Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 4/2001 15. duben 2001

4/2001

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR.

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>270 e-mail výtisků)

OBSAH : **Str.**

Příloha :
Neschválený návrh slovenského zákona o elektronickém podpisu (zeopsr.zip)

A. Kryptografie a normy , Díl 6.
Normy IETF – S/MIME, část l.

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

Tento článek navazuje na úspěšný miniseriál Kryptografie a normy 1.-5.(přehled norem PKCS), který byl publikován v našem e-zinu v číslech 9/2000 až 1/2001 - redakce.

l. Úvod

Toto a následující pokračování seriálu „Kryptografické normy“ v Crypto-Worldu bude věnováno problematice bezpečnosti mailových zpráv neboli formátu **S/MIME**. První část bude věnována historii vzniku norem pro bezpečný mail, bude vysvětlena obsahová stránka formátu S/MIME a provedeno i určité stručné srovnání s formátem **PGP/MIME**. V druhé části bude proveden obsahový přehled dokumentů v rámci skupiny IETF-S/MIME (rfc a drafty).

2. Ke vzniku formátu S/MIME

V roce 1995 firma RSA a několik dodavatelů softwaru se rozhodlo spolupracovat na vytvoření nové moderní normy pro zasílání bezpečně chráněných zpráv – S/MIME. Jednou ze základních požadovaných vlastností nově vzniklé normy byla interoperabilita – libovolné dvě implementace musí být schopné si vyměňovat utajené a autentizované zprávy.

Internetová e-mailová zpráva sestává ze dvou částí – hlavičky a těla. Zasílaná data např. zašifrovaných či podepsaných zpráv jsou nejen v textové ale také i v binární podobě. Avšak standartním protokolem pro výměnu zpráv přes internet je protokol **SMTP** (Simple Mail Transfer Protocol - rfc822), obsah zprávy je dán jako text ASCII. Tento rozpor je řešen následovně. Specifikace **MIME** (Multipurpose Internet Mail Extensions - rfc1521) rozšířily formát SMTP tak, aby bylo možné přenášet zprávy obsahující více textových částí a také části binární (např. také grafiku, audio atd.) bez ztráty jakékoliv informace. Tj. tělo zprávy ve formátu MIME je již strukturováno. MIME však neobsahuje žádné služby bezpečnostního charakteru. Za tímto účelem byl vytvořen **S/MIME** (Secure MIME), který využívá syntaxi dle PKCS #7 (viz předchozí díly našeho seriálu) pro digitální podpisy a šifrování. MIME tělo zprávy pak obsahuje zprávu dle PKCS #7, která je výsledkem kryptografických operací.

S/MIME byl vytvořen tedy k tomu, aby zabezpečil požadované bezpečnostní služby a nebyla přitom narušena interoperabilita různých implementací. Opírá se přitom o využití celé řady již existujících doporučení a norem.

Pro ochranu mailových zpráv vzniklo historicky několik postupů jako jsou metody PGP, PEM, MOSS a posléze S/MIME. PGP je zde vlastně současně specifikace i konkrétní aplikace.

PEM (Privacy Enhanced Mail) je obsaženo v rfc1421-1424. Toto byla dřívější norma pro zabezpečení e-mailů, specifikovala formát zprávy a určitou hierarchickou strukturu. Formát zprávy PEM je založen na 7-bitových textových zprávách (S/MIME je konstruován tak, aby mohl pracovat s MIME přílohami i s textem, i z hlediska hierarchií je S/MIME flexibilnější).

MOSS byl navrhován tak, aby odstranil některé nedostatky PEM, mohl pracovat s MIME zprávami a byl liberálnější z hlediska požadavků na hierarchii. Avšak ukázalo se, že MOSS má tolik různých konkrétních implementačních možností, že je snadné, aby dva nezávislí vývojáři vytvořili formát dle normy MOSS a přitom jejich produkty nebyly schopné vzájemné komunikace. Specifikace MOSS jsou totiž spíše rámcové a při zpracování konkrétní implementace je třeba dořešit ještě řadu problémů.

Dále existuje ještě jeden nepříliš známý formát s označením **MSP** vzniklý v americké armádě. Tento formát je určen pro práci s mailem dle normy ITU X.400. V současnosti je stále dále rozpracováván.

3. Vlastnosti formátu S/MIME

Existuje několik bezpečnostních aspektů, které je třeba, aby byly zajištěny užitím protokolů pro bezpečnou výměnu zpráv:

1. *Autentizace*. Kdokoliv , kdo má k dispozici veřejný klíč příslušného uživatele, zprávu a podpis této zprávy musí být schopen ověřit, že danou zprávu skutečně odeslal tento uživatel.
2. *Nepopiratelnost*. Odesilatel nemůže později popřít, že zprávu odeslal
3. *Integrita zprávy*. Zpráva nebyla během přenosu modifikována Vlastnosti 1-3 jsou zajištěny užitím digitálního podpisu.
4. *Utajení*. Obsah zprávy má být znám pouze straně odesílající a straně přijímající. Toto je zajištěno šifrováním zprávy.

S/MIME podporuje nepopiratelnost zdroje (vysílající strana nemůže popřít, že zprávu odeslala), avšak nepodporuje nepopiratelnost doručení (přijímající strana může popřít, že zprávu obdržela).

V současné době se stále můžeme setkat s využívanými dvěma verzemi formátu S/MIME a sice S/MIME v2 (vyžaduje použití algoritmu RSA pro výměnu klíčů a vyžaduje použití slabé kryptografie) a S/MIME v3. Právě závislost na algoritmu RSA, resp. slabé kryptografii (tudíž nebylo možné, aby verze 2 prošla normativním procesem v IETF) vedla ke vzniku verze 3.

Základní specifikaci pro S/MIME v2 obsahuji dva dokumenty:

- S/MIME Message Specification (rfc2311)
- S/MIME Certificate Handling (rfc2312).

Základem S/MIME v3 je následujících pět dokumentů:

- Cryptographic Message Syntax (rfc2630)
- S/MIME Version 3 Message Specification (rfc2632)
- S/MIME Version 3 Certificate Handling (rfc2633)
- Enhanced Security Services for S/MIME (rfc2634)
- Diffie-Hellman Key Agreement Method (rfc2631)

CMS (Cryptographic Message Syntax) definuje syntaxi pro přenos kryptografické informace, která se vztahuje k chráněnému obsahu. Je to vlastně také určité rozšíření PKCS #7 (poslední je verze 1.6) vzhledem k potřebě zahrnout určité další bezpečnostní vlastnosti.

Hlavní rozdíl mezi PKCS #7 a CMS spočívá v tom, že jsou přidána pole pro syntaxi zabalených dat a to tak, aby byla zajištěna nezávislost na použitém kryptografickém algoritmu. Konkrétně - navíc jsou podporovány takové algoritmy jako Diffie-Hellmanovo schéma pro výměnu klíčů či KEA (Key Exchange Algorithm – implementováno na Fortezza Crypto Card).

Již S/MIME v2 pracuje s digitálními certifikáty dle **X.509 v3** a v S/MIME v.3 je další významnou změnou možnost zahrnout do syntaxe podepsaných a zabalených dat také X.509 atributové certifikáty. CMS je zahrnuto v protokolech skupiny IETF-pkix (Public Key Infrastructure Exchange). Dokument S/MIME v3 Certificate Handling Specification stanoví jako povinnou podporu X.509 verze 3 certifikátů a také podporu X.509 certifikátů a CRL dle profilů skupiny PKIX.

Materiál rfc2634 - Enhanced Security Services for S/MIME popisuje další služby, které lze spojit s ochranou v CMS (návrhy většinou vychází z požadavků amerického ministerstva obrany). Jsou to např. autentizace doručení (analog doporučené pošty), označení stupně utajení zasílané zprávy atd.

Přes původní ambice formátu S/MIME existují však stále určité rozdíly mezi jednotlivými implementacemi. Např. S/MIME nevyžaduje používání CRL (Certificate Revocation List), různým způsobem může být pojednána návaznost na protokol IMAP (rfc1730 - Internet Message Access Protocol), který se zabývá postupy, jakými uživatel má přístup k elektronickým zprávám na serveru.

Hlavní dodavatelé (proprietárního) softwaru pro zasílání zpráv - Microsoft, Novell and Lotus podporují S/MIME. Totéž se týká také produktů Netscape, Entrust Technologies, Worldtalk i dalších. Na webovské stránce

http://www.rsasecurity.com/standards/smime/interop_center.html

lze nalézt seznam produktů.které úspěšně absolvovaly testy S/MIME interoperability. Referenční implementací je Worldtalk's WorldSecure Client. Rovněž tak řada dodavatelů produktů **EDI** podporuje CMS formát v S/MIME, který se pro EDI ukázal být výhodnější než tradiční použití tzv. VAN (value-added networks). Hlavním důvodem jsou přitom nižší náklady, zatímco dosažená bezpečnost je zcela vyhovující.

4. Srovnání S/MIME a PGP/MIME

Oba formáty nabízí obdobné služby, ale mají zásadně odlišné formáty. PGP se také původně opíralo o využití jiného (proprietárního) formátu certifikátů. V současné době (verze 7.,0) však již podporuje obdobně jako S/MIME práci s certifikáty dle X.509 v.3.

S/MIME jak bylo řečeno se opírá pro zprávy o formát PKCS #7 (kódování dat dle ASN.1 DER). PGP používá jednoduchý binární kód. Oba formáty používají pro strukturování svých zpráv MIME (rfc1847 pro podepsané zprávy).

Implementace PGP/MIME se opírají o následující dokumenty:

- PGP Message Exchange Formats (rfc1991)
- MIME Security with Pretty Good Privacy (rfc2015)

V současné době probíhají práce ve vztahu k PGP/MIME v rámci pracovní

skupiny IETF OpenPGP. Klíčovými jsou následující dokumenty:

- MIME Security with Open PGP (draft-ietf-openpgp-mime-05.txt)
- Open PGP Message Format (rfc2440)

V následující tabulce jsou shrnuty základní rozdíly mezi S/MIME v3 a OpenPGP.

Vlastnosti	S/MIME v3	OpenPGP
Formát zprávy	Binarní, založená na CMS	Binarní, založená na předešlém PGP
MIME obálka podepsaných dat	Volitelná – více částí/podepsaných či CMS formát	Více částí/podepsaných ASCII
MIME obálka zašifrovaných dat	Aplikace/pkcs7-mime	Více částí/zašifrováno

5. Kryptografické algoritmy a S/MIME

Jak již bylo řečeno, ve svých prvních verzích podporoval S/MIME jen velmi omezený okruh algoritmů (symetrických i asymetrických). Ze symetrických to původně byly DES, 3-DES a RC2. V době platných omezení na vývoz kryptografických produktů z USA byl doporučován zejména tento poslední - RC2. Doporučována byla jeho 40 bitová varianta, která samozřejmě není dostatečně odolná a to dokonce ani proti totálním zkouškám klíče.

V rámci formátu S/MIME v3 jsou v současné době podporovány následující algoritmy: 3-DES, RC2, KEA, Skipjack, CAST-128, IDEA a AES.

Z asymetrických algoritmů pro výměnu klíčů byl původně využíván algoritmus RSA Dnes je ve verzi 3 možno využívat jak Diffie-Hellmanovo schéma pro výměnu klíčů (DH - povinný algoritmus z implementačního hlediska – přitom jeho formulace vychází z normy ANSI X9.42) tak i eliptické křivky. Definice eliptických algoritmů (EC) vychází opět z ANSI norem – X9.62 a X9.63.

Podporované algoritmy pro podpis jsou RSA, DSA a nověji ECDSA. V současné době je připravován formát pro dlouhodobě platné podpisy dokumentů (východiskem jsou zpracované dokumenty EU – ETSI).

6. Použité zkratky

V následujícím je stručně popsán význam zkratek, se kterými se čtenář může setkat v tomto článku (bylo jich přehršel) a také v jiných dokumentech zabývajících se problematikou bezpečnosti e-mailu.

ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One - ISO/IEC norma pro kódování
BER Encoding	Basic Encoding Rules

CAST	symetrický kryptografický algoritmus, autoři Carlisle Adams a Stafford Tavares (Entrust Technologies)
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List (seznam odvolaných certifikátů)
DER Encoding	Distinguished Encoding Rules
DES	symetrický kryptografický algoritmus, bývalá US norma(NIST)
3-DES	symetrický kryptografický algoritmus, současná US norma
DH	Diffie-Hellman (schéma pro výměnu klíčů)
DSA	Digital Signature Algorithm (US norma pro dig. podpis)
ECDSA	Elliptic Curve Digital Signature Algorithm
EDI	Electronic Data Interchange
ESS	Enhanced Security Services
ETSI	European Telecommunications Standards Institute
IDEA	symetrický kryptografický algoritmus
IETF	The Internet Engineering Task Force
IMAP	Internet Message Access Protocol
KEA	Key Exchange Algorithm
MIME	Multipurpose Internet Mail Extensions
MOSS	MIME Object Security Service
MSP	Message Security Protocol
NIST	National Institute of Standards and Technology (USA)
OpenPGP	OpenPGP, pracovní skupina IETF
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PKCS	Public Key Cryptographic Standard
PKIX	Public Key Infrastructure Exchange, pracovní skupina IETF
RC2	symetrický kryptografický algoritmus, autor Ronald Rivest
Rfc	request for comment
RSA	Rivest-Shamir-Adleman – algoritmus asym. kryptografie, první významný kryptosystém s veřejným klíčem
S/MIME	Secure/Multipurpose Internet Mail Extensions
Skipjack	symetrický kryptografický algoritmus
SMTP	Simple Mail Transfer Protocol
ITU	International telecommunication Union
VAN	Value-Added Networks
X.509	ITU-T digital certificate.

7. Literatura

[1] S/MIME Mail Security (smime) http://www.ietf.org/html.charters/smime-charter.html

[2] An Open Specification for Pretty Good Privacy (openpgp)
http://www.ietf.org/html.charters/openpgp-charter.html

B. e-komunikace, e-platby, e-projekty, e-platformy a „velcí hráči“

Mgr. Pavel Vondruška, ÚOOÚ

I. Rozdělení projektů e-komerce a e-komunikace podle zúčastněných stran

Původce informace	Adresát		
	Obchodník B=Business	**Spotřebitel C=Consumer**	**Státní instituce A=Administration (G=Government)**
Obchodník B=Business	**B2B** nákupní systémy velkých podniků (dříve EDI)	**B2C** prodej knih, CD, elektroniky, potravin, lístků **Bank2C** bankovní služby	**B2A (B2G)** nabídka služeb a zboží, komunikace se státní správou přes Internet
Spotřebitel C=Consumer	**C2B** sledování nabídek za účelem snížení ceny	**C2C** aukční systémy pro prodej použitého zboží ("bazar")	**C2A (C2G)** podávání daňových přiznání, volby, sčítání lidu
Státní instituce A=Administration (G=Government)	**A2B (G2B)** zadávání veřejných zakázek, vypisování grantových projektů	**A2C** poskytování informací o veřejné správě	**A2A (G2G)** koordinace činnosti orgánů veřejné moci, mezinárodní koordinace

II. Přehled projektů e-komerce a e-komunikace podle požadovaného stupně zabezpečení (mimo specifických výjimek)

Původce informace	Adresát			
	B=Business	**C=Consumer**		**A=Administration**
B=Business	**B2B**	**B2C**	**Bank2C**	**B2A (B2G)**
C=Consumer	**C2B**	**C2C**		**C2A (C2G)**
A=Administration	**A2B (G2B)**	**A2C**		**A2A (G2G)**

Zabezpečení

nízké	
zvýšené	
střední	
vysoké	

III. Česká republika B2C (přehled způsobů placení v e-obchodech)

a) dobírkou - Vybrané zboží je doručeno některou z přepravních agentur nebo Českou poštou. Vy zaplatíte až při převzetí tohoto zboží.

b) platební kartou - Detaily placení jsou různé a je tedy nutné se seznámit s konkrétními pravidly příslušného e-obchodu. Přijímány jsou převážně následující karty : MasterCard, VISA, American Express a JCB. Mezi českými zákazníky není v tento způsob placení velká důvěra.

c) běžným bankovním převodem - Platba pomocí tzv. zálohové faktury. Tuto fakturu vám e-obchod zašle, případně si ji lze stáhnout z příslušné adresy a vytisknout. Zboží je dodáno po zaplacení faktury.

d) OK kartou - Během objednávky vyplníte autorizační formulář. Při předání zboží předložíte svoji OK kartu a potvrdíte převod peněz svým podpisem.

e) Paegas GSM Banking - Údaje z příslušné stránky e-prodejce přepíšete do svého mobilního telefonu vybaveného kartou GSM Banking a tyto informace odešlete do "své" banky. Ta provede příslušný převod.

f) eBankou - Placení on-line. Zákazník po vybrání zboží vyplní formulář - příkaz k úhradě - v klientském systému eBanky. Banka částku převede.

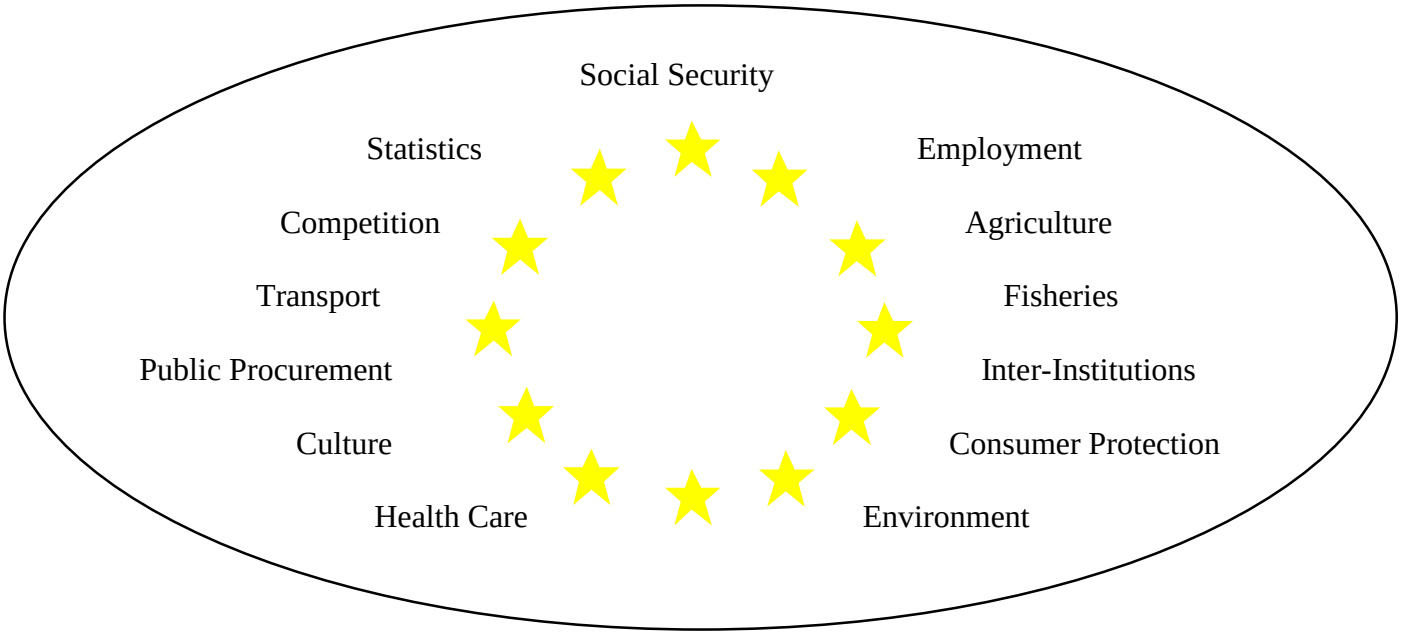
g) Citibank — kartou Juice Pay - Obdoba eBanky, Zde jste po výběru zboží "přesunuti" do Citibank Payment Gateway. Zadáte číslo vaší Juice Pay karty a svůj bezpečnostní kód. Tím potvrdíte peněžní transakci a banka příslušnou částku převede.

IV. Hlavní rozdíly PCS (poskytovatelů certifikačních služeb) v EU a ČR

EU	ČR
Zakladatelem je skupina subjektů (komerční, státní, univerzitní subjekty)	Samostatný subjekt (§ 10,6)
Dobrovolnost akreditace	V oblasti veřejné moci vyžadována akreditace (§ 11)
Vydávání certifikátů pro konkrétní aplikaci (PKA)	Vydávání “čistých” certifikátů, tedy PCS neví, ve které aplikaci budou používány - problém PCS není schopen kalkulovat cenu s ohledem na možné riziko
Podílí se na zisku z PKA (v některých aplikacích certifikáty vydávány dokonce zdarma, PCS placen ze zisku z nasazení aplikace)	Příjem z vydávání certifikátů a souvisejících služeb
Generování klíčů pro uživatele (čipové karty)	Uživatel si klíče generuje sám

V. Oblasti, v nichž se v EU připravují projekty "společného zájmu"

- tedy oblasti, v nichž vznikají na přípravu, vývoj a nasazení těchto projektů, velké nadnárodní skupiny řešitelů z různých oblastí (komerce, státní organizace, univerzitní podpora)



IDA Projects of Common Interest

VI. EVROPA

EEMA kicks-off PKI Challenge

PKI Challenge (pkiC) je dvouletý projekt, plně podporovaný Evropskou Komisí a organizovaný EEMA (the European Forum for Electronic Business). EEMA tvoří konzorcium 13-ti evropských organizací. Projekt začal 1.1.2001 . Hlavní koordinátor projektu je Frank Jorissen (vicechairman of EEMA and pkiC).

PKI Challenge (výzva) je určena tvůrcům aplikací a providerům v Evropě za účelem společného hledání řešení a vzájemné spolupráce na jednoduchých projektech.
Pomocí PKI Challenge jsou vyvíjena kritéria interoperability a podpory různých PKI technologií. Jedná se o provázání velkého počtu různých PKI/PKA produktů, které budou vzájemně testovány s ohledem na interoperabilitu. Tyto produkty (včetně deklarované vzájemné spolupráce) budou veřejně předvedeny na konferenci EEMA 2001 v červnu 2001 a ISSE 2001 (Information Security Solutions Europe) v září 2001.

Členy konzorcia jsou: KPMG (The Netherlands), Security & Standards (UK), Entegrity (UK), Belgacom (Belgium), SmartTrust (Sweden), Entrust (Switzerland), Makra (UK), University of Leuven (Belgium), University of Salford (UK), GlobalSign

(Belgium), UK Post Office (UK), Baltimore (Ireland), Utimaco Safeware (Belgium).
Informace na adrese : www.eema.org/pki-challenge

TRIANGLE

Projekt TRIANGLE je IST program (IST-2000-25296) - tedy program podporovaný Evropskou komisí. Byl zahájen 1.1.2001 a očekává se, že bude trvat 24 měsíců.

Cílem TRIANGLU je připravit jednoduché, přijatelné, lehce ovladatelné interoperabilní řešení pro cestování "z dveří do dveří" (door to door travel). Úkolem je tedy sloučit v jedno řešení platbu, rezervaci a přístup k dalším souvisejícím službám. Vše má být založeno na používání existujících technologií a již instalované infrastruktury. Projekt počítá s použitím čipové karty, která dovolí uložit dopravní lístky, bude sloužit jako elektronická peněženka a umožní přístup k dalším službám. Předpokládá se např. využití standardu CEPS. TRIANGLE bude kompatibilní s vytvářenými programy partnerů a profesionálních institucí. Projekt bude zahrnovat 3 města (Brusel, Londýn a Paříž), využívat mezinárodní dopravní služby (Thalys a Eurostar). Skládat se bude ze dvou etap: laboratorní zkoušky a následných testů, které připraví jednotliví partneři (pilotním projektem má být prodej lístků a služeb mezi městy Brusel a Paříž - "Thalys line"). Úspěch by měla zajistit spolupráce zemí, jejichž hlavní města spojí vysokorychlostní vlak a TRIANGLE bude řešení, které nabídne jednoduché využití všech souvisejících služeb.

Vedoucí řešitel projektu : STIB – MIVB (Société des Transports Intercommunaux de Bruxelles – Maatschappy voor het Intercommunaal Vervoerte Brussel) – Belgium
Partneři (abecedně):
ASK - France
ERRI (Stichting European Rail Research Institute) - The Netherlands with the UIC (Union Internationale des Chemins de fer) support Europay International – Belgium
Eurostar Group – United Kingdom
MTA (Marketing & Technolgies Avancées) - France
Proton World International (PWI) - Belgium
RATP (Régie des Transports Parisiens) - France
SNCF (Société Nationale des Chemins de fer Français) - France
Thalys International - Belgium
Transport for London (TfL) – United Kingdom

CEPS

CEPS je nový standard k dosažení technické interoperability mezi různými elektronickými peněženkami v Evropě .

Je založen na veřejném klíči, předpokládá se využívání čipových karet se šifrovacím čipem. Vyžadován je vysoký stupeň odolnosti proti možnosti klonovat takové karty nebo neoprávněně manipulovat s obsahem peněženky.

Pro některé typy operací není požadována autentizace/identifikace držitele karty a tedy v tomto případě není požadována technologie elektronického podpisu.

Nabíjení je standardní kredit/debetní operace a je založená na EMV specifikaci pro autentizaci.

EMV

Tři hlavní platební systémy, EuroPay International, MasterCard International & Visa International (EMV) vytvořily společnou specifikaci pro interoperabilitu při platbách a dalším používání těchto čipových karet.

První standard byl vydán v roce 1996 a nazýval se EMV 3.1.1. Poslední verze se nazývá EMV 2000 (verze 4) a byla vydána v prosinci 2000.

Ve standardu je popsán soubor používaných funkcí s různými stupni bezpečnosti. Autentizace ke kartě používá statické nebo dynamické ověření údajů. Při použití dynamické autentizace se používá elektronický podpis (soukromý klíč) a tedy je nutno použít speciální šifrovací čip. Terminál musí ověřit veřejný klíč karty zkontrolováním certifikátu vydaného bankou k příslušnému veřejnému klíči. Při použití statické autentizace se příslušný stupeň bezpečí zajišťuje pomocí symetrické kryptografie. Klíč je bezpečně uložen v kartě. Autentizace držitele karty není povinná (například není užívána v současné době v UK), k autentizaci se předpokládá vložení PINU v otevřené podobě nebo šifrování pomocí veřejného klíče.

Project MEDEA A111

Jedná se o společný projekt firem Bull CP8 (vedoucí projektu), Xiring, Cyber-Comm, STMicroElectronics, Banksys. Cílem je vytvoření levného integrovaného obvodu pro spolupráci s čipovými kartami. Předpokládá se vývoj pro různá nasazení a pro různé hladiny bezpečnosti. Počítá se s výrobou od jednoduchých, transparentních čteček až po speciální zařízení s vestavěnou klávesnicí a obrazovkou. Z hlediska bezpečnosti se opět předpokládá škála zařízení od nízkého zabezpečení (low-level) až po EAL 4+ (podle ISO 15408) (Cyber-comm vytvořil dokonce vlastní Protection Profil pro tato zařízení).

Nejbezpečnější z těchto čipů (EPCM) podporuje všechny základní funkce požadované pro klasické terminály, ale i funkce pro terminál, který akceptuje čipové karty firmy Cyber-Comm. Integrování těchto funkcí do jednotné architektury je ekonomické a ukazuje se, že je lze provést bezpečným způsobem.

STIP

STIP je nevýdělečná organizace (STIP "Small Terminal Interoperability Platform"). O jejím vytvoření bylo rozhodnuto na JavaCard fóru v 1999.
Za tímto účelem se blíže definuje softwarová platforma, která:
- podporuje opakované bezpečné transakce terminálu
- poskytuje potřebnou interoperabilitu k nasazení aplikací s využitím velkého množství různých typů zařízení
- poskytuje platformu a aplikaci pro správu životního cyklu
- může být implementována na malá zařízení s omezenými zdroji (typicky čipové karty)

STIP vytvořilo první verzi 1.0 svého API v prvním pololetí 2000, draft verze s plnou specifikací má být publikován na začátku roku 2001. Konečná verze (2.0) bude publikována

na konci jara 2001.

Členové této organizace jsou Verifone, Dassault AT, Bull, Gemplus, Racal, KeyCorp, Ingenico,Schlumber, Smart Move, Lip, Landis&Gyr.
Adresa : http://www.stip.org

Utimaco Safeware Limited

Utimaco má 4 vývojová centra - dvě v Německu, jedno v Rakousku a jedno v Belgii. Utimaco Safeware Limited vyvíjí unikátní "viewer" technologii jako integrovanou součást vlastního řešení Secure Messaging. Vytvářený dokument je sejmut z monitoru ("Snapshot"), zabalen do obálky ("an envelope") a pak podepsán i s obálkou. To zajišťuje, že odesílatel i příjemce vidí stejný text, není možno "přibalit" nějaká záludná makra atd.

Produkty SafeGuard® Sign&Crypt obsahují komponentu pro bezpečné generování a snímání dokumentu (generování textu do grafického formátu a následné sejmutí tohoto dokumentu z monitoru. Co vidím, to podepisuji ("What you see was signed!").
SafeGuard® Sign&Crypt umí vytvořit text a zajistit jeho podpis v e-mailu nebo samostatném souboru.

Detaily na adrese : http://www.utimaco.com

FRANCIE

CertPlus

Je prvním a současně nejdůležitějším PCS ve Francii. Byl založen již v roce 1998 skupinou: Gemplus, France Telecom, Aerospatiale Matra a Verisign.

Skupina připravila zkušební projekt v oblasti B2C. Projekt B2C eCommerce byl zpočátku zahájen třemi bankami BNP Paribas, Credit Lyonnais, Societe Generale a subjekty Francie Telecom, Gemplus a Visa. Na začátku roku 2000 se banky spojily do Banques Populaires Group. CertPlus je operátor skupiny Cyber-COMM, připravované řešení je založené na PKI. (CertPlus používá US Verisign technologii).
Adresa http://www.certplus.com

Certinomis

Certinomis je další francouzský PCS, tentokráte jsou zakládajícími členy : La Poste a Sagem. V rámci nevyhlášené "ekonomické války mezi EU a US" je jejich řešení založeno pouze na francouzských technologiích.
Adresa: http://www.certinomis.fr

Cashware

Dalším operátorem (PCS) je Cashware. Adresa http://www.cashware.com/

MEFI
(Ministère de l'Economie, des Finances et de l'Industrie = francouzské ministerstvo hospodářství, financí a průmyslu)

MEFI je projekt z oblasti B2A mezi francouzskou administrativou a obchodním (business) sektorem (SME, ...). Předpokládá se, že během několika měsíců budou francouzské podniky moci vyplňovat daňová přiznání on line na Internetu. MEFI definuje certifikační politiku pro předpokládanou PKI implementaci. Předpokládá se dodávání certifikátů od CertPlus a Certinomis.
Adresa : http://www.finances.gouv.fr/innovation

ChamberSign

ChamberSign je iniciativou národních obchodních komor deseti evropských zemí (Rakousko, Belgie, Francie, Německo, Itálie, Lucemburk, Nizozemí, Španělsko, Švédsko, UK) pro B2B služby. Adresa http://www.chambersign.co.uk

ChamberSign France je zapojen do MEFI projektu. Předpokládá dodávat B2A služby založené na softwarovém řešení. Certifikáty a RSA klíče (veřejný a soukromý) budou uložené na pevném disku PC koncového uživatele (společnosti). Francouzská obchodní komora bude fungovat jako registrační autorita (RA) PKI. Jako certifikační autority (PCS), která vydává certifikáty a vede jejich správu, se předpokládá využití jednoho ze dvou hlavních operátorů na trhu (v tomto okamžiku o něm není rozhodnuto).

French Chartered Accountant Council

French Chartered Accountant Council realizuje vlastní B2A projekt (pro své účetní) založený v první fázi na používání hesel ... ale již teď se připravují práce na definici PKI využívající elektronický podpis založený na čipové kartě (SINUS).

Identrus

Jedná se o B2B projekt mezi bankami, využívající PKI a založený na čipových kartách. Adresa http://www.identrus.com

Mezi sedmi klíčovými hráči tohoto projektu je i firma Ernst & Young. Projekt má být připravován během následujících 18-ti měsíců. Identrus má dobré vyhlídky v zavedení těchto služeb, protože i nyní jsou již jeho služby globální a celoevropské... výsledky mohou být využity pro platební režimy v rámci EMV v celé Evropě.

C. Jak se lámal podpis (útok na PGP)

RNDr. Miroslav Šedivý, soudní znalec v oboru kryptologie

V polovině března tohoto roku se země zachvěla. Na lopatkách ležel jeden z pilířů našeho elektronického života – sám elektronický podpis. Před námi se rýsovala chmurná budoucnost (především našich účtů) a ….. a dost. Tato mediální bomba se rychle vysvětlila, firma ICZ si po svých příslovečných minutách slávy dojedla i následné hořké plody svého úsilí, a teď je tedy čas se zamyslet i nad odbornou stránkou věci, která – na rozdíl od té mediální – jistou hodnotu má.

Oč tedy v kauze PGP jde.

Nebudeme se zabývat vznikem PGP, jeho historie je obecně známá. Zastavme se jen u faktu, že Zimmermann nebyl kryptolog (především byl programátor), pociťoval však nedostatek kvalitního software, který by poskytoval kryptografickou ochranu během přenosu dat Internetem a tak ho tedy dodal. Tam je pravděpodobně příčina toho, že později navrhovaný standard „Open PGP“ (RFC 2440 - *OpenPGP Message Format*), který vycházel právě z existujících verzí PGP, obsahuje několik hrubých chyb.

Jaké že to jsou chyby a jak je lze využít?

Programy rodiny PGP používají pro ukládání klíčů (veřejných a privátních) soubory obecně pojmenované *pubring.pkr* a *secring.skr*. V těchto souborech je veřejný klíč uložen otevřeně, privátní klíč (je uložen jen v *secring.skr*) je přešifrován pomocí klíče odvozeného z přístupového hesla uživatele,. V případě, že uživatel potřebuje pracovat s uvedenými klíči, program si „natáhne“ tyto informace ze souboru (pokud jde o privátní klíč, dešifruje data, která jej obsahují). V případě privátního klíče navíc zkontroluje jejich celistvost. Pokud je vše v pořádku, pokračuje dále.

Hlavní chyba spočívá v tom, že některé programy PGP (a o ty právě jde) nemají dostatečnou kontrolu souborů s uloženými klíči. Veřejný klíč zde není zabezpečen vůbec (toho využívá útok proti DSA), jediná kontrola privátního klíče spočívá ve výpočtu kontrolního součtu (aritmetický součet dvoubajtových hodnot modulo 2^{16}), kterou je relativně snadné obejít (další chyba - toho využívá útok proti RSA). Program sám již dále vůbec nekontroluje, zda používá skutečně správná data. Díky tomu je možné programu podvrhnout jiné parametry veřejného klíče (případ DSA) nebo poškodit pomocný parametr použitý pro výpočty (případ RSA). Poslední chybou je špatný výběr módu pro šifrování – CFB – jak uvidíme dále.

Podívejme se nyní na jednotlivé útoky, nejdříve RSA. Jak známo, výpočet podpisu (což je vlastně šifrování hash hodnoty zprávy pomocí tajného exponentu *d*) se neprovádí tak, jak je uveden ve vlastní definici RSA, tedy jako $S=(H)^{d} \bmod N$, kde H je hash zprávy, ale kvůli zefektivnění výpočtu je použita formule vyplývající z čínské věty o zbytcích:

$S = S_p + InvP * p * (S_q - S_p);$ $\qquad N=p * q;$
kde

$InvP = p^{-1} \bmod q$
$S = H^{(d \bmod (p-1))} \bmod p$
$P = H^{(d \bmod (q-1))} \bmod q$.

Tento postup vychází z PKCS #1 (viz např.[4], kde však je role p a q přehozena).

Právě parametr *InvP* je oním citlivým místem, protože je pro každou zprávu stejný (závisí jen na *p* a *q*) a je tedy možné (a tak je to i v PGP) tento parametr spočítat předem a uložit ho s ostatními částmi privátního klíče.

Co se stane, jestliže tento parametr změníme na *InvP´*, aniž by si toho uživatel všiml? Především se špatný parametr použije při výpočtu podpisu a ten tedy bude špatně, takže podpis se neověří (ověřující nezná *p* a *q*, takže musí vycházet při výpočtu ze vzorce daného definicí, tedy „otrocky"). Předpokládejme, že tuto zprávu získáme. V tom případě máme:

- správnou hash hodnotu *H* zprávy (získáme výpočtem ze samotné zprávy)
- špatnou hodnotu *S'* podpisu, o které víme, že

$S´ = S_p + InvP´ * p * (S_q - S_p)$
Jenže správně mělo být
$S = S_p + InvP * p * (S_q - S_p)$

Jestliže tyto dvě rovnice odečteme, dostaneme
$S´ - S = (InvP´ - InvP) * p * (S_q - S_p)$,
$S´ = S \bmod p$

Takže rozdíl *S´- S* je dělitelný *p*!!! My ovšem známe jen *S´*, nikoliv už *S*. To ale nevadí, protože známe, případně umíme spočítat
$(S´)^e$
protože známe *S´* a *e* - veřejný exponent
$(S)^e = H$
S je správná hodnota podpisu a uvedená rovnost je z definice RSA, *H* prostě spočítáme ze zprávy. Umocníme proto poslední kongruenci na exponent *e* a máme

$S' \equiv S \bmod p$
$(S´)^e \equiv (S)^e \bmod p$
$(S´)^e \equiv H \bmod p$
takže $p \mid (S´)^e - H$

Nyní již je hračkou spočítat *p* jako největšího společného dělitele čísel $(S´)^e - H$ a *N (= p * q)*. Pravda, může se stát, že číslo $(S´)^e - H$ bude dělitelné i *q*, pravděpodobnost je však velice malá (řádově q^{-1}).

Pro provedení útoku je tedy dostačující změnit parametr *InvP* , odchytit podepsanou zprávu a uvedeným jednoduchým postupem získat nejdříve *p* a poté již i vše ostatní podstatné hodnoty (samozřejmě pak rychle vrátíme původní *InvP* - přesněji vrátíme celý původní soubor *secring.skr*). Zbývá jediný problém - jak pozměnit *InvP*, aby si toho program nevšiml. Již bylo uvedeno, že údaje týkající se privátního klíče jsou šifrovány a zabezpečeny kontrolním součtem. Ve verzi 3 (RFC 2440 uvádí dvě verze – starší verzi 3, která zná jen RSA, a novou verzi 4) je situace jednoduchá - šifrován je pouze obsah jednotlivých položek (*d, p, q, InvP*), ne však jejich délky. Rovněž kontrolní součet není šifrován. Stačí tedy změnit délku *InvP* a o rozdíl mezi původní a pozměněnou délkou změnit i kontrolní součet. Vzhledem k tomu, že jde o aritmetický součet (mod 2^{16}), tato operace způsobí, že nový kontrolní součet bude opět odpovídat sčítaným hodnotám.

Ve verzi 4 již je situace složitější. Šifruje se celé pole parametrů včetně následujícího kontrolního součtu. Použit je však „bohužel" mód CFB (cipher feedback) a pokud si

uvědomíme, že poslední blok šifrového textu vznikl operací XOR otevřeného textu a hodnoty, která na posledním bloku otevřeného textu nezávisí, je jasné, že pokud změníme jakýkoliv bit posledního bloku šifrového textu, projeví se to (po dešifraci) změnou odpovídajícího bitu posledního bloku otevřeného textu. A poslední blok otevřeného textu je tvořen právě bity kontrolního součtu (těch je jen 16) a dále posledními bity *InvP*, neboť právě tento parametr leží před kontrolním součtem (počet těchto posledních bitů závisí na délce bloku použitého symetrického algoritmu pro přešifrování, s velkou pravděpodobností tam ale vždy nějaký bajt *InvP* bude). Můžeme tedy změnit např. poslední bit kontrolního součtu a poslední bit *InvP* (bude o 16 bitů zpět). Pravděpodobnost, že takto upravená data budou „sedět“ oproti upravenému kontrolnímu součtu je ½ . Pokud se tak nestane, pozměníme jiný bit (variací je tady mnoho, vždy jde o změny bitů na odpovídajících si místech vzdálených od sebe o násobek 16). Útok v případě verze 4 je tedy úspěšný jen s určitou pravděpodobností, nicméně s počtem pokusů se pravděpodobnost zvyšuje.

Poznamenejme ještě pro úplnost, že myšlenka útoku využívající speciální výpočet podpisu podle [4] není nová, o podobných technikách nalezneme zmínku i v [1] a [2] . I když je v uvedené literatuře v detailech přístup trochu odlišný, výsledný efekt je stejný.

Jiný přístup byl zvolen v případě algoritmu DSA. Zde je použita myšlenka nahradit původně výpočetně složitou grupu grupou, která má jednoduchou strukturu.
DSA používá následující parametry:

- prvočísla p a q taková, že platí $2^{1023} < p < 2^{1024}$, $2^{159} < q < 2^{160}$ a $q \mid p-1$ ·
- dále necht' g je generátor cyklické podgrupy řádu q grupy Z_p* (zpravidla se volí libovolné h a položí se $g = h^{(p-1)/q}$, pokud je $g = 1$, volí se jiné h)
- zvolí se privátní klíč x, $0 < x < q$ a vypočte se $y = g^x$.
- hodnoty g, p, q, y jsou veřejné, hodnota x je tajná.

Postup výpočtu podpisu je následující:
- vybere se (tajný) parametr k, $0 < k < q$. a vypočtou se
- $R = (g^k \bmod p) \bmod q$, (1)
- $S = (k^{-1} * (H + x * R)) \bmod q$,

R a S tvoří podpis, parametr k se dále nepoužije.

Myšlenka útoku v podstatě tkví v degradaci algoritmu podpisu tak, aby byl výpočetně zvládnutelný a zároveň aby nedošlo ke ztrátě podstatné informace o klíči x. Tentokrát jsou měněny veřejné parametry (nejsou programem kontrolovány!!!), konkrétně p a g. První myšlenka je změnit p na $p´$ tak aby $p´$ bylo menší než q, tím se totiž ve vzorci (1) odstraní kongruence *mod q* a tento vzorec nyní vypadá takto :

$$R = g´^{k} \bmod p´ \qquad (2)$$

Původní generátor g jsme změnili na g´, s tím, že g´ teď bude generátorem grupy $Z_{p´}$* . Generátor g´ určíme takto: zkoušíme různé hodnoty g´, zda pro ně platí, že pro všechna prvočísla l z rozkladu čísla p´- 1 je

$$g´^{(p´-1)/l} \neq 1 \bmod p´,$$

až takové g´ najdeme (proces hledání je relativně rychlý). Poznamenejme ještě, že vždy platí
$g´^{(p´-1)} = 1 \bmod p´$ (3)

Předpokládejme, že jsme zachytili zprávu podepsanou pomocí našich pozměněných parametrů a původního x. Je tedy

$R = g'^{k} \bmod p'$
$S = (k^{-1} * (H + x * R)) \bmod q,$
takže
$x = R^{-1} * (S * k - H) \bmod q.$

Jediné, co potřebujeme k určení x je hodnota k (vše ostatní známe). Pokud dokážeme získat tuto hodnotu, získáme i x.

Hodnotu k máme šanci získat ze vzorce (2), pokud bychom ovšem uměli řešit úlohu diskrétního logaritmu pro grupu $Z_{p'}^*$. I tak bychom ovšem získali pouze hodnotu $k_0 = k \bmod (p'-1)$. To ale nebude vadit, pokud se p a q nebudou příliš lišit, protože pro skutečné k platí

$k = k_0 + t * (p - 1) \quad 0 < k < q,$

tedy
$0 < t < (q - k_0) / (p - 1) \leq q / (p - 1)$

Pokud tedy bude p' řekněme v rozmezí $2^{158} < p' < 2^{159}$, bude v nejhorším případě $t < 4$ (takže budeme mít pro t možnosti 0, 1, 2, 3). Stejný počet možností bude pro k a tedy i pro x. Správnou hodnotu x najdeme pak prostým přezkoušením pomocí jiné podepsané zprávy se správnými hodnotami p a q.

Zbývá tedy určit hodnotu $k \bmod (p' - 1)$, kterou dále budeme značit pro jednoduchost k. Už víme, že jde o úlohu diskrétního logaritmu pro multiplikativní grupu $Z_{p'}^*$. Tato grupa má řád p'- 1 a je známo, že pokud se v rozkladu čísla p'- 1 vyskytují pouze malá prvočísla, lze tuto úlohu řešit. My jsme zatím prvočíslo p' omezili podmínkami na jeho velikost, z faktu v předchozí větě plyne tedy ještě omezení na jeho tvar.

Jestliže tedy najdeme prvočíslo p' takové, že $2^{158} < p' < 2^{159}$ a zároveň je
$p' - 1 = \Pi\, l_j^{ej}$ (kde všechna l_j jsou malá)
jsme schopni úlohu diskrétního logaritmu řešit, tedy zjistit k z rovnice (2) při znalosti g' a R.

Postup hledání k je jednoduchý. V tomto místě (viz [5]) se autoři útoku poněkud nechali unést výkladem základů teorie konečných polí, my je však potřebovat nebudeme. Nechť l je jedno z prvočísel v rozkladu a e je jeho exponent v rozkladu. Napišme k ve tvaru
$k = m_0 + l * n_0, \qquad 0 \leq m_0 < l$

Máme
$R = g'^{\,m0 + l * n0} \bmod p'$

takže po umocnění na exponent $(p' - 1) / l$ (celé číslo) dostaneme
$R^{(p' - 1) / l} = (g'^{(p' - 1) / l})^{m0} \bmod p' \qquad (4)$
Vše ostatní je pryč díky rovnosti (3). Čísla
$(g'^{(p' - 1) / l})^{m0} \bmod p'$

probíhají, pokud budeme volit m_0 v daném rozmezí od 0 do l - 1, navzájem různá čísla

(jinak by totiž $g´$ nebyl generátor dané grupy $Z_{p´}$*), takže jen pro jedno (a právě jedno) m_0 může být rovnice (4) splněna. Je tedy $k = m_0 + l * n_0$, kde m_0 již známe. Pokud je exponent e roven 1, jsme hotovi, pokud je $e \geq 2$, pokračujeme dále a můžeme rozepsat k jako

$$k = m_0 + l * m_1 + l^2 * n_l, \qquad 0 \leq m_1 < l$$

a je tedy

$$R = g´^{\,m_0 + l * m_1 + l^2 * n_l} \ mod\ p´$$

takže

$$R * g´^{\,-m_0} = g´^{\,l * m_1 + l^2 * n_l} \ mod\ p´$$

Nyní tuto rovnici umocníme na exponent $(p - 1) / l^2$ ($e \geq 2$, takže jde opět o celé číslo) a po úpravách získáme obdobnou rovnici jako byla (4), ale nyní již pro m_l:

$$\left(R * g´^{\,-m_0}\right)^{(p´-1)/l^2} = \left(g´^{\,l * m_1 + l^2 * n_l}\right)^{(p´-1)/l^2} \ mod\ p´$$

$$R_1 = \left(R * g´^{\,-m_0}\right)^{(p´-1)/l^2} = \left(g´^{\,(p´-1)/l}\right)^{m_1} \ mod\ p´ \qquad 0 \leq m_1 < l$$

kde R_1 je hodnota, kterou umíme spočítat. Opět stačí probrat hodnoty m_1 od 0 do $l - 1$ a zjistit, kdy nastane v (5) rovnost.

Stejně postupujeme dále pro další koeficienty v rozvoji a nakonec tak určíme všechna čísla $m_0 , m_1 , \ldots, m_{e-1}$ taková, že platí

$$k = m_0 + l * m_1 + \ldots + l^{e-1} * m_{e-1} + l^e * M_e$$

$$k = (m_0 + l * m_1 + \ldots + l^{e-1} * m_{e-1}) \ mod\ l^e$$

Našli jsme tedy číslo k_l takové, že platí

$$k \equiv k_l \ mod\ l^e$$

přičemž uvedený postup můžeme aplikovat pro všechna prvočísla l z rozkladu $p´ - 1$. Je jasné, že praktická možnost určení čísla k_l závisí jen na velikosti l. Po určení k_l pro všechna l již jen stačí aplikovat čínskou větu o zbytcích a získáme

$$k \ mod\ (p´ - 1),$$

což jsme potřebovali.

Autoři útoku zvolili $p´ = 167 * 2^{151} + 1$, takže v rozkladu jsou pouze prvočísla 2 a 167, jimi uváděný tvar ($t * 2^s + 1$) však není vzhledem k výše uvedenému postupu podstatný, vyhovuje jakékoliv prvočíslo námi uvedeného tvaru.

Literatura

[1] D. Boneh, R. A. DeMillo, R. J. Lipton : „*On the Importance of Eliminating Errors in Cryptographic Computations"*; rozšířená verze příspěvku pro Eurocrypt 97.

[2] A. K. Lenstra.: „*Memo on RSA signature generation in the presence of faults"*; manuscript; 1996

[3] RFC 2440 - *OpenPGP Message Format*

[4] PKCS #1, v. 2.0, RSA Laboratories 1998

[5] V.Klíma, T.Rosa Rosa : „*Útok na privátní podpisové klíče formátu OpenPGP, program PGP ™ a dalších aplikací kompatibilních OpenPGP*“, zveřejněno na http://www.i.cz

D. Smart-Card with Quantum Entanglement

Jaroslav Hrubý, Ondřej Haderka

Abstract

We present an application of quantum cryptography with quantum entanglement for smart-cards.

1. Introduction

An interesting application of quantum cryptography for smart-cards using quantum transmission of photons and an application of quantum key distribution for the quantum identification system were published [1]. Here we present a new application of quantum entanglement for smart-cards.

The necessity to look for more secure smart-cards follows as the consequence of the fault case presented in the New York Times headline [2] or new attacks via power and differential power analysis [3].

Generally there are the following basic problems with existing identification systems using smart-cards:

1) the customer must type the PIN (Personal Identification Number) to an unknown teller machine which can be modified to memorize the PIN;
2) the customer must submit the smart-card with information needed for the identification to an unknown teller machine; in presence of an eavesdroper it can be also memorized together with the PIN.
3) the smart-card based on silicon technology can be attacked even without its interaction with the teller machine via many noninvasive physical attacks.

In this way such identification system via smart-card can fail. The solution of these problems is to employ optical fibres and optoelectronics on the smart-card together with entangled quantum optical states.

Here we present a new identification system, which in principle can be based on quantum entanglement of two photons and which solves these basic problems in the following way:

1) PIN will be typed directly to the card for activation of the optoelectronics devices located on the smart-card and no PIN information will be exchanged with the teller machine.
2) The information needed for the identification of the card inside the teller machine will be protected against an eavesdropper through non-local projection of the state of one member of the pair of entangled photons which will happen during its propagation directly on the smart card.
3) The power source is put directly on the smart-card (e.g., a photocell).

It is well known that in the ordinary teller machine without quantum channels all carriers of information are physical objects open to copying or cloning. The information for the identification of the card is enclosed by modification of their physical properties. The laws of the classical theory allow the dishonest eavesdropper to measure and copy the cryptographic key information precisely.

This is not the case when the nature of the channels is such that quantum theory is needed for their description. Any totally passive or active eavesdropper operating on the quantum

channel can be detected.

The current development of technologies of fiber and intergrated optics makes it possible to construct quantum optoelectronic smart-card for our application. The travelling distance for quantum transmission is very short here. This means, that the problems appearing in application of ordinary quantum cryptography in optical communications are negligible here.

The new idea presented here is, that the projection on a selected polarization basis of the entangled photon from the Einstein-Podolsky-Rosen (EPR) pair of polarized photons occurs directly inside the smart-card, at the moment when the second member of the pair is measured in the same basis inside the teller machine.

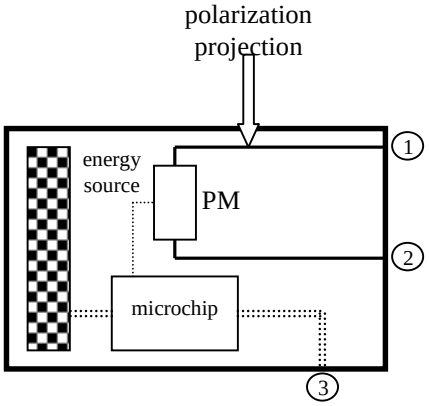


Figure 1. Schematic representation of the QC smart-card

2. The quantum entanglement for the smart-card

A scheme of the QC smart-card with the quantum entanglement is given in Fig.1. Here the solid line presents the quantum channel (optical fiber), the double dotted line presents the electric connection from the photocell source and signal connection with teller machine. The single dotted line is the signal pulse connection between the microchip and polarization modulator, which are integrated and with active shielding are ”secure“ against external measurements of electromagnetic fields from signal pulses. An arrow indicates the position of the correlated photon on the smart-card at the instant of the measurement of the other member of the pair in the teller machine.

This quantum card consists of:

a) a PIN activator, which can have the form of the ordinary card light-source calculator with sensor keys; the user puts the PIN on the card to identify himself in a secure distance from the teller (i.e. unknown quantum cryptographic verification device) and in a secure outer area; the card will be blocked when the sequence of the three incorrect PINs will be given; as soon as the activated card is not used within short time period (say, 20 s), the activation is closed;
b) a microchip with the implemented cryptographic key $\{0,1\}^n$ which is long enough to yield required security for the given protocol; the microchip is activated when correct PIN is entered on the card;
c) a polarization modulator (PM), which transforms the cryptographic key $\{0,1\}^n$ to the optical polarization states of the photon under the following encoding rules:
   “0” is encoded as no change of the polarization;
   “1” is encoded as change of the polarization state to the other basis state.
d) a quantum channel consisting of a singlemode optical fiber.

The smart-card is equipped with the optical connectors ①,② for connecting the quantum channel to the teller machine and electric connector ③ that serves for auxiliary communication needed to trigger and synchronize the operation of the smart-card with the arrival of photons from the teller and possibly also for the exchange of classical information needed for realization of the cryptographic protocol.

Present technologies give the possibility to construct the card without significant radiation of electromagnetic energy and a new generation of microchips, which together with optoelectronics elements are resistant against possible known physical attacks. The main advantage is that no classical secret information ever leaves the smart-card, only quantum information is going out.

In this way the smart-card controls the polarization of the photon which was projected randomly at one of the two possible polarization states directly on the smart-card and no eavesdropper inside the card slot has a chance to read-out the authentication information without being detected.

3.The teller machine with quantum entanglement

The teller machine, which is based on the quantum correlation principle, is plotted in Fig.2 and consists of :

i) source of EPR photons; a pulsed laser source can be used to pump the down-conversion process in a nonlinear crystal;
ii) the delay line that determines the moment of the projection of the polarization state of the correlated photon on the smart-card at the moment of the detection of the second member of the pair in the teller machine;
iii) the polarization controller serves for compensation of the polarization changes in the device,
iv) Wollaston prism I serves for random projection of the polarization of one of the photons while Wollaston prism II is used to analyze the resulting polarization state of the other photon;
v) the two pairs of photon-counting detectors are used to detect the outputs of the Wollaston prisms. The first pair of detectors (A,B) detects the realization of random projection in the Wollaston prism I for the photon that remains inside the teller machine. The second pair of detectors (C,D) is used to measure the state of the second EPR photon which is coming modified or not-modified from the smart-card. Via modification of the polarization smart-card sends its secret;
vi) the computer that drives the operation of the whole device and where the information obtained by measurement on the detectors A,B,C,D is processed according to the given cryptographic protocol and the authentication key is compared to its stored replica;
vii) all quantum optical paths inside the teller machine can be done with ordinary optical single-mode fibers (solid line) and electric signal channel (dotted line) are in the same quality like on the smart-card;

In such realization the smart-card controls polarization while the teller machine controls detectors and can obtain the secret information from smart–card only via quantum transmission. The teller machine accepts or rejects the smart-card if the secret information coincides with the replica stored in its database up to a tolerable amount of errors. Some amount of errors must be tolerated due to physical imperfections of the device.

This is the authentication of the smart-card, which can be improved via known cryptographic protocols that combine sending the classical public information, which can be under eavesdropper’s control, and quantum secret information, where eavesdropper’s activity will be detected.

4. Conclusions

We have discussed the possibility to utilize the advantages of quantum correlation for authentication. Of course if we have more ”robust“ smart-card with detectors we can provide the mutual identification between smart-card and teller machine via quantum cryptography.

Manufactures should be encouraged to develop enough cheap photon-counting detectors and smaller optoelectronics elements integrating the new generation of microchips with polarization modulators.

We have shown a new positive solution to the open problem connected with the smart-card security.

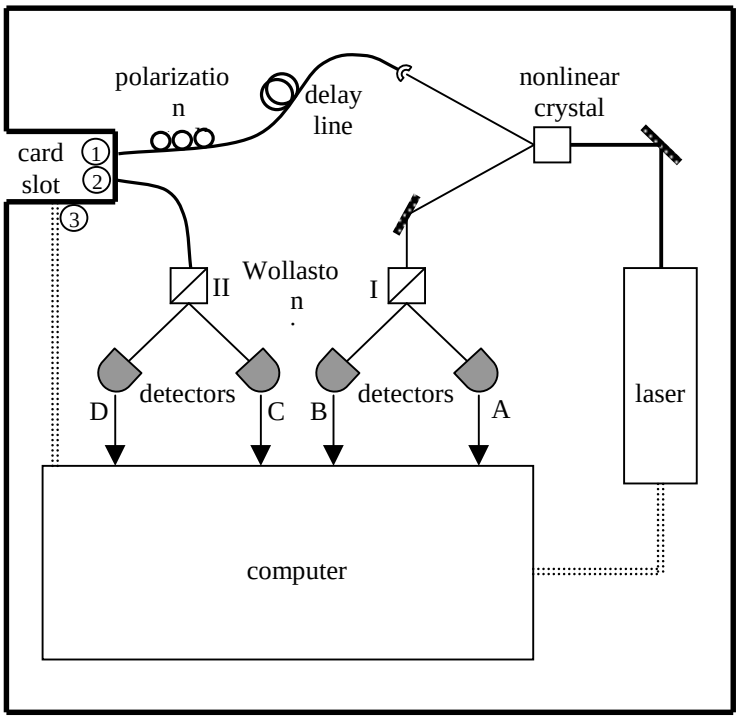


Figure 2. Scheme of the quantum teller machine based on the quantum correlation

Acknowledgement

This work was supported by grants RN19982003012, RN19982003013 and LN00A015 with subvention of the Ministry of Education of the Czech Republic.

References

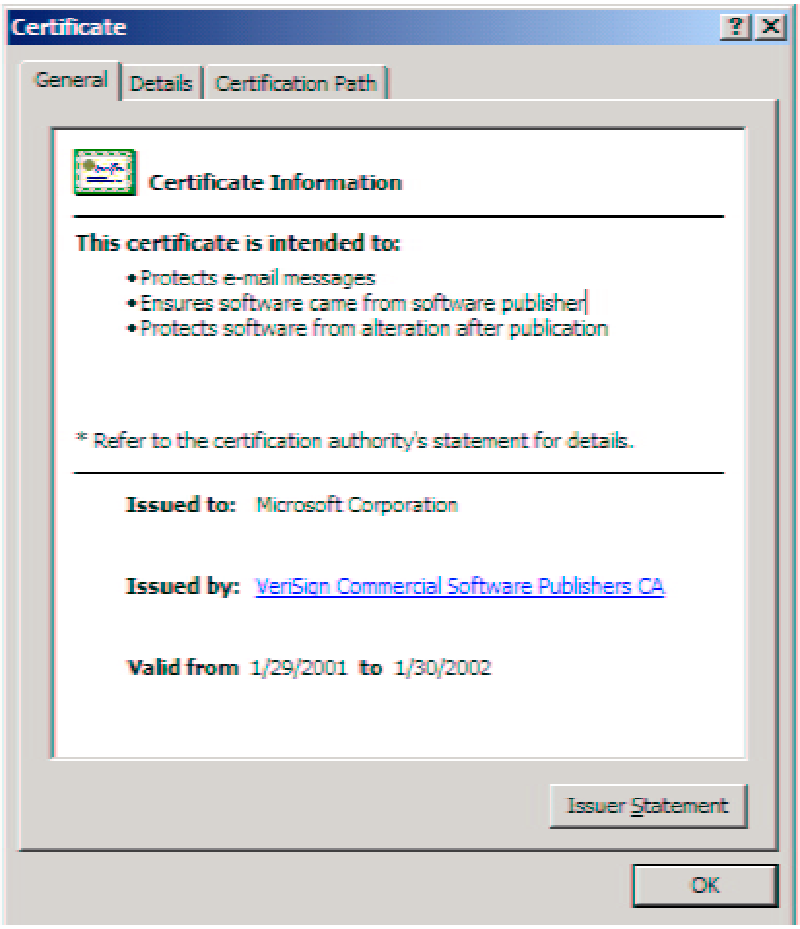
[1] J.Hrubý,“Smart-card with Interferometric Quantum cryptography device“, Lecture Notes in Computer Science 1029 (1995), p.282; M. Dušek, O. Haderka, M. Hendrych and R. Myška, “Quantum identification system“, Phys. Rev A, v.60 ,n.1 (1999), p.149.

[2] One Less Thing to Believe In: Fraud at Fake Cash Machine, New York Times 13 May 1993, pp. A1 \& B9.

[3] ASIACRYPT 2000

E. Letem šifrovým světem

1. **Elektronický / digitální podpis od Microsoftu nemusí být to pravé :-) !**
   Uprostřed března se přišlo na to, že jedna z největších a nejznámějších certifikačních autorit VeriSign, Inc. vydala dva certifikáty (ve velice důvěryhodné třídě - Class 3) fyzické osobě, která se vydávala za zaměstnance Microsoftu. Jméno, na které byly certifikáty vydány, zní "Microsoft Corporation". Tyto certifikáty byly vydány 29.1. a 30.1.2001.
   Co s nimi může potenciální útočník provádět ? Útočník může jménem firmy Microsoft podepsat řadu spustitelných programů, které se používají k update produktů Microsoftu, podepsat komponenty jako ActiveX, makra ve Wordu apod. K podpisu přiloží získané certifikáty. Systém má v takto podepsané komponenty / produkty důvěru a automaticky je otevře, neboť při ověření použije data z těchto certifikátů znějících na jméno Microsoft. Firma VeriSign ihned poté, co zjistila, že byla oklamána, tyto certifikáty zneplatnila a umístila informaci do CRL (seznamu zneplatněných certifikátů). Jenže, ruku na srdce, kdo z nás si kdy stáhnul seznam zneplatněných certifikátů firmy VeriSign ? Firma Microsoft se zachovala velice zodpovědně. Nebezpečí ihned přiznala. Vydala příslušné bezpečnostní prohlášení, včetně technických detailů. Dále připravila bezpečnostní záplatu, kterou si můžete pro všechny verze Windows bezplatně stáhnout z jejího webu. Jak záplata funguje? V podstatě velice jednoduše. Obsahuje informace o těchto dvou zneplatněných certifikátech. Před každým ověřením podpisu Microsoftu se nejdříve kontroluje, zda se nejedná o tyto "nepravé" certifikáty. Rada na závěr , jak poznat neplatné certifikáty? Velice snadno - datum vystavení 29.1. a 30.1.2001 totiž žádný platný certifikát Microsoftu nemá!



Prvý ze dvou neoprávněně vydaných certifikátů

2. Skončil březen - měsíc Internetu. Na tyto oslavy navázala jiná událost, která předchozí akci "zdařile" parodovala. Prvního dubna se v Praze na Letné uskutečnil "Den bez Internetu". Účastníci si vyměňovali ručně psané e-maily, soutěžili ve vyhledávání informací na známých "portálech" (např. hledáním v tištěném telefonním seznamu). Uskutečnila se i soutěž v downloadu (stahování svetru). Vypsána byla i soutěž v napodobení "elektronického" podpisu pana poslance Vladimíra Mlynáře.

3. Krátká informace o jedné nechtěně rozšířené aplikaci elektronického podpisu.
   Touto aplikací je W32/Hybris. Je to e-mailový červ s implementovanou schopností modifikovat své vlastnosti prostřednictvím doplňků - pluginů, které mohou být distribuovány prostřednictvím Internetu. Červ kontroluje získaný plugin (prvé 4 znaky jsou "název" a další 4 znaky verze pluginu). Každého čtenáře jistě napadne, že by nějaká antivirová firma mohla vytvořit vhodný plugin, pomocí kterého by se dalo červa elegantně po celém Internetu zbavit. Toto ale bohužel nelze. Červ je vybavený mechanizmem autorizace pluginů, který zabezpečí, že jsou akceptovány jen ty moduly, které autor červa elektronicky podepsal.

4. **'High risk' bug found in Internet Explorer** (5.01 - 5.5), James Middleton , Monday 02 April 2001 . IE looks at the Multipurpose Internet Mail Extension (Mime) header of the email to determine which attachments it should open automatically. But it is possible to modify the Mime header and trick the browser into opening files such as executables automatically....
   Další informace jsou dostupné na http://vnunet.com/News/1120040 a dále na http://vnunet.com/News/1120450

5. Dne 15.-16 června 2001 se koná v Bratislavě mezinárodní konference IFIP (The IFIP WG 9.6/11.7 Working Conference on Security and Control of IT in Society-II - SCITS-II). Jedná se o prestižní odbornou akci v oboru bezpečnosti.
   Spojení na organizační výbor :
   SCITS-II organizing committee
   doc. RNDr. Daniel Olejár, CSc.
   KI FMFI UK
   Mlynská dolina
   842 48 Bratislava
   Slovak Republic
   e-mail scits@dcs.fmph.uniba.sk

6. Konference zabývající se informační bezpečností Information Security Conference (ISC'01) se koná v říjnu ve Španělsku (Malaga). Detaily lze nalézt na adrese http://www.isconference.orgfriends

7. O čem jsme psali před rokem ?
   Crypto -World 4/2000
   http://www.mujweb.cz/veda/gcucmp/casop2/Crypto4_00.html

   A. Prohlášení odborné skupiny pro zpracování pozměňovacích návrhů k předloze zákona o elektronickém podpisu
   B. Fermatova čísla (P.Vondruška)
   C. Lekce pro tajné agenty - č.1 : "Neztrácejte své laptopy "
   D. Opět INRIA ! (J.Pinkava)
   E. Nový efektivní kryptosystém s veřejným klíčem na světě? (J.Pinkava)
   F. Code Talkers (I.díl) (P.Vondruška)
   G. Letem šifrovým světem

F. Závěrečné informace

1. Sešit

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

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

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

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

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

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

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

3. Spojení

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

pavel.vondruska@post.cz