvím portálu veřejné správy a stanovuje podmínky pro použití důvěryhodných elektronických dokumentů (e-dokumentů) ve státní správě. Tím také otevírá prostor pro vznik nových aplikací pro využití služeb elektronického notáře (e-notáře), jehož povinností bude elektronické dokumenty u něj uložené důvěryhodně spravovat, zajistit jejich management, včetně ověření a elektronickou archivaci.

Důvěryhodným e-dokumentem z informačního systému veřejné správy se zde rozumí jakákoliv datová zpráva v elektronické podobě, jejíž výstup z informačního systému veřejné správy je podepsán zaručeným elektronickým podpisem oprávněné osoby správce nebo

označen elektronickou značkou správce, že tento zaručený elektronický podpis nebo elektronická značka jsou platné a jejich kvalifikovaný certifikát nebo kvalifikovaný systémový certifikát nebyly zneplatněny a výstup z informačního systému veřejné správy nebyl následně změněn.

Pro aplikaci vícenásobného el.podpisu a e-notáře je důležitá rovněž existence dokumentu v daném čase, což stvrzuje tzv. kvalifikované časové razítko, ve smyslu novely č.440/2004 Sb. zákona o elektronickém podpisu, které v současnosti poskytuje akreditovaná certifikační autorita (např. I.CA, PostSignum, e-Identity).
Rovněž je důležité zaznamenání telekomunikačního spojení čísla, které vyžaduje službu e-notáře, u mobilního operátora, lokalizace čísla a zaslání potvrzení o elektronickém podepsání a archivaci dat a jejich atributů v daném okamžiku u e-notáře.
Tyto změny umožní rychlý rozvoj praktického využívání e – dokumentů široké vrstvě občanů, kteří mají přístup ke komunikačnímu rozhraní, které je napojeno na e-notáře. Přitom se nejedná pouze o vlastníky počítačů, nebo mobilních komunikátorů, ale i o vlastníky mobilních telefonů, což mnohonásobně zvětšuje okruh uživatelů aplikace e-notáře a na ni navazující ICT aplikací a činí tak tuto oblast obchodně zajímavou. Předpokládání uživatelé jsou uvedeni jako účastníci projektu.
Jako příklady je možné uvést následující: např. občana, který zašle elektronickou obchodní smlouvu e-notáři podepsanou zaručenými elektronickými podpisy smluvních stran přes internet, kde komunikační rozhraní s e-notářem mohou poskytovat provozovatelé webovských stránek (seznam.cz, centrum.cz, posta.cz atd.). Nebo občana, který chce pouze důvěryhodně uložit elektronický otisk (hash) dokumentu a využije služby mobilního nebo jiného telekomunikačního operátora vlastnícího komunikační rozhraní s e-notářem.
Občan dokonce nemusí vlastnit zaručený elektronický podpis ani počítač, aby získal elektronický otisk e-dokumentu. Stačí mu mobilní telefon s fotografickým přístrojem a obrazová zpráva zaslaná přes komunikační rozhraní mobilního operátora e-notáři vytvořit z ní důvěryhodný e-dokument, který bude opatřen zaručeným elektronickým podpisem či elektronickou značkou e-notáře a kvalifikovaným časovým razítkem. Takto archivovaná obrazová zpráva má garantovanou integritu dat a jejich existenci v daném okamžiku podepsání u e-notáře a dále u něj může být důvěryhodně archivována pro další využití v právních procesech.

Tento příklad je obchodně z hlediska rozvoje aplikací využívající e-notáře a veškeré infrastruktury elektronických služeb s ním souvisejících nejzajímavější. Každý si dovede představit např. řidiče po autonehodě (obzvláště po novelizaci Silničního zákona, kdy při částkách zhruba do 100 tis. Kč není potřeba policie) pořizující si obrazovou dokumentaci z místa nehody pro dokumentaci k pozdějšímu právní řízení, odesílající ji na komunikační kontakt svého operátora a ve chvilce dostávající SMS potvrzení, že tato obrazová dokumentace je důvěryhodně elektronicky podepsána a opatřena kvalifikovaným časovým razítkem, dále spravována a archivována u e-notáře. Takových momentů v životě každého občana (možné právní využití obrazové e-dokumentace) je celá řada.

Nabídka aplikace přitom může např. vycházet z technické implementace pilotního projektu PKI (např. na bázi Entrustu v Telefónica O2 a bezpečného vnoření do prostředí IS/ICT v této Společnosti), dále rozšíření implementace pro zákonné uchovávání telekomunikačních dat a dále ze současné aplikace ISDS, na jejímž vývoji se tato společnost podílí s Českou poštou.

Rovněž může také vycházet z požadavku v celé naší společnosti (tedy v celém státě), a to pomocí e-administrativy snížit personální požadavky na administrativu. Nabídka rovněž

vychází z klíčového požadavku komplexní bezpečnosti PKI z hlediska legislativy ČR, včetně do budoucna státem požadované aplikace elektronických voleb, které jsou modelově zvládnuty a v některých státech realizovány.

Nabídka by měla být komplexnější právě o nabídku aplikace vícenásobného podpisu, než např. samotná aplikace důvěryhodného elektronického archivu. Vícenásobné elektronické podepisování tzv. referátníků na ministerstvech, popřípadě daňových přiznání jsou jenom příklady pro dokreslení potřeby této aplikace.

Důvěryhodný e-archiv pouze s propojením aplikace vícenásobného podepsání nejenom v rámci archivních procesů, ale především možnost elektronického podepsání dokumentu více osobami z hlediska platné legislativy ČR, umožňuje praktické využití ve státním sektoru, bankovnictví i telekomunikacích.

Proto v současnosti nabízená komerční řešení nejsou příliš aplikována, a pokud, tak pouze jako vylepšený datový sklad pro jednotlivé zákazníky.

Ani nabízená řešení samotného e-archivu v bankách nejsou vnímána jinak.

Pro vytvoření komerčně úspěšné aplikace je nutno spojit vícenásobné elektronické podepisování dokumentů, důvěryhodný e-archiv se službami v limitním případě se blížící k e-notářským službám.

Ukazuje se vhodné využít pro tyto služby společnost se zázemím silné telekomunikační společnosti, garantující jak služby mobilní, tak síťové i webovské. Ve spojení s integrátorem se zkušenostmi s projekty ve všech sektorech (goverment, banking a telco) a předními specialisty je pak možné takovýto projekt realizovat i s případným využitím prostředků EU.

Technicky může být architektura aplikace postavena na řadě SW a HW produktů.

Např. aplikace může být postavena s využitím špičkového hardwarového řešení firmy nCipher a softwarovém řešení firmy Entrust, popřípadě softwarového řešení od firmy Symantec pro e-archivaci (toto je možné chápat pouze jako příklad, který autor detailně zná, nikoliv jako doporučení, jelikož řešení od jiných firem mohou být stejně vhodná).

Pro konkrétní technické řešení se může jednat tedy např. o rozšíření pilotní PKI na Telefónica O2 na bázi Entrustu dle právě o aplikaci s praktickým využitím vícenásobného elektronického podepisování, včetně analýz a předpisové základny pro rozšíření ISDS.

Výše uvedené řešení naplňuje požadovanou certifikaci celého systému na bezpečnostní úroveň EAL 4 specifikovanou zadavatelem a FIPS 140-2 Level 3 na hardwarové komponenty.

Např. samotný Entrust bez implementace např. na hardwarové bezpečnostní moduly firmy nCipher, včetně aplikace elektronické značky a časového razítka (popř. kvalifikovaného časového razítka) toto přímo negarantuje a další rozšíření PKI pro aplikace vícenásobného elektronického podpisu to však vyžaduje. Entrust zároveň neumožňuje vícenásobný elektronický podpis.

Z tohoto hlediska rovněž úložiště telekomunikačních dat u telekomunikačních společností ne zcela splňují požadavky kladené legislativou na důvěryhodný e-archiv.

Pro vytvoření úspěšné aplikace je ovšem třeba mít kvalitní návrh řešení a správný výběr typu řešení aplikace vícenásobného el. podpisu v daných podmínkách, a to pro každé konkrétní využití nabízené služby pro konečného zákazníka např. pro podepisování e-referátníků, e-smluv (např. hypoték v bankovním sektoru atd.), e-dat pro státní sektor (MV dopravní data, fotografie atd.) a e-archivaci všech e-dokumentů.

Pro úspěšnou realizaci takového případného projektu považujeme v první fázi za nejdůležitější vytvoření aplikace pro vícenásobné podepisování a ověřování, její bezpečné implementace a převedení do rutinního provozu v rámci prostředí IS/ICT .

Rychlá realizace dodávky této aplikace může přinést řadu výhod jejímu realizátorovi pro zefektivnění řízení procesů e-administrativy, a to dle současných úsporných trendů vlády ČR.

Stručná analýza a nástin řešení

V první fázi analýzy dostupných norem, standardů a metod pro vytváření a ověřování vícenásobného elektronického podpisu rozebereme a navrhneme nejvhodnější řešení s vícenásobným elektronickým popisem pro praktické využití z dosud existujících řešení:
1) Vícenásobné podpisy (Multi-Signatures) - Existuje již celá řada různých modifikací schémat skupinového podpisu. Základní dvě varianty skupinového podpisu jsou určeny tím, že buď A) všichni podepisující připojí svoje podpisy k dokumentu, nebo B) první podepisující připojí podpis k dokumentu, druhý podepisující podepíše (dokument+ první podpis) a tento podpis připojí k (dokument+ první podpis), třetí podepisující podepíše ((dokument+ první podpis)+druhý podpis) a připojí svůj podpis atd. Další rozlišení určuje, zda je potvrzeno převzetí (dokument+všechny podpisy) každým účastníkem apod. Podepisovaný dokument je většinou předpokládán ve formátu PDF.
2) Kruhový podpis (Ring Signatures) – Definice a možné aplikace takovéhoto podpisu nalezneme například v příspěvku R.Rivest, A.Shamir, Y.Tauman : How to leak a secret. (In Proceedings of Asiacrypt 2001, volume 2248 of LNCS, pages 552-65. Springer - Verlag, 2001.)
3) Skupinové podpisy (Group Signatures) - Ve schématu přeHPtaveném Chaumem a Heystem v roce 1991 se předpokládá vytvoření skupiny n uživatelů, která je spravována jedním manažerem. (např. v pracích D.Chaum, E. van Heyst: Group Signatures. In Proceedings of Eurocrypt 1991, volume 547 of LNCS, pages 257-265. Springer - Verlag, 1991., G.Ateniese, G.Tsudik: Some open issues and directions in group signatures. In Financial Crypto ´99, volume 1648 of lNCS, pages 196-211. Springer - Verlag, 1999., M.Bellare, D.Micciancio, B.Warinschi: Foundations of Group Signatures : Formal Definitions. Simplified Requirements, and a Construction Based on General Assumptions. In Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 614-30. Springer - Verlag, 2003)
4) Hromadné podpisy (Aggregate Signatures) - lze je najít v literatuře (např. S.Kent, C.Lynn, K.Seo: Secure border gateway protocol, IEEE J.Selected Areas in Comm., 18(4), pages 582-92, April 2000., D.Boneh, C.Gentry, B.Lynn, H.Schaham: Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Proceedings of Eurocrypt 2003, volume 2656 of LNCS, pages 416-32. Springer - Verlag, 2003).

Je zajímavé existující řešení, např. Adobe Acrobat, a to v návaznosti na existující řešení v pdf využívající elektronické značky (např. s razítkovačem DSE 200) a další nabízená řešení.

Na základě provedené analýzy a vyhodnocení možností je nutné udělat výběr podle optimálních kriterií a platné legislativy ČR pro e-podpis:

- jednoduchosti uživatelského postupu při tvorbě a ověření vícenásobného podpisu, možnost postupného připojování podpisů, možnost zneplatnění certifikátů, použití časových razítek, možnost ověření podpisu v některé běžné aplikaci (předběžně lze za tuto aplikaci považovat podepisování formátů XML a PDF).

- platnosti 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., kterými se otevřela v ČR široká oblast pro používání různých druhů elektronického podpisu, včetně nejrůznějších variant jeho používání.

Vytvoření aplikace pro vícenásobný podpis a jeho ověřování

Doporučujeme navrhnout a vytvořit aplikaci pro vícenásobný elektronický podpis v jazyce Java. Domníváme se, že to je optimální volba vzhledem k požadavku provozovatelnosti na co nejvíce platformách. Jedná se o ověřenou, vyzrálou technologii, která je na trhu již přes deset let a která reálně naplňuje slogan Write Once, Run Everywhere (naprogramuj jednou, spouštěj kdekoli).[1] Domníváme se, že tento přístup je daleko výhodnější nežli se snažit vyvinout (a udržovat) několik větví softwaru pro různé platformy.
Uživatelské rozhraní může být vytvořeno pomocí technologie Swing, která umožní vyhovět požadavku na intuitivnost.
Aplikace musí podporovat základní činnosti vytvoření a ověření vícenásobného elektronického podpisu maximálně přímočaře, aby byla použitelná i méně zkušenými uživateli. Tato aplikace musí také obsahovat uživatelskou nápovědu, příručku aplikace dostupnou on-line z webu, přímo z aplikace, i ve formě dokumentu v PDF. Součástí uživatelské příručky musí být metodické pokyny pro provádění hlavních činností.

Tato aplikace bude muset být spouštěna z webu pomocí technologie Java Web Start. Právě tato technologie umožňuje jednoduché první spuštění aplikace a naprosto transparentní aktualizaci. Případná aktualizace se potom provede naprosto transparentně, bez nutnosti uživatelova zásahu. Tím je tedy ošetřena distribuce aplikace pomocí webu. Na webovém serveru přitom budou přítomny v zásadě jen statické stránky, takže požadavky kladené na jeho výkon nejsou nijak vysoké.

Dokumentace k aplikaci by měla obsahovat tyto součásti:

- klasická uživatelská příručka k aplikaci dostupná přímo z aplikace, na webových stránkách aplikace (tedy bez nutnosti jejího spuštění) i ve formě stránkovaného dokumentu pro tisk ve formátu PDF
- tooltipy a kontextová nápověda
- průvodci v aplikaci pro usnadnění obtížnějších či často používaných činností.

Programátorská dokumentace by měla být pak vytvořena jednak v podobě Javadoc (HTML stránky dokumentující veřejné třídy a rozhraní ze zdrojového kódu v jazyku Java), jednak v podobě dokumentu či hypertextového dokumentu udržovaného pomocí nástroje Wiki (stejná technologie, kterou je realizována Wikipedia).
Tuto podmínku lze splnit v principu dvěma postupy – buď vytvořit (a udržovat) několik větví programového kódu pro různé platformy, nebo právě využít vlastností Javy, která umožní odstínit aplikaci od platformy a aplikace pak běží na všech platformách, na kterých je Java implementována. (Java je implementována např. na všech verzích Windows – od Windows 98

[1] Implementace virtuálního stroje Javy existují pro nejpoužívanější operační systémy pracovních stanic:
MS Windows (verze 98, 2000, XP), Linux, Macintosh, FreeBSD, a to jak 32-bitové, tak 64-bitové procesory.
Kromě toho existují implementace i pro mnoho serverových platforem (Solaris, AIX, O2-UX, S/390…).

po Windows XP a na všech budoucích verzích Windows bude ihned po jejich uvolnění implementována, na všech verzích Linuxu, na Macintosh, na Solaris atd.)

Při použití jiného postupu (bez využití Javy) není myslitelné, aby byla aplikace provozovatelná na všech těchto platformách (navíc vzniká problém např. s novými verzemi Windows, které teprve přijdou – při použití našeho postupu je rozšíření aplikace na tyto nové verze automaticky zaručeno producentem Javy, tj. firmou SUN).

Lze konstatovat, že z hlediska optimalizace finančních nákladů na řešení je požadavek „co nejvíce běžně užívaných platforem“ , splnitelný pouze s využitím Javy.

Další výhodou navrženého řešení je možnost automatické aktualizace aplikace při každém jejím spuštění, a to bez nutnosti zásahu uživatele. Toto řešení také zaručuje, že všichni uživatelé pracují s aktuální verzí aplikace.

Rámec komplexní bezpečnosti

Vzhledem k dynamickému rozvoji v oblasti výzkumu v nových technologiích pro bezpečnostní aplikace, a to především v oblasti informačních systémů, informačních technologií, informační bezpečnosti a kryptologie ve světě i u nás, úroveň globální i informační bezpečnosti v každé organizaci, a tedy i v námi rozpracovávané (tj. způsobu jejího řízení, dokumentace a kontroly v oblasti globální i informační bezpečnosti), za tímto rozvojem zaostává.

Ve Společnosti, která bude nabídku realizovat, se musí daná problematika řešit koncepčně, komplexně a systematicky a v souladu s požadavky a platnými směrnicemi při budování celé aplikace. Řešení musí být oproštěno od lokálních názorů, přístupů, činností nebo nečinností jednotlivých subjektů uvnitř Společnosti, odpovědných zaměstnanců nebo dodavatelů.

Jediným řešením jak předejít nežádoucím incidentům s orgány provádějícími kontrolu dodržování těchto zákonů je komplexní správa bezpečnosti.

U Společnosti se předpokládá existence kvantitativního popisu komplexní bezpečnosti a bezpečnostních metrik v oblasti bezpečnosti IS/ICT , aby měřitelnost bezpečnosti PKI byla realizovatelná.

Dále se předpokládá existence úplné bezpečnostní předpisové základny, akceptující právní řád ČR, české a mezinárodní normy v této oblasti, a také stanovení plánu jejich implementace s horizontem dosažení stanovené úrovně bezpečnosti EAL 4.

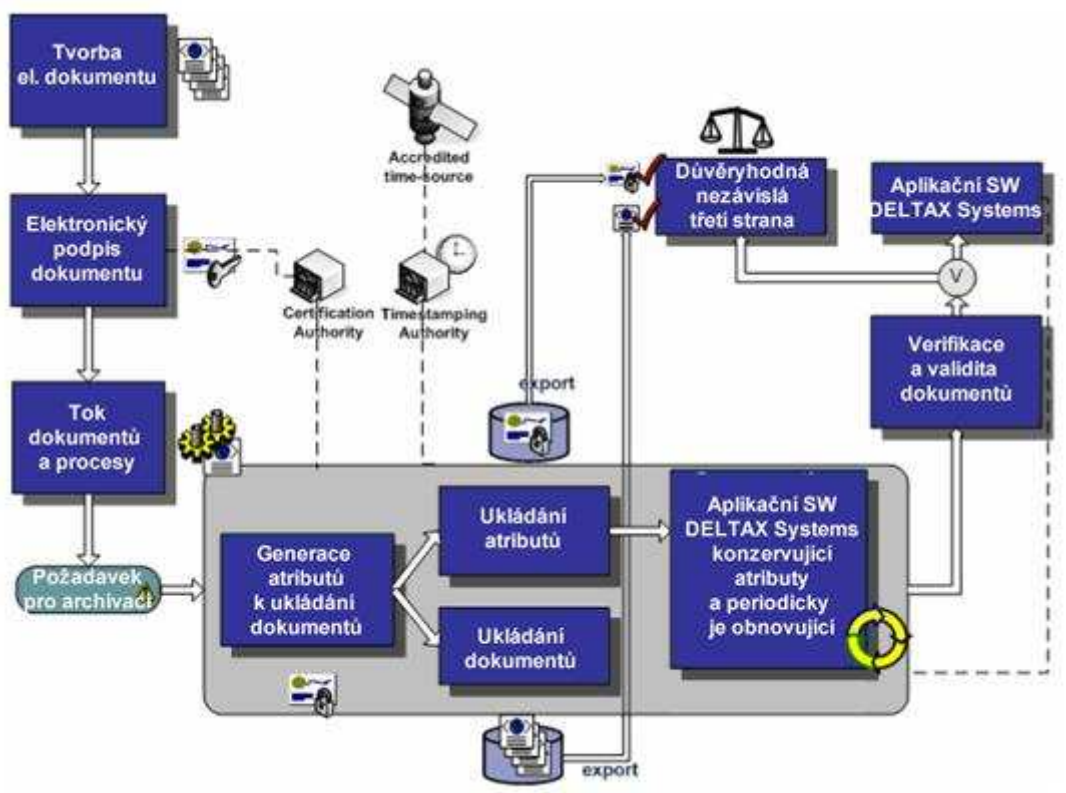
Rovněž se předpokládá, že ve Společnosti bude zabezpečena správa komplexní bezpečnosti, jejíž nedílnou částí je správa informační bezpečnosti a to tak, aby infrastruktura komplexní a informační bezpečnosti uvnitř organizace plnila bezpečnostní politiku v jednotě s komplexními i informačními bezpečnostními cíly a strategiemi. Přijaté řády bezpečnosti musí respektovat jistou vizi rozvoje resortů, pro které bude aplikace realizována (např. ministerstva) tak, aby byly v platnosti v co nejdelším časovém horizontu a aby byly co nejstálejší při případných změnách. To by mělo platit i pro bezpečnost IS/ICT a všech provozovaných aplikací ve Společnosti.

Důvěryhodná správa e-dokumentů Společnosti přitom vychází z platné legislativy ČR a může být tvořena třemi následujícími pilíři:

1) Managementem klíčů pro aplikaci asymetrické šifry a elektronického podepisování u aplikace e-notáře na bázi řešení od firmy nCipher (viz dokument nCipher key managment solution suite).
2) Řešením aplikace elektronické archivace dat včetně kvalifikovaného časového razítka) na bázi produktu od firmy Symantec neb SAP.
3) Řešením vyhledávaní dokumentů na bázi produktu od firmy Symantec neb SAP, nebo využití informační rafinerie.

Společnost, která bude aplikaci nabízet, musí však řešit i některé další problémy. Např. současné kryptografické algoritmy, které realizují elektronický podpis a šifrování pro zabezpečení elektronických dokumentů, totiž používají klíče s danou omezenou délkou a dané hashovací funkce k vytvoření elektronického otisku, se stávají s časovým vývojem překonatelné díky dynamickému vývoji výpočetní techniky a kryptologie. S časovým vývojem je tedy nutné užití nových mohutnějších klíčů či hash funkcí, a také nových certifikátů, když platnost těch původních vypršela (ve smyslu PKI certifikační politiky). Například je-li certifikační politikou platnost certifikátu omezena na jeden rok, je nutné ty e-dokumenty, které jsou podepsány daty příslušejícími k danému certifikátu, opětovně elektronicky podepsat. Opakované elektronické podepisování, obzvláště je-li e-dokument podepsán několika podpisy, je pro aplikaci e-archivu prakticky nerealizovatelné.

Jediným možným řešením je aplikace elektronické značky obsahující časové razítko nebo přímo kvalifikované časové razítko ve smyslu novelizovaného zákona o elektronickém podpisu č.440/2004 Sb. Toto řešení garantuje existenci daného e-dokumentu v okamžiku uvedeném v časovém razítku. I když se pracuje s nepodepsanými e-dokumenty (např. scanovaný e-mail neb faktura) pouze periodická aplikace časového razítka zabezpečí průkaznost, že daný dokument existoval v daný okamžik v minulosti a jeho integrita nebyla pozměněna.



Řešení Společnosti musí vyloučit jakoukoliv nezaznamenanou manipulaci s dokladem i v případě oprávněných osob s přístupem k této aplikaci uvnitř Společnosti. Základním přínosem elektronické archivace je možnost úplné důvěryhodné převoditelnosti libovolných papírových dokladů do elektronické formy, a to s využitím služby klasického či elektronického notáře. Jedná se tedy především o novou službu zákazníkům, kteří mají problémy s archivací velkého množství dokladů, které potřebují hodnověrným způsobem zabezpečit v dlouhodobém časovém horizontu. Právě toto řešení je pro vybudování IS s aplikací e-notáře nezbytné.

Schéma řešení pro důvěryhodnou správu e-dokumentů, jejich managment a archivaci může být znázorněno např. následovně (dle schématu dřívější firmy Deltax) :

Pro vlastníky komunikačních rozhraní s e-notářem Společnost musí být schopna vybudovat IS komunikující s aplikačním serverem u e-notáře. Ten pak vlastní pouze aplikační server komunikující s akreditovanou certifikační autoritou, realizující elektronický podpis a kvalifikované časové razítko na dokumentu a dále toky dokumentů a procesy související s požadavky na důvěryhodnou archivaci e-dokumentů.

Závěr

Obchodní motivace Společnosti, která službu e-notáře a vícenásobného e-podpisu bude realizovat, může být pro investice do vybudování IS/ICT aplikace e-notáře a infrastruktury služeb s ní souvisejícími je založena na následovně uvedených odhadech a obchodních modelech souvisejících s frekvencí zasílaných MMS zpráv, ukládaných e-dokumentech, daňových přiznáních atd. Územní dopad této aplikace je v celé ČR a cílovou skupinou jsou vlastníci mobilních telefonů a vlastníci IT prostředků s přístupem na Internet.
Rizikem projektu může být nižší obchodní zájem o aplikaci než odhady uváděné v obchodním modelu a jeho snížení lze dosáhnout marketingovou propagací aplikace např. ze strany mobilního operátora v návaznosti na připravovaný silniční zákon a rozšíření marketingové propagace MMS služeb. Toto riziko dále snižuje široká možnost využití ve státní správě, kde snaha po optimalizaci a šetření v době celosvětové krize by měla být maximální, a tedy zájem o využití aplikace značný.
V současné době lze pouze smutně konstatovat, že aplikace elektronického notáře v ČR neexistuje a rozvoj aplikací s elektronickým podpisem není tak rozvinutá, jak se očekávalo v pionýrských dobách jeho zavádění v ČR.
Aplikace e-notáře v souvislosti se zaváděním ISDS rozšíří a doplní tuto nově zaváděnou službu, právě díky možnosti opatřovat elektronické dokumenty elektronickou značkou e – notáře i pro zákazníky nevlastnící zaručený elektronický podpis, a to i cestou SMS zpráv. Rozšíří okruh uživatelů a umožní další rozvoj infrastruktury, jak u IS veřejné správy, tak i v komerční sféře.

Závěrem si autor příspěvku dovoluje podotknout, že bude rád, pokud vyvolá alespoň polemiku k danému tématu.

Poznámka: dokument nebyl vypracován ani konzultován se společnostmi, které jsou v článku jmenovány.

D. Bedna 2009 – pozvánka

Během posledních 10 let se v České republice rozmohl obrovský fenomén, kterým se staly terénní šifrovací hry. S termínem „šifrovací“ lze sice někdy úspěšně diskutovat, protože řadu úloh tvoří spíše rébusy než šifry, ale rozumím, že s klasickými šiframi a jejich modifikacemi organizátoři již prostě nevystačí a vymýšlí tak další a další varianty šifro-rébusů …

Velký zájem o tento typ soutěží způsobil, že se dnes koná již několik desítek šifrovacích her ročně pro stovky týmů po celé republice. Mezi ty nejstarší a nejznámější patří i **Bedna**, která letos pokračuje osmým ročníkem.

Bedna 2009 se bude konat v ulicích Prahy o víkendu 16. – 17. května. Začátek bude v sobotu asi v 15.00 hod a potrvá do neděle dopoledne (předpokládaný konec 12.00).

Hra je určena pro starší 18-ti let, mladším 18-ti let není účast ve hře dovolena. Do hry se mohou přihlásit dvou až pětičlenné týmy.

Hru pořádá neformální skupina vystupující pod značkou *Svobodní Bednáři*, s vydatnou podporou mnoha svých kamarádů a spřátelených organizací.

Registrace na akci již byla zahájena!

Formulář a další aktuální informace najdou zájemci na stránce věnované soutěži http://bedna.org/2009

Zaregistrováno je (v době přípravy tohoto e-zinu) již **183 týmy** (celkem **684 účastníků)**. Pozor z organizačních důvodů je počet týmů omezen na **225**! Registrační poplatek je letos stanoven na 499 Kč za celý tým. Akce je nezisková, to znamená, že všechny vybrané poplatky budou použity při realizaci soutěže…

Všem účastníkům přeji pěkné počasí a pěknou zábavu.

Štěstí přeje připraveným, a proto si na závěr této pozvánky dovolím doporučit účastníkům prolistovat soutěžní úlohy z Crypto-Worldu a také moji knížku věnovanou šifrování.

[1] Soutěže v luštění pořádané e-zinem Crypto-World 2000-2008, http://crypto-world.info/souteze.php

[2] P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006, http://crypto-world.info/oko/index.php

E. O čem jsme psali v dubnu 2000 – 2008

Crypto-World 4/2000

Crypto-World 4/2001

Crypto-World 4/2002

Crypto-World 4/2003

Crypto-World 4/2004

Crypto-World 4/2005

Příloha (PR) :
J.Strelec (Secunet) : SINA – Bezpečná komunikační infrastruktura

Crypto-World 4/2006

Příloha: version_0.zip, version_1.zip (programy pro hledání kolizí MD5 , Klíma: 18.3, 28.3)

Crypto-World 4/2007

Crypto-World 4/2008

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/