Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 6/2002 **17. červen 2002**

6/2002

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/

(327 e-mail výtisků)

Obsah : **Str.**

A. Historie a statistika Crypto-Worldu
Mgr. Pavel Vondruška, GCUCMP

Prvé číslo sešitu vzniklo a bylo rozesláno v září roku 1999. Předcházelo mu nepravidelné rozesílání informací a upozornění na zajímavé články, které souvisely s kryptologií. Sešit sloužil původně velmi úzké skupině lidí – členů kryptologické sekce Jednoty českých matematiků a fyziků (GCUCMP). Postupně byl rozesílán dalším zájemcům. Do září roku 2000 na přípravě sešitu pracoval pouze Mgr. Pavel Vondruška. Na podzim roku 2000 se přidal k přípravě místopředseda GCUCMP ing. Jaroslav Pinkava, CSc. Jeho zásluhou je otiskován rozsáhlý seriál „Kryptografie a normy“. Tento seriál může sloužit jako velice slušný podklad k základní orientaci v dané problematice. Z ohlasů víme, že si jej řada studentů skutečně za tímto účelem uschovává a používá. Některé články k elektronickému podpisu byly zase použity jako podklad pro bakalářské a diplomové práce jiných našich čtenářů / odběratelů. Úspěšná byla i soutěž v luštění klasických šifer (podzim 2000) a moderních šifer (podzim 2001). Postupně se také začal zvyšovat počet našich odběratelů. Od listopadu 2001 vychází Crypto-World za podpory brněnské firmy AEC spol. s r.o. Sešit se vyhýbá všem komerčním článkům a snaží se poskytovat aktuální, seriózní, komerčně nezabarvené informace. Hlavním tématem je v poslední době elektronický podpis a související normy a předpisy.

Od září roku 2001 se počet čtenářů výrazně nemění. V této době byla také zrušena možnost registrace k odběru přes internet. V současné době jsem odstranil všechny adresy, které byly při rozeslání sešitu 5/2002 nedostupné. Pro jednodušší způsob přihlášení k odběru e-zinu, než je zaslání e-mailu na mou adresu, jsem opět na domácí stránku Crypto-Worldu umístil možnost registrovat se pouhým vyplněním zde vyvěšeného formuláře. Pomocí formuláře lze také informovat o tom, že jste nedostali Crypto-World, přestože byl již registrovaným čtenářům rozeslán. Jiný zde umístěný formulář lze zase použít k zaslání dotazu.

Statistika rozvoje Crypto-Worldu

1999

	9/99	10/99	11/99	12/99
Odběratelů	25	31	35	47
Stran	7	10	9	9
Bytů	118 655	163 382	312 601	370 720

2000 – I.pololetí

	1/2000	2/2000	3/2000	4/2000	5/2000	6/2000
Odběratelů	62	76	90	102	107	116
Stran	9	11	11	13	15	16
Bytů	208 173	215 768	212 279	333 340	354 749	502 347

2000 – II.pololetí

	7-8/2000	9/2000	10/2000	11/2000	12/2000	V/2000
Odběratelů	163	190	200	228	230	230
Stran	19	20	24	19	21	17
Bytů	150 000	188 227	284 108	254 586	146 382	291 528

2001 – I.pololetí

	1/2001	2/2001	3/2001	4/2001	5/2001	6/2001
Odběratelů	240	250	260	270	280	300
Stran	22	29	23	25	19	28
Bytů	166 242	231 824	206 663	304 903	391 948	1 084 637

2001 – II.pololetí

	7-8/2001	9/2001	10/2001	11/2001	12/2001
Odběratelů	308	320	322	324	331
Stran	28	23	24	24	22
Bytů	608 089	399 741	609 199	761 270	540 562

2002 – I.pololetí

	1/2002	2/2002	3/2002	4/2002	5/2002	6/2002
Odběratelů	340	344	350	361	342	327
Stran	36	17	27	22	23	20
Bytů	758 126	242 631	445 937	769 920	775 361	259 584*

* velikost e-zinu ve formátu doc

Koncem roku 1999 byla založena a využívána tato webovská stránka :
http://www.mujweb.cz/veda/gcucmp

Přes různé nabídky nebyl (především z „historických“ důvodů) obsah převeden na jinou stránku (např. domény I.řádu).

Stránku a její obsah lze vyhledat pomocí běžných prohlížečů – heslo Crypto-World.

Články (1999-2002), které vás dle kladných reakcí nejvíce zaujaly:

1. Soutěž (9/2000-12/2000)
2. Seriál článků o prvočíslech (4/2000-78/2000)
3. Seriál článků „Kryptografie a normy“ (9/2000-5/2002)
4. Soutěž (9/2001-12/2001)
5. Seriál článků „Codetalkers“ (4/2000-6/2000)

Odkud jsou naši čtenáři :
Česká republika, Slovenská republika, Spolková republika Německo, USA, Rakousko, Belgie, Bulharsko, Polsko

A závěrem malá statistika přístupů na www stránku Crypto-Worldu

Datum zahájení sběru dat pro statistiku:	**11.srpen 2000**
Datum a čas posledního přístupu	**15. červen 2002** (12:39:03)
Počet přístupů za tento měsíc (červen)	161
Počet přístupů za tento rok	2992
Celkový počet přístupů	13484
Průměrný denní počet přístupů	20.04
Průměrný počet přístupů za hodinu	0.83
Nejúspěšnější den těchto stránek byl (tento den zahájeno I.kolo soutěže v řešení úloh)	12. září 2000 s 188 přístupy
Nejúspěšnější měsíc těchto stránek byl	říjen 2000 s 1071 přístupy
Nejúspěšnější rok těchto stránek byl	2001 s 6528 přístupy
Mezi 0:00 a 3:59	359 přístupů (2.66 % všech přístupů)
Mezi 4:00 a 7:59	852 přístupů (6.32 % všech přístupů)
Mezi 8:00 a 11:59	3947 přístupů (29.27 % všech přístupů)
Mezi 12:00 a 15:59	4063 přístupů (30.13 % všech přístupů)
Mezi 16:00 a 19:59	2499 přístupů (18.53 % všech přístupů)
Mezi 20:00 a 23:59	1760 přístupů (13.05 % všech přístupů)
Pondělky	2510 přístupů (18.61% všech přístupů)
Průměrně	26.14 přístupů
Úterky	2477 přístupů (18.37% všech přístupů)
Průměrně	25.80 přístupů
Středy	2528 přístupů (18.75% všech přístupů)
Průměrně	26.33 přístupů
Čtvrtky	2121 přístupů (15.73% všech přístupů)
Průměrně	22.09 přístupů
Pátky	2334 přístupů (17.31% všech přístupů)
Průměrně	24.06 přístupů
Soboty	713 přístupů (5.29% všech přístupů)
Průměrně	7.35 přístupů
Neděle	801 přístupů (5.94% všech přístupů)
Průměrně	8.34 přístupů

B. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 4. Řídící protokol CRMF a CMC.

Jaroslav Pinkava, AEC spol. s r.o.

1. Úvod

Minulá část seriálu se zabývala vlastnostmi protokolu CMP (Certificate Management Protocol - definuje inicializaci, certifikaci, obnovu a odvolávání entit PKI).

Formát CRMF (Certificate Request Message Format) vyvinula skupina PKIX. Tento se opirá jak o CMP tak i o přihlášení dle CRS, ale nepoužívá formát žádosti dle PKCS-10.

Tímto formátem a také protokolem CMC, který napomáhá využívání protokolu pracovní skupiny S/MIME pro řízení PKI bez nutnosti využití CMP (používá PKCS-10) se budou zabývat následující řádky.

2. Formát CRMF

Syntaxe definuje postup jak dopravit žádost o certifikát do CA (možná prostřednictvím RA) s cílem vytvořit digitální certifikát dle normy X.509. Žádost obvykle obsahuje veřejný klíč a s ním spojenou informaci o registraci.

Při vytváření žádosti o certifikát je postup následující:

- je spočtena hodnota `CertRequest value`. Tato hodnota může v sobě zahrnovat veřejný klíč, část či celé jméno koncové entity, další požadovaná pole certifikátu a dále i kontrolní informace ve vztahu k registračnímu procesu;
- je spočtena hodnota `proof of possession` (POP - důkaz vlastnictví soukromého klíče, který odpovídá veřejnému klíči obsaženému v požadovaném certifikátu);
- také lze kombinovat i další informace získané při registraci a tak spolu vytvořit zprávu `CertReqMessage` ;
- tato zpráva je pak přenesena bezpečnou cestou do CA.

Tedy zprávu tvoří žádost o certifikát, dále pole obsahující POP a pole obsahující informace získané při registraci. Poslední dvě pole nejsou povinná. ASN syntaxe je následující:

```
   CertReqMessages ::= SEQUENCE SIZE (1..MAX) OF CertReqMsg

   CertReqMsg ::= SEQUENCE {
      certReq   CertRequest,
      pop       ProofOfPossession  OPTIONAL,
      -- content depends upon key type
      regInfo   SEQUENCE SIZE(1..MAX) of AttributeTypeAndValue
OPTIONAL
   }
```

Vzhledem k tomu, že existují určité možnosti útoků proti postupům při vydávání certifikátů a také, aby bylo umožněno CA (resp. RA) ověřit platnost propojení entity a příslušné dvojice klíčů, vytváří řídící operace PKI postup, který žádající entitě umožňuje prokázat, že vlastní příslušný soukromý klíč. Samozřejmě bez toho, aby tento soukromý klíč byl vyzrazen (komukoliv mimo právoplatného vlastníka). V tomto směru má CA (resp. RA) určitou možnost volby konkrétních postupů, kterými toto provede. Musí však mít k dispozici nějaké prostředky, kterými informaci POP získá a následně zverifikuje. Konkrétní vytváření POP závisí mj. i na typu klíče, pro který je certifikát požadován. Konkrétní postupy také závisí na certifikační politice (kdo ověřuje POP – zda je to CA nebo stačí RA).

V případě klíčů určených pro podpis podepíše koncová entita nějakou konkrétní hodnotu svým soukromým klíčem. Pokud se jedná o klíče sloužící k přenosu jiných klíčů (key encipherment keys) koncová entita získá svůj klíč od CA (resp. RA) anebo je na ní požadováno, aby dešifrovala určitou konkrétní hodnotu (přímo – CA resp. RA zašle náhodné číslo a požaduje okamžitou odpověď; nepřímo – vydáním certifikátu, který je zašifrován veřejným klíčem koncové entity). Třetí situací jsou klíče určené pro dohodu na klíč (key agreement keys) – zde lze použít libovolnou z technik výše popsaných pro šifrovací klíče. Cílem je ustavení sdíleného tajného klíče, tímto způsobem je pak prokázáno, že koncová entita provedla důkaz vlastnictví soukromého klíče (POP). Možnou alternativou je i využívání MAC (Message Authentication Code).

Samotná žádost o certifikát obsahuje identifikátor žádosti, šablonu obsahu certifikátu a nepovinně kontrolní informace. ASN syntaxe je následující:

```
CertRequest ::= SEQUENCE {
   certReqId     INTEGER,        -- ID for matching request and reply
   certTemplate  CertTemplate, --Selected fields of cert to be issued
   controls      Controls OPTIONAL } -- Attributes affecting issuance

CertTemplate ::= SEQUENCE {
   version      [0] Version               OPTIONAL,
   serialNumber [1] INTEGER               OPTIONAL,
   signingAlg   [2] AlgorithmIdentifier   OPTIONAL,
   issuer       [3] Name                  OPTIONAL,
   validity     [4] OptionalValidity      OPTIONAL,
   subject      [5] Name                  OPTIONAL,
   publicKey    [6] SubjectPublicKeyInfo  OPTIONAL,
   issuerUID    [7] UniqueIdentifier      OPTIONAL,
   subjectUID   [8] UniqueIdentifier      OPTIONAL,
   extensions   [9] Extensions            OPTIONAL }

OptionalValidity ::= SEQUENCE {
   notBefore  [0] Time OPTIONAL,
   notAfter   [1] Time OPTIONAL } --at least one must be present

Time ::= CHOICE {
   utcTime        UTCTime,
   generalTime    GeneralizedTime }
```

Vzhledem k postupů při procesování žádosti o certifikát mohou být v žádosti obsaženy pole obsahující jednu či více hodnot, které slouží pro kontrolní mechanizmy. V materiálu [6] jsou definovány následující kontroly:

regToken; authenticator; pkiPublicationInfo; pkiArchiveOptions; oldCertID; protocolEncrKey.

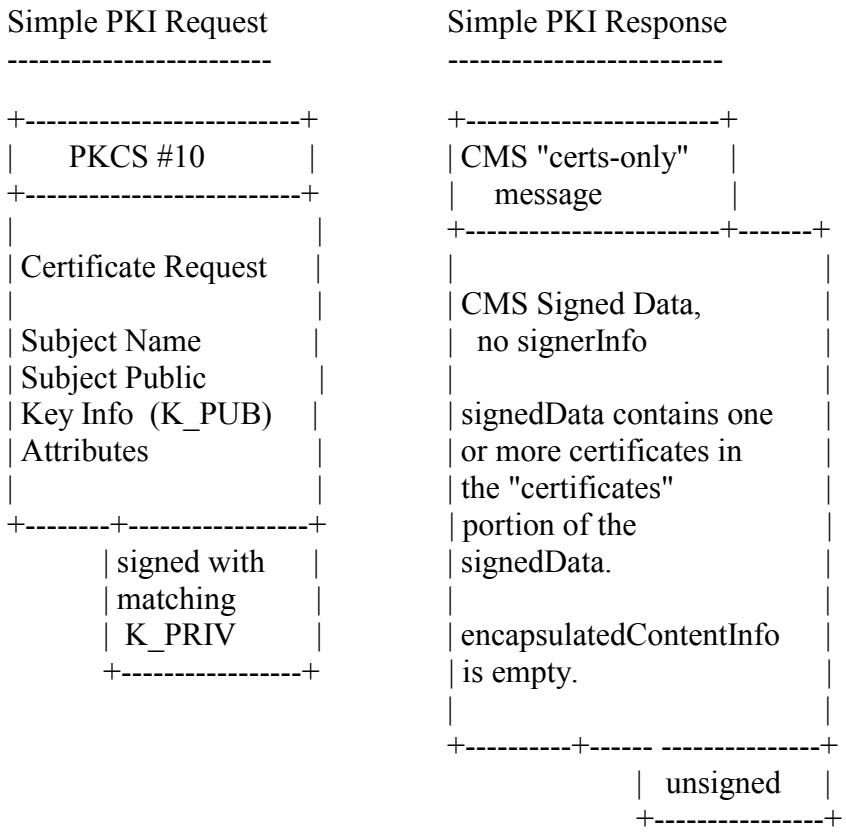
3. Protokol CMC

Popis protokolu pro řízení práce s certifikáty, který se opírá o využití CMS (Cryptographic Message Syntax) obsahuje rfc2797 (lit. [3]) . Tento protokol vznikl na základě potřeby vytvořit jakýsi interface mezi certifikáty veřejných klíčů a službami, které jsou založeny na CMS a PKCS10. Rovněž tak bylo třeba řešit potřebu protokolu pro práci s certifikáty, které jsou podepsány DSA klíčem a obsahují veřejné klíč pro Diffie-Hellmanovu dohodu na klíči.

Specifikace podporuje dva různé typy žádostí a rovněž tak dva různé typy odpovědí.

Těmito dvěma typy žádostí jsou:
- žádost využívající čistě PKCS 10;
- žádost, která je zprávou ve smyslu PKCS10 či CRMF a je zabalena v obálce CMS jako část objektu PKIData.

Odpovědi používají CMS objekt signedData a mohou být:
- buď degenerovaným CMS objektem signedData (pokud nejsou požadovány další služby);
- nebo objektem ResponseBody, který je zabalen v CMS objektu signedData.



Obrázek dokumentuje průběh protokolu (v té jednodušší situaci).

K obrázku:

Nejjednodušší cestou pro přihlášení žádosti je obyčejná zpráva dle PKCS10. Pokud je přihlašován požadavek vztahující se k podpisovému klíči, musí být příslušné PKCS10 podepsáno tímto klíčem (pro DH klíče je využíván POP mechanismus popsaný v [7]). Tento postup musí být podporován na serverech a obdobně musí zde být podporováno i vytváření odpovědí.

Tyto zprávy, které se týkají práce PKI mohou být v případě potřeby zašifrovány. součástí zpráv (žádostí i odpovědí) mohou být různé kontrolní atributy.

Jsou používány tři různé způsoby zabalení (wrapping) zpráv pro přenos:

- MIME (hlavně pro http a elektronickou poštu);
- ve formě binárního souboru (stále jsou často používány obyčejné diskety);
- objekt zakódovaný dle BER (tzv. socket based transport) pro přímou cestu.

.

Materiál [5] definuje řadu transportních metod pro přenos zpráv CMC (http, file, mail a TCP).

4. Literatura

[1] Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510)

[2] Internet X.509 Certificate Request Message Format (RFC 2511)

[3] Certificate Management Messages over CMS (RFC 2797)

[4] Internet X.509 Public Key Infrastructure Certificate Management Protocols

[5] Transport Protocols for CMP

[6] Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)

[7] Diffie-Hellman Proof-of-Possession Algorithms (RFC 2875)

C. Bezpečnost informačního systému pro certifikační služby (ISCS) a objektová bezpečnost

Mgr. Pavel Vondruška, GCUCMP

1. Úvod do problematiky

Tuto problematiku obecně řeší prováděcí vyhláška ÚOOÚ k elektronickému podpisu (Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu) v § 4, odst.4.

Příslušná citace z této vyhlášky :
(4) Prostory, kde dochází k činnosti podle odstavců 1 až 3 (§ 4) a podle § 5 odst. 1, musí být zabezpečeny obdobně jako objekty kategorie „D“ podle zvláštního právního předpisu.

Tímto zvláštním předpisem je vyhláška NBÚ (Národní bezpečnostní úřad) - Vyhláška č. 339/1999 Sb., o objektové bezpečnosti.

Nejprve se seznámíme s obsahem zde citovaných odstavců :

§ 4

(1) Používaný informační systém pro certifikační služby se považuje za bezpečný, pokud u dat, která zpracovává, je zajištěna důvěrnost, integrita, dostupnost a prokazatelnost jejich původu a pokud odpovídá požadavkům technické normy upravující oblast informační bezpečnosti.

(Příslušná technická norma je : ČSN ISO/IEC 15408 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti informačních technologií,bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.)

(2) Za účelem doložení bezpečnosti postupů podle § 6 odst. 1 písm. j) zákona o elektronickém podpisu poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí zaznamenávání událostí při

a) ***vydání kvalifikovaných certifikátů,***
b) ***ukončení platnosti kvalifikovaných certifikátů,***
c) ***nakládání s daty pro vytváření elektronického podpisu a jim odpovídajícími daty pro ověřování elektronického podpisu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty (dále jen „párová data poskytovatele“), a to během jejich celého životního cyklu, a***
d) ***nakládání s kvalifikovaným certifikátem poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, a to během celého životního cyklu tohoto certifikátu.***

(3) Záznamy o událostech podle odstavce 2 musí být pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, dostupnosti, integrity, časové autentičnosti a důvěrnosti těchto záznamů.

§ 5

Bezpečnost postupu při nakládání s párovými daty poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty

(1) Při vytváření, používání a uchovávání párových dat poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty musí být jakákoliv manipulace s těmito daty prováděna

a) ***výhradně fyzickými osobami, které jsou pro tuto činnost určeny poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty,***
b) ***podle postupů stanovených certifikační prováděcí směrnicí a***
c) ***v souladu se systémovou bezpečnostní politikou.***

2. Komentář a výklad

V prováděcí vyhlášce ÚOOÚ k elektronickému podpisu č.366/2001 Sb. se odkazuje na zvláštní právní předpis, který upravuje objektovou bezpečnost (Vyhláška č. 339/1999 Sb). Vyhláška využívá z tohoto předpisu požadavky pouze na jednu kategorii, a to kategorii „D“, neboť požadavky na zabezpečení prostor poskytovatele, ve kterých bude docházet k činnosti podle § 4 odst. 1 až 3 a § 5 odst. 1, jsou z hlediska zabezpečení objektu obdobné. Vytvářet novou právní úpravu v případě, kdy lze využít již existující a vyhovující právní úpravu, by bylo nadbytečné. Technické prostředky obsahující obdobné požadavky, které stanoví vyhláška č. 339/1999 Sb., o objektové bezpečnosti, jsou prostředky volně dostupnými na trhu. Jejich předností je, že již jsou certifikovány jako způsobilé pro navrženou kategorii.

Technické předpisy upravující oblast informační bezpečnosti stanoví obecné požadavky na bezpečnost; požadavky na zabezpečení prostorů stanovené v těchto technických předpisech jsou obdobné jako požadavky na zabezpečení objektů kategorie „D“ stanovené vyhláškou č. 339/1999 Sb., o objektové bezpečnosti.

Začlenění prostorů poskytovatele, ve kterých se budou provádět tzv. „choulostivé operace“, do kategorie „D“, bylo určeno na základě obdobných požadavků pro tuto činnost. Konkrétně stanovená opatření ochrany prostoru z hlediska
a) fyzické ostrahy objektu,
b) požadovaných technických prostředků, a
c) režimových opatření
jsou vhodná i pro prostory, ve kterých se budou provádět tzv. „choulostivé operace“

Požadavky na kategorii „V“ lze vzhledem k určenému účelu považovat za příliš „slabé“ (například u objektů kategorie "V" se fyzická ostraha objektu zajišťuje pouze v pracovní době). Požadavky na kategorii „T“ jsou nadbytečně přísné a neodpovídají stanovenému účelu.

Pokud jde o vymezení příslušného prostoru, vždy se bude jednat o prostory, ve kterých bude poskytovatel provozovat informační systém pro certifikační služby. Oddělení prostorů, ve kterých bude docházet k činnosti podle § 4 odst. 1 až 3 a podle § 5 odst. 1 od ostatních prostorů (tzv.„demilitarizované zóny“) popíše poskytovatel certifikačních služeb v systémové bezpečnostní politice. Obecně platí, že v odděleném prostoru se zpracovávají všechny z hlediska bezpečnosti důležité informace. Zejména se v odděleném prostoru bude uskutečňovat **vytváření a podepisování kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů,** které mají být zneplatněny, **správa databáze informací o klientech a správa databáze všech vydaných kvalifikovaných certifikátů**. Tato databáze se může replikovat do tzv. „demilitarizované zóny“ pro usnadnění přístupu například k informacím o statutu certifikátu pomocí protokolu OCSP.

3. Doporučený postup

Poskytovatel certifikačních služeb popíše v příslušné povinné a doporučené dokumentaci svého ISCS (informačního systému pro certifikační služby) zabezpečení objektové bezpečnosti. V jednotlivých dokumentech jsou samozřejmě popsány různé aspekty tohoto zabezpečení a různý rozsah a detaily a to především podle typu příslušné dokumentace. Důležité je, aby poskytovatel přesně vymezil v těchto dokumentech svůj ISCS a vymezil prostory, kde se provozují činnosti, které mají být podle vyhlášky ÚOOÚ č.366/2001 Sb. zabezpečeny obdobně jako objekty kategorie „D" podle vyhlášky NBÚ č. 339/1999 Sb., o objektové bezpečnosti. Pro účely zabezpečení těchto prostor poskytovatele se, v souladu s Vyhláškou NBÚ**, vytváří zabezpečená oblast kategorie „D", třídy II.**

Obecně poskytovatel certifikačních služeb zpracovává následující dokumentaci:

***Doporučené dokumenty* :**

- **bezpečnostní projekt ochrany objektu**, který obsahuje umístění zabezpečených oblastí v objektu a způsob použití bezpečnostních opatření při vnější a vnitřní ochraně objektu,
- **technická dokumentace objektové bezpečnosti,** která obsahuje technické údaje, pokyny a pravidla pro používání technických prostředků, schéma jejich rozmístění v objektu,
- **provozní řád PCS**, který stanovuje zejména režim pohybu osob a dopravních prostředků v objektu, režim pohybu citlivých aktiv v objektu, režim manipulace s klíči a pravidla pro výkon fyzické ostrahy objektu,
- **směrnice a metodické pokyny**, popisují např. další požadavky na osoby poskytovatele, dále způsob auditu, kontroly chování zaměstnanců PCS, dozor nad chováním zaměstnanců poskytovatele apod. V metodických pokynech může být např. rozbor bezpečnostního incidentu, který se stal a výklad správného a závazného chování osob v jednotlivých rolích zaměstnavatele, tak jak je upraven v předpisové základně poskytovatele.

Povinné dokumenty (předkládají se při žádosti o akreditaci):

- **certifikační prováděcí směrnice**, ve které jsou uvedeny chráněné informace o postupech při zajišťování služeb spojených s elektronickými podpisy,
- **celková bezpečnostní politika**, ve které je konkrétně popsán způsob zajištění celkové bezpečnosti PCS,
- **systémová bezpečnostní politika**, ve které je konkrétně popsán způsob zajištění bezpečnosti ISCS (způsoby ochrany dat, popis bezpečnostních opatření, vyhodnocení analýzy rizik, …),
- **plán pro zvládání krizových situací**, ve kterém jsou stanoveny postupy (včetně krizového plánu ochrany objektu), které jsou uplatněny v případě mimořádné události,
- **plán obnovy**, ve kterém jsou stanoveny postupy pro obnovu řádné funkce ISCS.

Údaje uvedené v doporučených dokumentech není třeba v povinných dokumentech „opakovat". Doporučuje se na doporučené dokumenty pouze odvolávat.

Dokumentace objektové bezpečnosti je uložena u statutárního orgánu PCS nebo jím pověřené osoby. Statutární orgán odpovídá za shodu dokumentace se skutečným stavem bezpečnostních opatření odpovídajících vyhodnoceným rizikům.

Kontrola shody skutečného stavu s dokumentací se provádí nejméně každých 12 měsíců. Při realizaci objektové bezpečnosti musí být dodržena zásada, že počet osob, které jsou určovány k seznamování s informacemi o technických prostředcích a bezpečnostních

opatřeních k ochraně objektů, se musí omezit pouze na osoby, které se na procesu realizace objektové bezpečnosti nezbytně podílejí.

.

4. Ochrana objektu

Ochrana objektu se zabezpečuje kombinací bezpečnostních opatření, kterými jsou:

a) fyzická ostraha objektu,
b) technické prostředky,
c) režimová opatření.

Fyzická ostraha objektu

U objektů kategorie „D“ se zajišťuje nepřetržitě. Fyzickou ostrahu objektu zajišťuje na stanovišti určeném pro stálý výkon ostrahy objektu nejméně 1 pracovník fyzické ostrahy objektu. Stanoviště určené pro stálý výkon fyzické ostrahy objektu může být umístěno mimo tento objekt za předpokladu, že kombinace bezpečnostních opatření (fyzická ostraha objektu, technické prostředky, režimová opatření) umožní náležitě rychlý zásah. Na stanoviště určené pro stálý výkon fyzické ostrahy objektu musí být vyveden výstup hlášení od zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocování neoprávněného vstupu. K fyzické ostraze objektu lze využít i strážní službu. Strážní služba je určena mimo jiné jako odstrašující prostředek pro osoby, které by mohly plánovat porušení používaných bezpečnostních opatřen. Povinnosti osob, které strážní službu vykonávají, stejně jako intervaly obchůzek se stanovují vzhledem k míře rizika a k ostatním použitým bezpečnostním systémům. Pravidla pro výkon strážní služby je nutno stanovit písemnou formou.

Technické prostředky k zabezpečení objektů kategorie „D“:
K ochraně hranic objektů kategorie „D“ se používají:

- mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla,
- zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocování neoprávněného vstupu.

K ochraně zabezpečené oblasti kategorie „D“ se používají:

- mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla,
- zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocování neoprávněného vstupu,
- zařízení fyzického ničení nosičů informací.

K ochraně zabezpečené oblasti kategorie „D“, **v nichž je zajištěna trvalá přítomnost** zde pracujících osob, se používají:

- mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla,
- tísňové systémy, zejména tísňové hlásiče, které fungují jako součást elektrické zabezpečovací signalizace.

Režimová opatření

Režimová opatření musí být konkrétně stanovena v dokumentaci poskytovatele certifikačních služeb.

Režimovými opatřeními jsou:

-režim vstupu a výstupu osob, který stanoví:

a) oprávnění osob pro vstup do objektu, výstup z objektu a způsob kontroly;

b) podmínky a způsob kontroly vynášení citlivých aktiv z objektu;

- definování bezpečnostních opatření a specifikace citlivých aktiv a všech chráněných skutečností, které podléhají bezpečnostní manipulaci v zabezpečené oblasti kategorie „D“.

Rozsah, způsob a podmínky použití bezpečnostních opatření se určují na základě vyhodnocení rizik;

-režim pohybu osob a zabezpečení citlivých aktiv v objektu a v zabezpečených oblastech v pracovní a mimopracovní době;

-režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů (zejména se určuje systém a způsob označování, přidělování a odevzdávání klíčů, jejich úschovy a evidence, uložení duplikátů a způsob jejich použití);

-režim manipulace s technickými prostředky a jejich používání.

Zacházení s klíči od úschovných objektů

Nastavení kombinace u kombinačního zámku úschovného objektu se musí osoby, které je potřebují znát, naučit nazpaměť. Náhradní klíče a písemný zápis každého nastavení kombinace pro případ použití v mimořádných situacích musí být uloženy v zapečetěné neprůhledné obálce u statutárního orgánu PCS nebo jím pověřené osoby. Pracovní a náhradní klíče od úschovných objektů musí být uloženy odděleně. Zápis každé kombinace musí být uložen ve zvláštní obálce. U klíčů, zápisů nastavení kombinací a obálek musí být zajištěna dostatečná ochrana.

Znalost nastavení kombinací u kombinačních zámků úschovných objektů musí být omezena na co nejmenší počet osob. Nastavení kombinací se musí měnit v následujících případech:

- při prvním převzetí úschovného objektu do užívání,
- vždy, když dojde ke změnám v okruhu osob, kterým byla tato kombinace známa,
- vždy, když dojde k neoprávněnému nakládání s citlivými aktivy, nacházejícími se v úschovném objektu nebo existuje-li podezření, že k němu došlo,
- v intervalech nepřekračujících 12 měsíců.

Oprávnění ke vstupu do objektu

Seznam osob (oprávněné osoby) oprávněných vstupovat do stanoveného objektu a seznam dopravních prostředků oprávněných vjíždět do objektu, včetně podmínek organizačního zajištění, se stanoví v provozním řádu k zabezpečení objektové bezpečnosti v souladu s Celkovou bezpečnostní politikou a Certifikační prováděcí směrnicí PCS.

Oprávnění ke vstupu do objektu vydává statutární orgán PCS nebo jím pověřená osoba. Oprávněnost ke vstupu osob do objektu se prokazuje stanoveným způsobem popsaným ve výše uvedených dokumentech, který umožňuje jednoznačnou identifikaci osob.

V objektech kategorie „D“ je návštěvám dovolen pohyb jen v doprovodu oprávněné osoby. V uvedených dokumentech musí být stanovena opatření, která zabrání návštěvám, aby se neoprávněně seznámily s chráněnými / citlivými aktivy. Za dodržování stanovených opatření odpovídá osoba, která návštěvu doprovází.

Vstupy do objektu se v době, kdy nejsou využívány, zabezpečují kombinací bezpečnostních opatření k zabezpečení objektů kategorie „D“.

Kontrolní opatření při vstupu do objektu

Kontrolu oprávněnosti vstupu osob a vjezdu dopravních prostředků do objektu provádí fyzická ostraha nebo osoba pověřená statutárním zástupcem PCS způsobem stanoveným v v provozním řádu k zabezpečení objektové bezpečnosti v souladu s Celkovou bezpečnostní politikou a v souladu s Certifikační prováděcí směrnicí poskytovatele certifikačních služeb.

Vnější ochrana objektu

Vnější ochrana objektu je zajišťována fyzickou ostrahou objektu, technickými prostředky a režimovými opatřeními. K ochraně hranice objektu kategorie „D“ se používají technické prostředky k zabezpečení objektů kategorie „D“.

V případě, že hranice objektu je zároveň i hranicí zabezpečené oblasti, používají se technické prostředky v souladu s požadavky na zabezpečené oblasti kategorie „D“.

V pracovní době mohou být vyřazena některá bezpečnostní opatření použitá pro ochranu hranice objektu. V mimopracovní době se celá hranice objektu nepřetržitě zabezpečuje bezpečnostními opatřeními stanovenými v souladu s Celkovou bezpečnostní politikou a Certifikační prováděcí směrnicí PCS. Rozsah, způsob a podmínky použití bezpečnostních opatření se určují na základě vyhodnocení rizik a provedeného vyhodnocení stavu bezpečnostních opatření.

Vstupy do objektu kategorie „D“ se v době, kdy nejsou využívány, zabezpečují kombinací bezpečnostních opatření a technickými prostředky k zabezpečení objektů kategorie „D“.

Tam, kde to umožňuje charakter hranice objektu, jsou po celém jejím obvodu vyžadovány fyzické bariéry. Jejich efektivnost závisí na stupni úrovně zabezpečení přístupových bodů. Brány musí být konstruované ve stejném bezpečnostním provedení jako oplocení, musí být zajištěn stejný standard kontroly vstupu ve všech přístupových bodech.

Vnitřní ochrana objektu

Vnitřní ochrana objektu je zajišťována souborem bezpečnostních opatření k zajištění zabezpečené oblasti kategorie „D“.

Pro efektivní střežení hranice zabezpečené oblasti se doporučuje využívat **perimetrické bezpečnostní systémy**, k nimž se řadí perimetrické detekční systémy, bezpečnostní osvětlení, kamerové systémy. Perimetrické detekční systémy mohou být instalovány skrytě (obvykle z estetických důvodů) nebo zjevně jako odrazující prvek. Perimetrické detekční systémy jsou ze své podstaty náchylné k falešným poplachům, a proto by měly být doplněny o další kontrolní systém, jako jsou například kamerové systémy.

Zabezpečené oblasti, v nichž je zajištěna trvalá přítomnost zde pracujících osob, musí být vybaveny úschovnými objekty pouze v případě, že se v nich hromadně ukládají citlivá aktiva. Úschovný objekt musí být umístěn tak, aby byl zabezpečen trvalý přímý dohled přítomných osob.

V případě, kdy zabezpečené oblasti současně plní úlohu stanovišť určených pro stálý výkon fyzické ostrahy objektu, nemusí být vybaveny tísňovými systémy.

Vyhodnocení rizik

Základním předpokladem pro efektivní a ekonomické využití bezpečnostních opatření je vyhodnocení rizik, na jehož podkladě se stanovují příslušná opatření pro objektovou bezpečnost. Stanovuje se rozsah, způsob a podmínky použití bezpečnostních opatření.

Na základě vyhodnocení rizik se provádí:

- vyhodnocení stavu bezpečnostních opatření a posouzení, zda jejich realizace pro danou míru rizika odpovídá bezpečnostním standardům NBÚ pro zabezpečenou oblast kategorie „D“, třídy II,
- další vhodná bezpečnostní opatření, pokud bylo při vyhodnocení stavu zjištěno, že stav bezpečnostních opatření je nedostatečný,
- zjištění rizik, která přetrvávají i po aplikaci bezpečnostních opatření.

Existující stav bezpečnostních opatření se hodnotí podle „Bezpečnostních standardů objektové (fyzické) bezpečnosti“ NBÚ (Bezpečnostní standardy objektové (fyzické) bezpečnosti, zvláštní vydání Věstník NBÚ, Praha 2000) . Tento standard je předpisem doplňujícím vyhlášky NBÚ č. 339/1999 Sb. a č. 244/1998 Sb. ve znění vyhlášky č. 338/1999 Sb.

Na základě hodnocení se přijímá konkrétní způsob řešení ochrany. Je tak možné stanovit, je-li zabezpečení dané kategorie „D“ pro určenou míru rizika dostatečné a v případě, že ne, určit optimální způsob, jak zabezpečení zvýšit na požadovanou úroveň.

5. Terminologie a použité zkratky

ÚOOÚ	-	Úřad pro ochranu osobních údajů
ISCS	-	informační systém pro certifikační služby
PCS	-	poskytovatel certifikačních služeb

a) **objekt** – budova nebo jiný stavebně či jinak ohraničený prostor, ve kterém se nacházejí zabezpečené oblasti,
b) **zabezpečená oblast** - stavebně ohraničený prostor uvnitř objektu, kde se používá ISCS a bezpečnostní postupy, které tento systém podporují,
c) **hranice objektu** – plášť budovy, oplocení nebo jiné podobné ohraničení prostoru,

d) **vstup do objektu** – místo určené pro vstup a výstup osob z objektu a místo určené pro vjezd a výjezd dopravních prostředků z objektu,
e) **provozovatel objektu** – statutární orgán PCS , který v objektu vykonává činnost spojenou s povinnostmi PCS,
f) **mimořádná situace** – stav, kdy bezprostředně hrozí, že dojde k neoprávněnému nakládání s citlivými aktivy,
g) **hrozba** – možnost neoprávněného nakládání s citlivými aktivy při narušení objektové bezpečnosti,
h) **riziko** – pravděpodobnost, že se určitá hrozba uskuteční,
i) **nepovolaná osoba** – fyzická osoba, která není určena ke styku s citlivými aktivy nebo k dané oblasti činnosti,
j) **bezpečnostní incident** – narušení bezpečnosti chráněného zájmu,
k) **technický prostředek** - bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu nebo zabezpečené oblasti,
l) **informační systém pro certifikační služby** - informační systém, jehož prostřednictvím poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajišťuje služby spojené s elektronickými podpisy;
m) **perimetr** – hranice objektu nebo zabezpečené oblasti, které jsou chráněny technickými prostředky („bezpečná vzdálenost“).

6. Literatura

[1] Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu

[2] Vyhláška č. 339/1999 Sb., o objektové bezpečnosti.

[3] Bezpečnostní standardy objektové (fyzické) bezpečnosti, zvláštní vydání Věstník NBÚ, Praha 2000)

[4] Bosáková,D., Vondruška,P. : prezentace k vypořádání s připomínkami k návrhu prováděcí vyhlášky k zákonu o elektronickém podpisu, část objektová bezpečnost, 29.7.2001

[5] V.Vaněček : Objektová bezpečnost, připravovaný materiál ÚOOÚ

[6] Bosáková,D., Kučerová,A., Peca,J., Vondruška,P. : "Elektronický podpis - přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů", Nakladatelství ANAG, 2002

D. Informace - Cryptology ePrint Archive
(informaci zaslal V.Klíma)

Koncem května se na serveru Mezinárodní asociace pro kryptologický výzkum (IACR, http://www.iacr.org/) v sekci Cryptology ePrint Archive objevily dva nové články z pera českých autorů. Uvádíme zde jejich abstrakty, přičemž plná znění lze nalézt na http://eprint.iacr.org/curr/ pod čísly 061 a 071.

Strengthened Encryption in the CBC Mode

Vlastimil Klíma [1] and Tomáš Rosa [1,2]
[1] ICZ, V Olšinách 75, 100 97 Prague 10, Czech Republic, http://www.i.cz
[2] Department of Computer Science and Engineering, Faculty of Electrical Engineering,
Czech Technical University in Prague, Karlovo náměstí 13, 121 35 Prague 2, Czech Republic
{vlastimil.klima, tomas.rosa}@i.cz

Abstract. Vaudenay [1] has presented an attack on the CBC mode of block ciphers, which uses padding according to the PKCS#5 standard. One of the countermeasures, which he has assumed, consisted of the encryption of the message *M´= M || padding || hash(M || padding)* instead of the original *M*. This can increase the length of the message by several blocks compared with the present padding. Moreover, Wagner [1] showed a security weakness in this proposal. The next correction, which Vaudenay proposed ("A Fix Which May Work") has a general character and doesn't solve practical problems with the real cryptographic interfaces used in contemporary applications. In this article we propose three variants of the CBC mode. From the external point of view they behave the same as the present CBC mode with the PKCS#5 padding, but they prevent Vaudenay's attack.

Further Results and Considerations on Side Channel Attacks on RSA

Vlastimil Klíma [1] and Tomáš Rosa [1,2]
[1] ICZ, V Olšinách 75, 100 97 Prague 10, Czech Republic, http://www.i.cz
[2] Department of Computer Science and Engineering, Faculty of Electrical Engineering,
Czech Technical University in Prague, Karlovo náměstí 13, 121 35 Prague 2, Czech Republic
{vlastimil.klima, tomas.rosa}@i.cz

Abstract. This paper contains three parts. In the first part we present a new side channel attack on plaintext encrypted by EME-OAEP PKCS#1 v.2.1. In contrast with Manger´s attack, we attack that part of the plaintext, which is shielded by the OAEP method. In the second part we show that Bleichenbacher's and Manger's attack on the RSA encryption scheme PKCS#1 v.1.5 and EME-OAEP PKCS#1 v.2.1 can be converted to an attack on the RSA signature scheme with any message encoding (not only PKCS). This is a new threat for those implementations of PKI, in which the roles of signature and encryption keys are not strictly separated. This situation is often encountered in the SSL protocol used to secure access to web servers. In the third part we deploy a general idea of fault-based attacks on the RSA-KEM scheme and present two particular attacks as the examples. The result is the private key instead of the plaintext as with attacks on PKCS#1 v.1.5 and v.2.1. These attacks should highlight the fact that the RSA-KEM scheme is not an entirely universal solution to problems of RSAES-OAEP implementation and that even here the manner of implementation is significant.

E. Letem šifrovým světem

---

1. Kritika článku „Je 1024-bitová délka klíče RSA dostatečná?“ (Crypto-World 5/2002)

V pátek 14.6.2002 jsem obdržel kritiku článku Jaroslava Pinkavy, který vyšel v minulém čísle našeho e-zinu. Kritiku v podobě samostatného článku připravil pro toto dnešní číslo RNDr. Vlastimil Klíma. Vzhledem k tomu, že danému tématu již byla věnována dostatečná pozornost a vzhledem k tomu, že způsob kritiky v tomto článku je podle mne příliš osobní ("…čtenáře pěkně vodit za nos a ještě vytvářet dojem uvážlivého člověka..", "..je to zahaleno do líbivé slovní roušky…"), rozhodl jsem se tento příspěvek nezveřejnit. Z mého pohledu zvolená dikce článku do seriózního e-zinu (a Crypto-World se snažím takto směrovat) nepatří. Současně nechci potlačit jakoukoliv kritiku článků, které vyšly v Crypto-Worldu a po dohodě s autorem uveřejňuji informaci, že

- takovouto kritiku napsal
- se s ní může čtenář seznámit na www.hyperlink.cz/cryptography/kritika2.pdf (V.Klíma : „O RSA, rozumné dostatečnosti a dostatečné rozumnosti“)

Kontrolní součet : 'KRITIKA2.PDF' 125 635 byte:
MD5: 4401 63D3 A079 5E21 5132 B9F7 2D99 677F
SHA-1: 373D 0997 253F DEE2 C3A8 67E8 9A54 A124 EBAA 3443

Související články:
J. Pinkava : Bezpečnost RSA – význačný posun?, Crypto-World 3/2002
V.Klíma : Kritika článku "Bezpečnost RSA - význačný posun?, Crypto-World 4/2002
J. Pinkava : Je 1024-bitová délka klíče RSA dostatečná?, Crypto-World 5/2002

---

2. Zákon o elektronickém podpisu novelizován !!! - Zákon č. 226/2002 Sb.

Jak jsem již rozesílal ve speciální informaci, pod číslem zákona č. 226/2002 Sb. vyšla novela současného zákona o EP. Pokud jde o další uvádění názvu zákona, musí být nyní za dosavadním názvem zákona o elektronickém podpisu citována i tato novela.

Oficiální název je potřeba uvádět v následujícím tvaru:
Zákon c.227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 226/2002 Sb.

Celý název nově vyhlášeného zákona:
Zákon č.226/2002 Sb. ze dne 9.5.2002, kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů, a zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

Účinnost nastává dnem 1. července 2002.
Zveřejněn ve Sbírce zákonů částka 87, strana 5034-5036.

První část tohoto zákona je věnována změně trestního řádu, následuje změna občanského soudního řádu, změna zákona o správě daní a poplatků a změna správního řádu. Pátá část je věnována změně zákona o elektronickém podpisu. Změna se týká pouze úpravy paragrafu 11 zákona č.227/2000 Sb. Tuto změnu uvádíme v úplném znění.

ČÁST PÁTÁ

Změna zákona o elektronickém podpisu

Čl. V

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), se mění takto:

V § 11 se na konci odstavce doplňují tyto věty: „To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je zaručený elektronický podpis založený na kvalifikovaném certifikátu užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná.“.

---

3. Hackeři pomozte !

(Norway Post) Norské muzeum vyzývá hackery, aby mu pomohli rozluštit heslo jeho elektronického archívu. Pracovník, který vytvořil archív více jak 1500 knih a dokumentů, totiž zemřel, aniž komukoli heslo sdělil.

---

4. O čem jsme psali v červnu roku 2000 a 2001

Crypto-World 6/2000

Příloha : Navajo Code Talkers , revize z 15.6.1945, soubor Dictionary.htm

Crypto-World 6/2001

Příloha : priloha6.zip
(fotografie Security 2001, témata přednášek na konferenci Eurocrypt´2001)

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "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

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 k otištění** , informace
pavel.vondruska@uoou.cz (**vondruskap@uoou.cz**)
pavel.vondruska@post.cz
vondruska.p@seznam.cz