Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 8, číslo 10/2006 **15. říjen 2006**

10/2006

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1189 registrovaných odběratelů)

Obsah :

Příloha :
doprovodné materiály k Soutěži v luštění 2006 - vystava.pdf , epilog.pdf

A. Soutěž v luštění 2006 - průběh

Mgr. Pavel Vondruška, (pavel.vondruska@crypto-world.info)

Soutěž v luštění jednoduchých šifrových úloh, kterou tradičně na podzim pořádá náš e-zin, začala přesně před měsícem (15. 9. 2006). V době uzávěrky tohoto čísla již tři řešitelé vyřešili všechny úlohy. Blahopřejeme !

Soutěž bude ukončena počátkem listopadu, kdy vyjde kniha **Kryptologie, šifrování a tajná písma** v nakladatelství Albatros (http://crypto-world.info/oko/), neboť v šesté kapitole této knihy jsou uvedeny otevřené texty prvých třiceti úloh a to včetně stručného návodu na řešení. Přesné datum ukončení soutěže bude den, kdy kniha bude dána do prodeje. Termín bude oznámen v Crypto-NEWS na naší webové stránce. Tento den také bude uzavřena možnost vkládat řešení úloh a ze všech soutěžících, kteří dosáhnou stanovený limit 15-ti bodů budou vylosování tři řešitelé, kterým budou předány ceny od sponzorů soutěže (více viz http://soutez2006.crypto-world.info/index.php?crypto=ceny). Tento limit doposud splnilo 65 soutěžících.

Do soutěže se do jejího ukončení lze stále registrovat (kód máte uveden v e-mailu s kódy pro stažení e-zinu Crypto-World 9/2006 a 10/2006).

Vy, kteří ještě hledáte otevřené texty složitějších úloh, nezapomeňte využít nápověd, které byly postupně zveřejňovány buď v podobě chameleonů v oknu úlohy 31 nebo v Crypto-News. Abyste je nemuseli složitě dohledávat, máte tyto nápovědy uvedeny v příloze k tomuto e-zinu a to včetně popisu závěrečné úlohy 31.

Otevřené texty všech úloh a popis použitých systémů bude uveden v čísle 12/2006, které se bude soutěží zabývat.

Přeji pěknou zábavu a hodně dobrých nápadů.

Pro zájemce uvádíme statistiky jednotlivých ročníků soutěže od roku 2003.
Můžete porovnat jednotlivé položky nebo jen zavzpomínat na své umístění…

2006 (stav k 14.10, 00:10)

Celkem soutěžících:	106
všechny úlohy vyřešilo řešitelů:	3
Počet soutěžících zařazených do slosování:	65
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	96
Celkem publikovaných úloh:	31
Maximální počet bodů za publikované úlohy:	80
Počet bodů potřebných k zařazení do losování o ceny:	15

Pořadí na prvních 5-ti místech:

1 room132	80 23.09 (14:16)
2 peta007	80 24.09 (20:10)
3 MD5Mir	80 29.09 (10:14)
4 stanislaw	74 26.09 (01:32)
5 tvrz	67 23.09 (19:43)

2005

Celkem soutěžících:	153
všechny úlohy vyřešilo řešitelů:	8
Počet soutěžících zařazených do slosování:	51
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	137
Celkem publikovaných úloh:	26
Maximální počet bodů za publikované úlohy:	75
Počet bodů potřebných k zařazení do losování o ceny:	15

Pořadí na prvních 5-ti místech:

1 misof	75 02.11 (09:01)
2 pierre	75 02.11 (17:12)
3 alchymista	75 02.11 (17:46)
4 room132	75 03.11 (08:42)
5 Stanislaw	75 03.11 (20:28)

2004

Celkem soutěžících:	100
všechny úlohy vyřešilo řešitelů:	8
Počet soutěžících zařazených do slosování:	45
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	84
Celkem publikovaných úloh:	19
Maximální počet bodů za publikované úlohy:	50
Počet bodů potřebných k zařazení do losování o ceny:	15

Pořadí na prvních 5-ti místech:

1 misof	50 14.11 (16:57)
2 brubaker	50 14.11 (18:53) !
3 elpepe	50 14.11 (18:54) !
4 Dave	50 14.11 (19:03)
5 Stanislaw	50 17.11 (23:53)

2003

Celkem soutěžících:	107
všechny úlohy vyřešilo řešitelů:	11
Počet soutěžících zařazených do slosování:	32
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	53
Celkem publikovaných úloh:	19
Maximální počet bodů za publikované úlohy:	50
Počet bodů potřebných k zařazení do losování o ceny:	3

Pořadí na prvních 5-ti místech:

1 CyberMage	9
2 peta007	9
3 xnovakv	9
4 rkb	9
5 tnt	9

B. Elektronické cestovní doklady, část 1

Ing. Luděk Rašek, Logica CMG, (ludek.rasek@logicacmg.com)

V reakci na rostoucí požadavky na identifikaci osob cestujících po světě a zejména z důvodu, že tato opatření požadují Spojené státy americké pro zachování bezvízového styku, rozhodly orgány Evropské unie o vydávání pasů s biometrickými údaji držitele pasu [EU Bio]. Toto rozhodnutí se netýká Velké Británie a Irska, není závazné pro Dánsko. Naopak se vztahuje i na Island, Norsko a Švýcarsko, což je dáno dohodami těchto zemí o uplatňování a rozvoji schengenského acquis.

Samotná specifikace cestovních dokladů však neleží na bedrech EU, tou se zabývá organizace pro civilní letectví (ICAO) – mezinárodní organizace přidružená k OSN. Hlavním cílem ICAO je sice napomáhat v oblasti regulace mezinárodního civilního letectví, ale pomocí svých standardů mj. definuje i technologické vlastnosti cestovních dokladů.

1. Elektronické cestovní doklady

1.1 Česká legislativa

Do české legislativy zákon o cestovních dokladech ve znění pozdějších zákonů [329/1999 Sb.] zavádí pojem "cestovní doklad s biometrickými prvky". Tyto zákonné úpravy byly zavedeny z důvodu harmonizace českého práva s právem EU (viz [EU Bio] a [EU Bio Tech]).

V České republice platí, že od 1.9.2006 budou vydávány nové druhy dokladů již s čipem jako nosičem biometrických údajů. V České republice se vydávají následující druhy cestovních dokladů:

- cestovní doklad občana české republiky - vydávány obcemi s rozšířenou působností
  - pro občany 5 až 15 let věku jsou vydávány doklady s platností 5 let
  - pro občany starší 15 let jsou vydávány doklady s platností 10 let
- uprchlické pasy - jsou vydávány cizineckou a pohraniční policií osobám, které v ČR získali statut uprchlíka
- cizinecké pasy - jsou vydávány cizineckou a pohraniční policií osobám, které mají v ČR povolení k trvalému pobytu a doloží, že si nemohou pořídit pas dle svého občanství nezávisle na své vůli
- diplomatické pasy - jsou vydávány Ministerstvem zahraničních věcí (dále MZV) představitelům českého státu (prezident, člen vlády, poslanec, senátor, soudce Ústavního soudu, předseda Nejvyššího soudu, předseda Nejvyššího správního soudu, prezident Nejvyššího kontrolního úřadu, diplomat, manžel/manželka dříve uvedených a další dle rozhodnutí MZV)
- služební pasy - jsou vydávány MZV osobám vyjmenovaným v zákoně, které cestují do zahraničí ve věcech České republiky a to na dobu pobytu v zahraničí

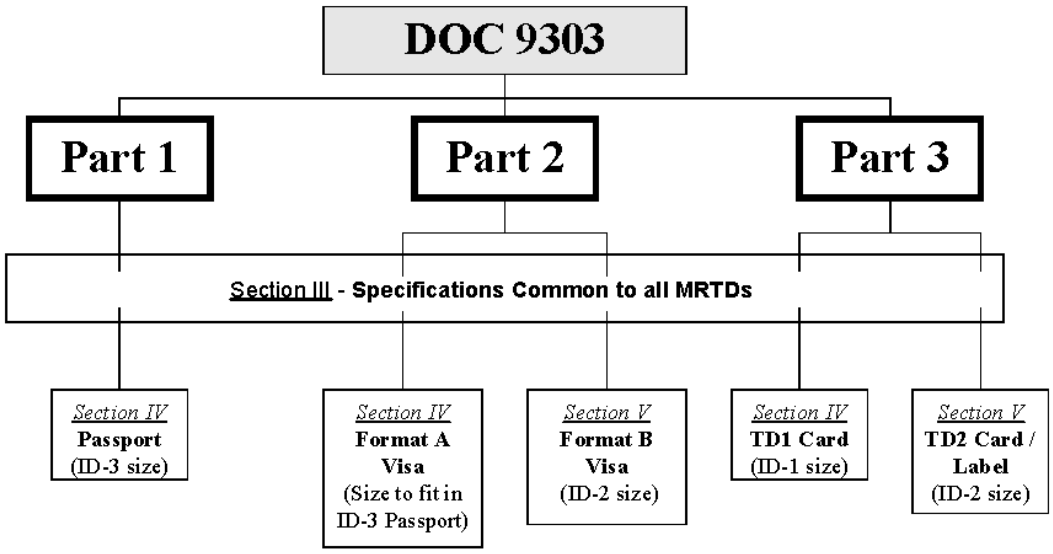
Pro úplnost je třeba dodat, že i nadále budou vydávány cestovní doklady bez biometrických údajů v případě rychlého vydání pasu (tzv. blesk) a pro děti mladší 5 let.

Vydávání cestovních dokladů se řídí zejména následujícími zákony a vyhláškami: 325/1999 Sb. a 326/1999 Sb. a 329/1999 Sb. a 642/2004 Sb.

1.2 ICAO

Mezinárodní organizace pro civilní letectví je organizací při OSN, která koordinuje způsob, jakým je provozována civilní letecká doprava na světě. Jedna z částí této organizace je vyčleněna pro definování jednotných vzorů pro doklady prokazující totožnost osob. V celé řadě specifikací vydávaných touto skupinou v rámci ICAO byly postupně definovány vlastnosti cestovních pasů a identifikačních karet (rozměry, obsah, formát strojově čitelné zóny apod.). V současné době se skupina zabývá také specifikací požadavků na cestovní pasy nesoucí biometrické údaje. Pokud je to možné, nejsou touto skupinou vytvářeny zcela nové technologické specifikace, ale jsou využívány již existující zdroje a specifikace, které prošly některým z mezinárodních normalizačních úřadů (nejčastěji ISO). Jen tam, kde existující normy nestačí, jsou navržena nová řešení (struktury dat s využitím ASN.1 apod.).

Jako nosič biometrických údajů v cestovním pasu byl zvolen bezkontaktní čip odpovídající specifikacím ISO 7816 a ISO 14443. Některé dokumenty jsou publikovány na stránkách ICAO. V některých případech je odkazováno na dokument Doc9303, což je sada předpisů a specifikací popisujících veškeré vlastnosti ID dokladů (vč. cestovních pasů). Sada Doc9303 je dostupná jako placená dokumentace.



Obr. 1 Struktura dokumentů ICAO Doc9303 od cestovních dokladech

2. Využité technologie

2.1. Pasová knížka

Pasová knížka pro e-pasy je tvořena stejně jako pasová knížka dosud používaných pasů (tedy pasů se strojově čitelnou zónou - MRZ) ve formátu ID3 (ISO 7810) o velikosti 125 × 88 mm (B7).

Ve světě je používáno několik různých konstrukcí pasů s biometrickým údaji. Konstrukcí pasu rozumíme umístění bezkontaktního čipu v pasové knížce. Bezkontaktní čip vyžaduje

speciální konstrukci některé ze stran pasu, která musí zakrýt a ochránit anténu, s jejímž využitím pas komunikuje. Používány jsou zejména následující konstrukce:

- čip v deskách pasu
- čip ve speciální papírové stránce uvnitř pasu
- čip v polykarbonátové stránce, na které je rovněž vytištěna datová stránka (osobní údaje, fotografie, MRZ)

Způsob vložení čipu do pasové knížky je jedním z důležitých ochranných prvků pasu, protože by měl znemožnit např. výměnu čipu mezi pasy nebo alespoň usnadnit detekci takovéhoto pokusu.

V českých pasech je využito technologie polykarbonátové stránky obsahující čip s laserovou personalizací osobních údajů do vnitřní světlocitlivé vrstvy s celou řadou dalších dodatečných ochranných prvků vytvořených s využitím technologií ceninového tisku a dalších moderních technologií.

2.2. Datová stránka a MRZ

V pasu je umístěna tzv. datová strana, na které jsou vytištěny veškeré základní údaje o držiteli pasu, včetně jeho fotografie a volitelně vzoru rukou psaného podpisu.

Obr. 2 Příklad kompletní datové stránky

Údaje na datové stránce jsou definovány v Doc9303. Je přesně specifikováno pořadí a význam jednotlivých prvků na stránce. Ve spodní části strany je vytištěna strojově čitelná zóna vhodná pro snímání pomocí OCR.

Jednotlivé položky uvedené v MRZ jsou povinné, mají různou délku a definovaný formát. V následující tabulce jsou uvedeny

Tabulka 1. Příklad výpočtu MRZ

Číslo položky	Význam	Hodnota z příkladu
01	typ dokumentu	P<
02	vydavatelský stát	CZE (Česká republika)
03	jméno držitele	EMILIE NOVAKOVA (Emílie Nováková)
04	číslo pasu - 9 nejvýznamnějších číslic; pokud je číslo pasu delší, než 9 číslic, je zbytek čísla pasu uložen v datové položce č. 12, kratší číslo je doplněno <	0000000017< (00000017)
05	kontrolní číslice k číslu dokladu; pokud je číslo dokladu delší než 9 číslic, bude zde výplňový znak < a kontrolní číslice bude v datové položce č. 12	8
06	občanství	CZE (Česká republika)
07	datum narození	680512 (12.5.1968)
08	kontrolní číslice data narození	6
09	pohlaví	F (žena)
10	datum platnosti	160613 (13.06.2016)
11	kontrolní číslice data platnosti	3
12	volitelné pole - pokud je číslo pasu delší než 9 číslic, jsou zde uvedeny nejméně významné číslice čísla pasu a kontrolní číslice čísla pasu oddělená výplňovým znakem <	6855121515<<<<
13	kontrolní číslice pole 12	9
14	celková kontrolní číslice (viz níže)	4

Strojově čitelná zóna je umístěna relativně k levému dolnímu rohu datové strany dokladu. Zóna je vytištěna fontem OCR-B o velikosti Size1 (cca 14 bodů). Více informací o fontu lze nalézt ve specifikaci [ISO 1073-2:1976].

MRZ na pasu se skládá ze dvou řádků po 44 znacích. Neobsahuje mezery, jsou nahrazeny tzv. výplňovým znakem (filler character) '<'. Pokud je potřeba, jsou položky doplněny znakem '<' do požadované délky. MRZ obsahuje pouze ASCII znaky a je definován způsob transkripce znaků v ASCII nepřítomných (např. Ä -> AE). Dle následujícího schématu popíšeme kódování:

Ptiiinnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn
#########CbbbYYMMDDCsyymmddCpppppppppppppppCX

- P - pro pasy je vyhrazeno písmeno P
- t - typ pasu přiřazený vydavatelem o délce jednoho znaku – např.: S - služební, D - diplomatický apod.; pro běžný pas nebo pokud není využito nahrazuje se '<'
- iii - kód země vydávající pas - pro ČR je to CZE (kódy vycházející z tabulky ISO 3166 3-písmenných kódů zemí rozšířené např. o příznak uprchlíka bez příslušnosti: XXA a další z Doc9303)
- nnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnnn - jméno držitele v pořadí - příjmení << jméno<další<jména - vše velkými písmeny, doplněné zprava '<' do délky 39 znaků; pokud jméno obsahuje doplňky typu Jr, II apod., kódují se do příjmení a oddělují se '<'
- ######### - číslo pasu, pokud číslo pasu obsahuje jiné znaky než číslice a písmena, jsou nahrazeny '<'
- C - kontrolní číslice, nebo '<' pokud je číslo pasu delší než 9 číslic, zbytek čísla je pak v poli pppppppppppppp
- bbb - státní příslušnost - pro ČR - CZE
- YYMMDD - datum narození
- s - pohlaví
- yymmdd - datum ukončení platnosti pasu
- C - kontrolní číslice data ukončení platnosti pasu
- pppppppppppppp - pomocné pole složené zbytku čísla pasu, kontrolní číslice tohoto čísla a ukončeného '<' zbytek do délky 14 znaků je možno vyplnit čímkoli; je zde např. rodné číslo
- C - kontrolní číslo z pppppppppppppp
- X - složená kontrolní číslice vypočtená ze znaků: 1-10, 14-20, 22-43 druhé řádky MRZ

Nástroj pro generování MRZ pro pas lze též najít na [MRZ Calc].

2.2.1. Postup výpočtu kontrolní číslice

Každý znak se nahradí číselnou hodnotou - číslice mají svou hodnotu, písmena se převedou dle následující tabulky (která mimochodem obsahuje výčet povolených znaků MRZ)

Tabulka 2. Tabulka pro výpočet kontrolní číslice

<	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

MRZ se tedy převede na řadu číslic a poté vypočteme vážený součet této řady. Váhy, které se používají, se cyklicky berou z této řady (7,3,1,7,3,1,7,3,1 atd.).

Vypočtený součet vydělíme 10 a zbytek po tomto dělení je kontrolní číslice. V následující tabulce je uveden krátký příklad

Vstup	1	6	0	9	0	5	-	
Hodnota	1	6	0	9	0	5	-	
	*	*	*	*	*	*	-	
Váha	7	3	1	7	3	1	-	
	7 +	18 +	0 +	63 +	0 +	5 =	93 % 10 =	3

Tabulka 3. Příklad výpočtu kontrolního čísla (viz výše uvedený příklad MRZ)

2.2. RFID

Pracovní skupina pro cestovní doklady nové generace (NTWG) rozhodla, že nosičem biometrických údajů bude čip a jeho rozhraní bude bezdrátové radiové. Vybrána byla existující specifikace bezkontaktního rozhraní ISO/IEC 14443 (vycházející z průmyslového standardu MIFARE). Samotný čip pak musí vyhovovat specifikacím pro čipové karty z řady ISO/IEC 7816 s využitím komunikačního protokolu T=CL (contactless). Další varianty, které přicházely v úvahu, skupina vyhodnotila jako nevhodné (např. 2D čárový kód pro malou kapacitu, holografickou paměť pro nezralost technologie apod.). Popis využití bezkontaktních čipů v e-pasech jsou popsány v [ICAO Bio Annex I].

Vybraná technologie je v současné době známa také pod názvem RFID. RFID zahrnuje celou řadu nejrůznějších zařízení, která dokáží komunikovat bezdrátově na bázi technologie popsané v ISO/IEC 14443. Čipy zpřístupňované tímto protokolem zahrnují celou škálu od jednoduchých paměťových čipů až po plnohodnotné čipy mikroprocesorové vybavené koprocesory pro kryptografii (symetrickou i asymetrickou).

Právě díky využití technologie RFID vzniká celá řada nedorozumění týkajících se tzv. čipové totality a velkého bratra, kdy je možno využívat bezkontaktní čipy ke sledování pohybu označeného předmětu a v případě pasu konkrétního člověka. Mezi RFID čipem použitým jako značkovače zboží v supermarketu a mezi čipem použitým v e-pasu je rozdíl zhruba odpovídající rozdílu mezi flashdiskem a PDA.

2.2.1. Hardware

Je až s podivem, co všechno dokáží výrobci vměstnat na jeden mikroprocesor, který je nutno nejen ovládat, ale hlavně napájet modulovaným elektromagnetickým polem. Existuje několik výrobců, kteří dokáží vyrobit čipy s požadovanými vlastnostmi. Čipy do e-pasu vyrábějí například následující výrobci: Philips (SmartMX P5CT072), Infineon (SLE66CLX641P), Toshiba (TLCS900), Sharp, Atmel (AT90SC12872RCFT), Samsung (S3CC9GCX), STMicroelectronics.

Pro využití v e-pasu specifikuje ICAO následující požadavky:

- kompatibilita s ISO 14443 s modulací typu A nebo B
- kompatibilita s ISO 7816 - 4 a vyšší pro práci s daty na kartě
- dostatečná paměť pro uložení požadovaných dat (obličej, otisk)

- podpora kryptografie na čipu pro zabezpečení dat (RSA, EC)
- volitelně implementace BAC (BAC viz dále)

2.2.2. Operační systém

Operační systémy využívané pro implementaci požadavků ICAO v e-pasech pokrývají širokou škálu od jednoúčelových OS specializovaných na e-pasy po JavaCard applety. OS pro e-pasy dodávají např. následující dodavatelé: SC2 (Apollo OS), IBM(JCOP), Axalto (Axseal), T-Systems (TCOS), G&D (Starcos 3.1PE), Oberthur (ID One e-pass), GemPlus (GemBorder) a další.

2.2.3. Náhodné UID

Identifikovatelnost čipu umístěného v e-pasu vyplývá ze specifikací ISO 14443, kde je definováno tzv. UID (U*niversal* I*dentifier)*, které se používá v rámci tzv. antikolizního mechanismu pro výběr čipu pro případ, kdy je v elektromagnetickém poli čtecího zařízení více čipů schopných komunikovat. Když čtecí zařízení zahajuje komunikaci s čipy ve svém okolí, vyšle příkaz REQ. V případě, že čip zaznamená tento požadavek, v definovaných časových okamžicích dle hodnoty jednotlivých bitů svého UID vysílá či mlčí a zároveň naslouchá vysílání ostatních. Takto je možno mezi "naslouchajícími" čipy zvolit jeden s nejvyšším UID (z hlediska mechanizmu volby). Pokud to není ten správný, čtečka mu jako další odešle příkaz HALT, který způsobí, že čip již v rámci "volby" neodpovídá a je možné zvolit čip s dalším UID podle velikosti.

Jak je vidět, je využití UID z hlediska funkcionality čipu nutné a toto UID musí být konstantní po dobu pobytu čipu v el. mag. poli. Tohoto požadavku využívají dodavatelé čipů pro elektronické pasy a implementují tzv. náhodné UID, kdy čip v pasu drží UID právě jen po dobu, kdy je přítomen v elektromagnetickém poli jednoho zařízení a při každém vstupu do pole (=zapnutí napájení) generuje nové pseudo-náhodné UID.

2.3. Souborová struktura

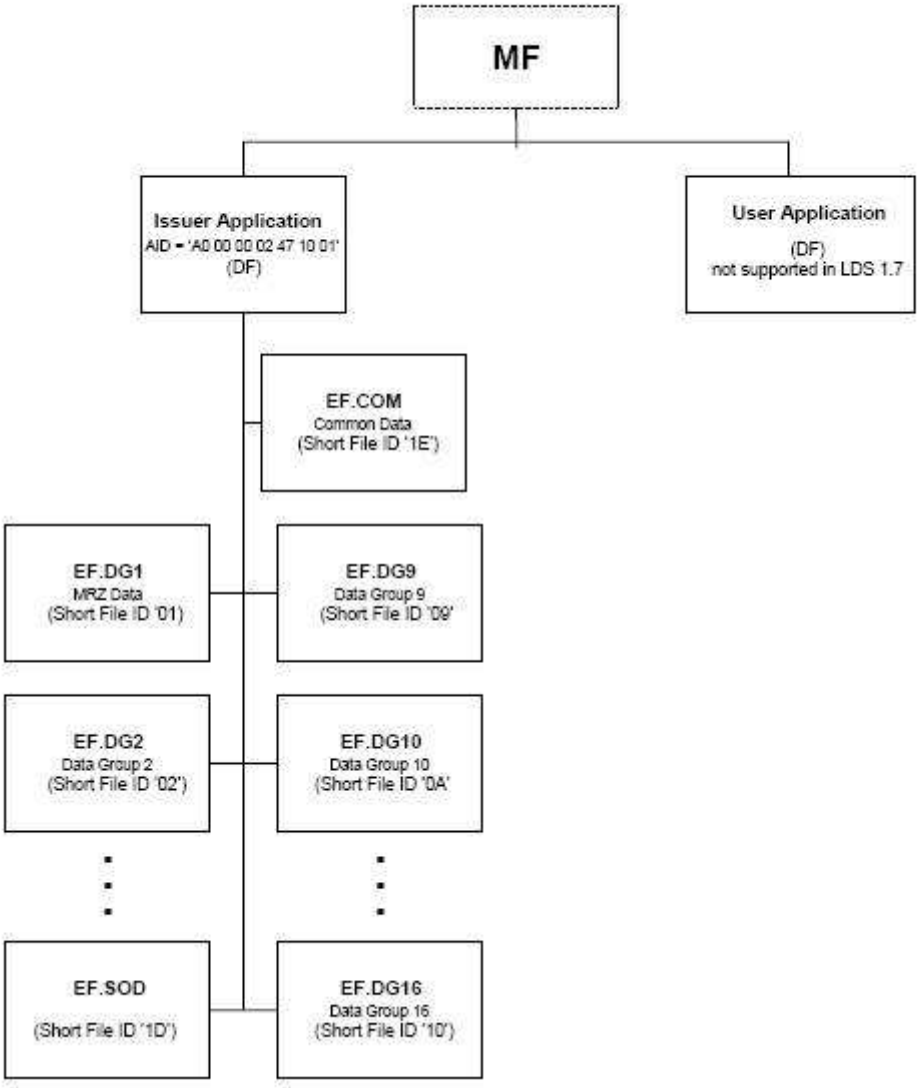
V případě bezkontaktních čipů se nejčastěji používají jednoduché registry pomocí kterých se řídí přístup do budov či obsah elektronické peněženky. Tj. v případě bezkontaktních čipů dosud nejsme zvyklí, že bychom využívali nějakou souborovou strukturu. Naopak u kontaktních čipů jsme na souborovou strukturu zvyklí. Standard ISO/IEC 7816 nám zavádí souborovou strukturu vzdáleně připomínající souborový systém používaný na discích. Dosud jsme takovou strukturu spojovali jen s kontaktními kartami.

V cestovních pasech se využívají bezkontaktní čipy, ale s souborovou strukturou podle standardů z rodiny ISO/IEC 7816. Tj. jedná se o pokročilé čipy, které bezkontaktně komunikují dle ISO 14443, ale jinak mají vlastnosti, se kterými jsme se dosud setkávali u kontaktních čipů.

Na obr. 3 je znázorněn příklad základní souborové struktury aplikace na čipu. Na obrázku nejsou soubory (jsou zpravidla řešeny v závislosti na operačním systému čipu):

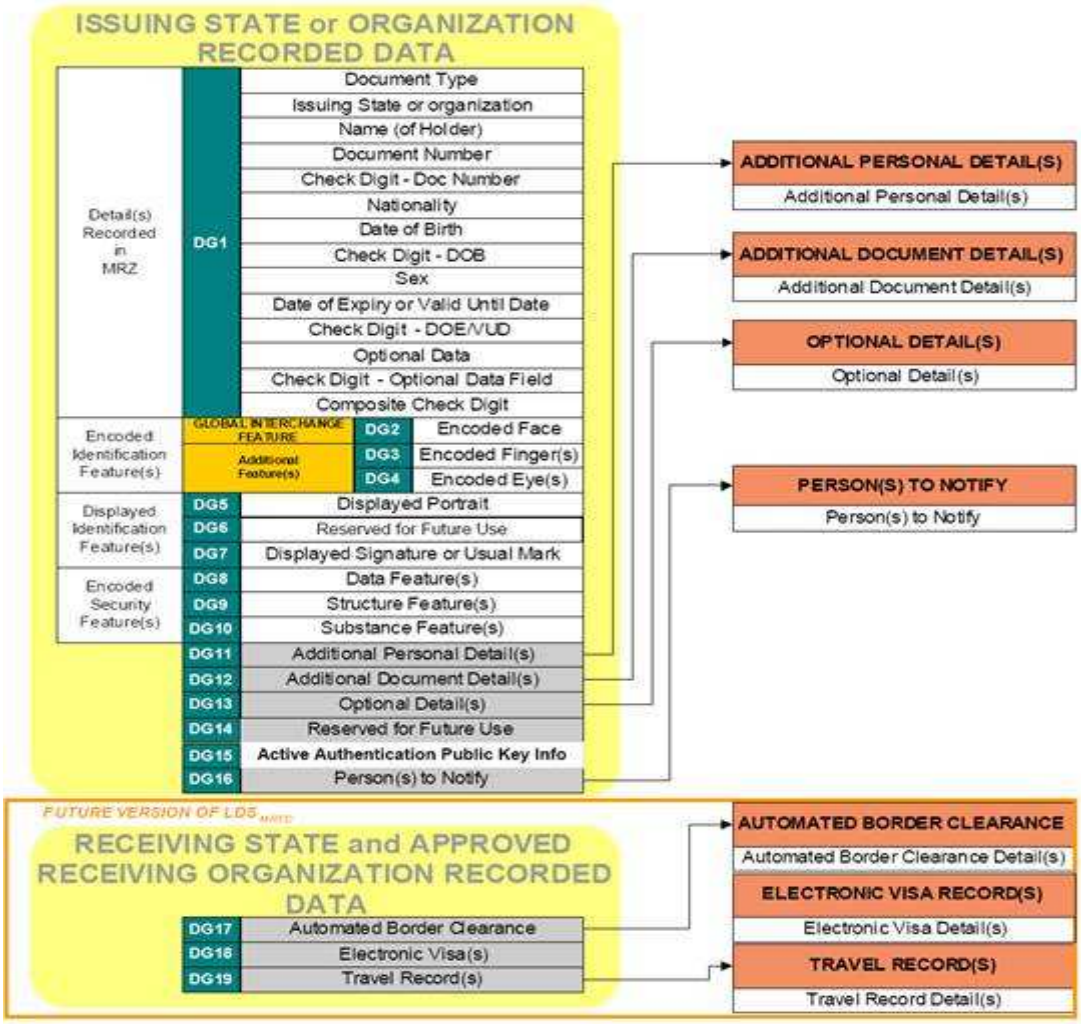
- s tajnými klíči pro Basic Access Control (zpravidla označované K_{ENC} a K_{MAC}),

- s privátním klíčem KPr_{AA} pro aktivní autentizaci,
- se soukromým DH číslem pro autentizaci čipu



Obr. 3 Souborová struktura aplikace e-pasu (levý podstrom).

Z pohledu dat uložených v uvedených souborech se zavádí pojem logické datové struktury – LDS. Data jsou obsažena v následujících datových skupinách (*Data Groups - DG*). Jednotlivé datové skupiny (DG) jsou definovány na obr. 4.



Obr. 4 Datové skupiny

Skupiny DG1 (kopie MRZ) a DG2 (obraz obličeje) jsou povinné. Od 28. 6. 2009 budou v pasech vydávaných členskými státy EU (s výjimkou GB, IRL) povinné rovněž otisky prstů (DG3). Dále je zajímavá skupina DG14, o které se zmíníme v kapitole Extended Access Kontrol (EAC). Datové skupiny jsou mapovány na elementární soubory (EF) v rámci struktury karty (viz obr. 3). Uvnitř souborů jsou pak data uložena s využitím kódování TLV (tag-length-value), které je definováno v ISO 7816-4 a -6 a vychází z ASN.1 DER kódování. Hodnoty jednotlivých tagů (jak následují za sebou a v jaké jsou struktuře) definuje tzv. šablona. Například data, která nesou biometrickou fotografii držitele pasu jsou v EF.DG2 uložena takto:

‘75’ ’82319C’
‘7F61’ ’823197’
‘02’ ’01’ ‘01’
‘7F60’ ‘82318F’
‘A1’ ‘26’
‘80’ ‘02’ ’0100’
‘81’ ’01’ ’02’
‘83’ ’07’ ’20020315133000’
‘84’ ’08’ ’2002040120070331’
‘86’ ’02’ ’0001’

‘87’ ’02’ ’000A’
‘88’ ’02’ ’0004’
‘5F2E’ ’823162’ ’… 12642 bajtů biometrických dat ve formátu CBEFF

Pro všechny skupiny jsou v dokumentu [ICAO Bio LDS] definovány šablony. Dle těchto šablon jsou pak data formátována a jediným stupněm volnosti je možnost vynechat volitelné položky.

2.4. Biometrie

V elektronických cestovních pasech je v současné době využíváno biometrického obrazu obličeje a pravděpodobně od 28. 6. 2009 budou pasy členských zemí EU vybaveny navíc ještě otisky prstů. Specifikace ICAO se v případě biometrie odkazuje na mezinárodní normy z rodiny ISO/IEC JTC 1/SC 37.

2.4.1. Obraz obličeje

ICAO pro biometrický obraz obličeje přebírá specifikaci [ICAO Bio Annex D]. V této normě jsou definovány požadavky na obraz obličeje, který je vhodným vstupem pro algoritmy rozpoznávání obličeje. Norma specifikuje několik druhů obrazů obličeje od základního obrazu obličeje (*basic face image type*), přes frontální obraz obličeje (*frontal face image type)*, plný frontální obraz obličeje (*full frontal image type*) až po tzv. token image (*token face image type*) určený pro uložení do čipu. Norma postupně zpřesňuje požadavky na jednotlivé typy obrazů. Každý následující vychází z předchozího.Výsledné obrazy jsou ukládány do obálky CBEFF, která pro obraz obličeje stanovuje dodatečné typy metadat.

Požadavky na frontální obraz (*frontal image*) jsou následující (příkladem je obrázek s vyznačenými MPG4 body):

- požadavky na scénu:
  - pozice - žádný z měřených úhlů nesmí být od střední polohy odchýlen více jak o 5 stupňů v absolutní hodnotě
  - na fotografii nesmí být další obličej
  - fotografovaný musí stát čelem ke kameře bez natáčení hlavy
  - osvětlení by mělo být rovnoměrné - žádné směrové světlo
  - na obličeji by neměly být žádné stíny
  - oční důlky by neměly být zastíněné
  - je třeba zamezit vytváření tzv. hot-spot - přesvětlených míst
  - brýle nesmí mít silné obroučky a obroučky nesmí zakrývat oči, na brýlích by neměly vznikat odlesky, jiné než čiré brýle jsou povoleny jen ze zdravotních důvodů
  - páska přes oko smí být použita pouze ze zdravotních důvodů a musí být popsána v metadatech
- fotografické požadavky:
  - správná saturace (ani pře- ani podexponováno)
  - fotografie by měla být ostrá od nosu po uši a od brady po temeno hlavy
  - barevné vyvážení obrazu by mělo být neutrální (důležité je nastavit dobře bílou), červené oči nejsou akceptovatelné

    - nemělo by docházet ke zkreslení vlivem objektivu pozorovatelnému lidským okem (zkreslení objektivu typu rybí oko)
- požadavky na digitalizaci obrazu:
    - poměr velikosti pixelů musí být 1:1
    - souřadnice v obrázku musí mít počátek v levém horním rohu a rostou směrem doprava a dolů do kladných hodnot
- barevný profil:
    - hustota šedé - v oblasti obličeje musí být dynamický rozsah minimálně 128 stupňů šedé bez přepálení
    - barevný prostor - RGS, YUV, grayscale, pomocí barevného profilu zařízení musí být generován normalizovaný obrázek např. s RGB
- obrázek nesmí být prokládaný, ani nesmí vzniknout z prokládaného obrázku pomocí filtrování

Požadavky na plný frontální obraz (full frontal) zahrnují požadavky na frontalní obraz a doplňují

- fotografické požadavky
    - obličej musí být na fotografii horizontálně vycentrovaný (linka AA musí být vertikální osou fotografie)
    - pozice očí (délka BB) musí být vzdálena od spodního okraje na vzdálenost mezi 50% do 70% z výšky obrazu
    - šířka hlavy (délka CC) musí být taková (vůči šíři celého obrazu), aby platilo A:CC = 7:5
    - výška hlavy (BB) by neměla přesáhnout 80% výšky obrázku
- požadavky na digitalizaci - obrázek má mít minimální šířku min. 180 pixelů a vzdálenost očí musí být minimálně 60 pixelů

A jako poslední uvedeme požadavky na tzv. token image (obraz pro umístění do čipu)

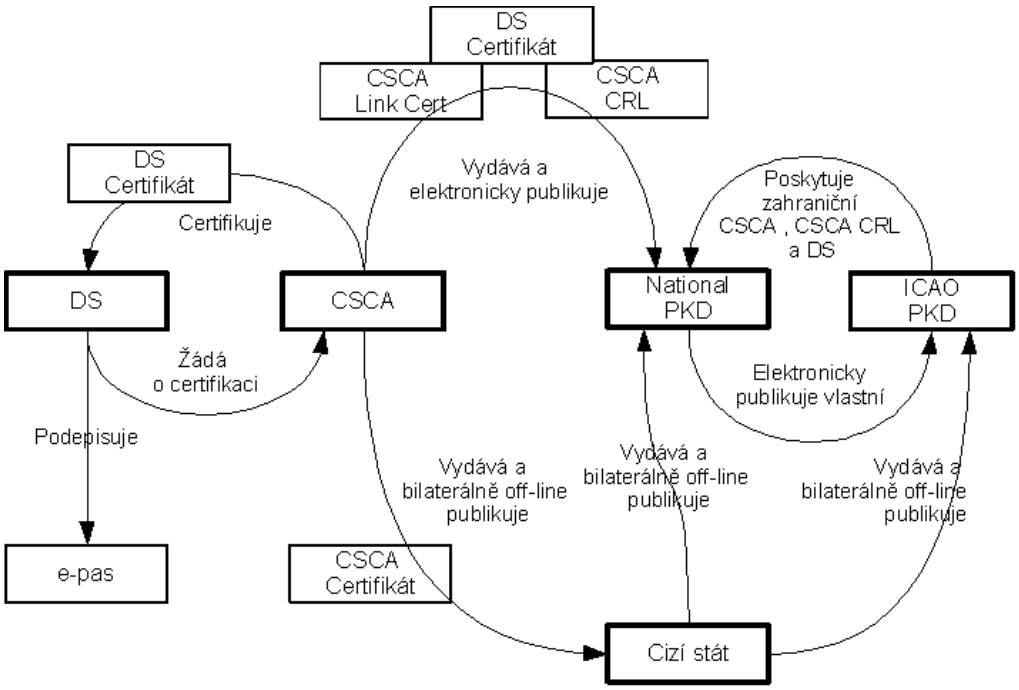
- poměr stran obrazu je 3:4
- pozice očí od horního okraje je 0.6 x šířka obrázku
- vzdálenost očí je 0,25 x šířka obrázku
- pozice pravého oka od levého okraje snímku je (0.625 x šířka obrázku)-1
- minimální šířka obrázku je 240 pixelů (60 pixelů mezi očima)

Další požadavky na obraz obličeje jsou: uniformní pozadí 18% šedé.

Doporučeným formátem pro ukládání fotografií do čipu je JPEG2000 a povolen je rovněž JPEG.

2.5. PKI

Pro ověřování pravosti elektronických dat v pasech byla navrženo v dokumentu [ICAO Bio PKI] relativně jednoduchá infrastruktura veřejných klíčů. Tato infrastruktura je jednoúrovňová. Každý stát je povinen pověřit nějaký subjekt provozováním národní CA (*CountrySigning CA*), která certifikuje klíče výrobce dokladů tzv. document signer (DS). Využití PKI a role jednotlivých komponent je následující (tučně jsou označeny organizace, jinak jde o přenášená data):



2.5.1. Country Signing Certification Authority (CSCA)

Country Signing Certification Authority (CSCA) je zřízena státem, nebo státem povařenou organizací. Jde o off-line certifikační autoritu. Vydává kořenový self-signed certifikát ke svému privátnímu klíči. Privátní klíč se zpravidla obnovuje každých 5 let. Při obnovení privátního klíče se vydává nový kořenový certifikát a tzv. link certifikát (speciální certifikát využívaný při obnově klíče CA, který slouží k provázání starého a nového klíče; nový klíč je certifikován s využitím starého a při včasné obnově umožňuje distribuovat nový certifikát CA s využitím důvěry ve starý - odpadá nutnost protokolárního předání a nový certifikát lze šířit elektronickou cestou). Doba platnosti certifikátu CSCA se vypočte jako Doba používání klíče + Délka platnosti certifikátu DS (typicky 5 let + (10 let + 3 měsíce)).

CSCA pravidelně vydává CRL s periodou maximálně 90 dnů.

2.5.2. Document signer (DS)

Document signer je subjekt, který elektronicky podepisuje elektronická data v pasu - obvykle výrobce dokladů. Pro podepisování používá privátní klíč ocertifikovaný CSCA. Privátní klíč DS se zpravidla používá po dobu cca 3 měsíců a každý klíč DS je ocertifikován CSCA. Platnost certifikátu DS musí pokrývat celou dobu, kdy jsou platné dokumenty podepsané s využitím tohoto certifikátu. Při platnosti dokumentu 10 let je délka platnosti certifikátu DS 10 let a 3 měsíce.

2.5.3. Distribuce certifikátů a ICAO Public key directory (PKD)

Důvěryhodné předání národního kořenového certifikátu je základem pro bezpečně pracující systém pro inspekci e-pasů. Spoléhající se stát musí být přesvědčen o původu tohoto kořenového certifikátu. Proto se kořenové certifikáty jednotlivých národních certifikačních

autorit se primárně distribuují bilaterálně offline diplomatickou poštou na datových nosičích. Kořenové certifikáty se takto distribuují mezi státy a také do centrálního systému nazvaného ICAO PKD. Rovněž bilaterálně se distribuují CRL.

ICAO PKD je adresářový server, který slouží k publikaci certifikátů DS a CRL vydávaných národními autoritami jednotlivých států, které vydávají e-pasy. Tento server je primárním zdrojem certifikátů DS a sekundárním zdrojem CRL. CSCA certifikáty se pomocí ICAO PKD nedistribuují, ale jsou využívány v rámci ICAO PKD k ověřování certifikátu DS a CRL, které jsou do ICAO PKD importovány.

2.5.4. Národní Public key directory (PKD)

Pro komunikaci s cizími státy a pro distribuci certifikátů cizích států do systémů uvnitř státu se doporučuje využívat jednoho centrálního systému - Národního PKD.

2.5.5. Ověřování platnosti podpisu v pasu

ICAO stanovuje, že i v případě selhání ověření elektronického podpisu nebo certifikátu, kterým je ověřen klíč použitý k vytvoření podpisu, může být nadále pas považován za platný, ale podléhá podrobnějšímu zkoumání při průchodu přes inspekční systémy. Dojde-li tedy v průběhu období platnosti pasu (a tedy i certifikátů použitých pro zabezpečení) ke kompromitaci některého z použitých privátních klíčů a tak k jeho uvedení na CRL, pas může být nadále používán, ale držitel pasu je vystaven důkladnějším prohlídkám při překračování hranic.

2.5.6. Kryptografické algoritmy a jejich síla

Pro vytváření a ověřování elektronického podpisu v systému e-pasů je možno využívat asymetrické algoritmy RSA, DSA a Eliptické křivky DSA (ECDSA). Vzhledem k relativně dlouhé platnosti certifikátů a podpisů je nutno volit silnější algoritmy, než pro běžné krátkodobé použití. Klíč CSCA by měl být délky nejméně 3072 bitů pro RSA a DSA a 256 bitů pro EC; pro DS pak 2048 bitů pro RSA a DSA a 224 pro ECDSA; pro Aktivní autentizaci pak 1024 pro RSA a DSA a 160 bitů pro ECDSA . Jako hash funkci je doporučeno používat funkce ze třídy SHA-2 (SHA-256, 512 apod.). Pro vytváření elektronického podpisu s využitím RSA je doporučeno používat podpisové schéma RSA-PSS.

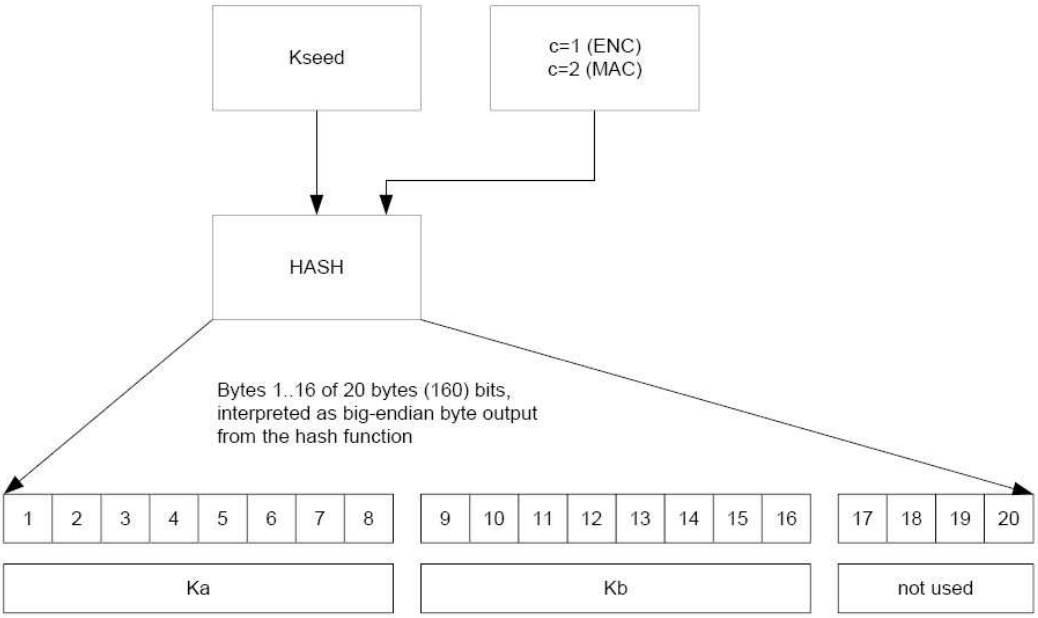
2.6. Zabezpečení elektronické části

Celý pas je vybaven bezpečnostními prvky, které mají zamezit vyrobení falešného pasu. Rovněž elektronická část pasu je chráněna před falšováním. Kromě ochrany před kopírováním bylo nutno z důvodu využití bezkontaktního rozhraní (a možnosti čtení na dálku bez vědomí držitele) zavést ochranu před neoprávněným čtením dat z čipu.

2.6.1. Basic access control

Mechanismus Basic access control je navržen s cílem zabránit neoprávněnému čtení pasu bez vědomí držitele. Je založen na vlastnosti čipových karet tzv. secure messagingu. V rámci secure messagingu se používá jeden klíč pro autentizaci zpráv pomocí MAC a druhý pro

šifrování zpráv algoritmem 3DES. Klíče se odvozují jednoduchým mechanismem z údajů v MRZ datové stránky - číslo pasu (9 znaků), datum narození držitele (6 znaků data YYMMDD), datum ukončení platnosti pasu (6 znaků data YYMMDD). Klíče se odvozují dle následujícího obrázku:



Pro vygenerování klíčů je tedy nutno přečíst MRZ. Díky této vlastnosti je možno data z čipu číst pouze pokud držitel pasu umožnil přečíst MRZ, což chrání pas před neoprávněným čtením bez vědomí držitele. Díky šifrování jsou data rovněž chráněna před odposlechem.

Nevýhodou mechanismu BAC je jeho slabost. Zdrojem pro generování klíče nejsou dostatečně náhodná data a v mnoha případech jsou velmi omezená (zejména při sekvenčním číslování pasů). Síla ochranného mechanismu je dostatečná pro on-line ochranu přístupu k pasu, takže útočník nedokáže přečíst data z pasu, který má např. člověk procházející kolem čtecího zařízení. Při odposlechnutí oprávněného čtení pasu (možné až na vzdálenost metrů) a zaznamenání komunikace je možné zachycená data dešifrovat s běžně dostupným HW v krátkém čase (hodiny).

Implementace mechanismu BAC není ve specifikacích ICAO povinná. EU pro členské státy určuje BAC jako povinný.

2.6.2. Elektronický podpis data v čipu

Data uložená v čipu jsou elektronicky podepsána vydavatelem pasu DS s využitím privátního klíče certifikovaného národní certifikační autoritou (CSCA).

Při generování resp. verifikaci podpisu jsou prováděny následující kroky

1. Ze všech datových skupin DGn jsou vypočteny hodnotu otisku a jsou shromážděny do ASN.1 struktury LDSSecurityObject

2. DER kódování LDSSecurityObject je datovým obsahem CMS zprávy typu SignedData - je vypočten otisk a je uložen mezi podepisované atributy CMS v CMS zprávě
3. Do CMS zprávy je vložen certifikát DS a je provázán s obsahem SignerInfo struktury pomocí IssuerAndSerial hodnoty
4. S použitím odpovídajícího algoritmu pro otisk a elektronický podpis se vytvoří samotná hodnota elektronického podpisu z DER kódování podepsaných atributů CMS zprávy

Takto vytvořený elektronický podpis zabraňuje tomu, aby si při falšování pasu mohl padělatel naplnit elektronickou část dle svého.

2.6.3. Aktivní autentizace

Výše popsaný elektronický podpis dat v čipu e-pasu nebrání tato data kopírovat. Doporučení ICAO proto specifikuje ještě volitelný mechanizmus tzv. aktivní autentizace (AA), který s využitím vlastností čipu bezpečně uchovat privátní klíč zajistí, že čip nebyl zkopírován. V čipu e-pasu je uložen privátní klíč (generovaný přímo v čipu nebo v rámci bezpečného prostředí personalizace). Veřejný klíč příslušející k tomuto privátnímu je zapsán do DG15 a je zahrnut do dat vybavených elektronickým podpisem (viz předchozí kapitola). Tímto elektronickým podpisem je zajištěn správný původ tohoto klíče. Pokud by se padělatel pokusil pas zkopírovat, nutně musí zkopírovat i DG15 beze změny a tedy i hodnotu veřejného klíče. Odpovídající hodnota privátního klíče je však bezpečně uložena v čipu bez možnosti ji přečíst. Při kontrole takto falšovaného pasu pak mechanizmus AA selže (nebude v souladu veřejná část klíče v DG15 a privátní část v čipu).

Aktivní autentizace probíhá takto:

1. Čtečka provede čtení dat z pasu včetně DG15 a ověří jejich integritu a původ pomocí elektronického podpisu
2. Čtečka vygeneruje náhodná data a pošle je do čipu
3. Čip v pasu tato data podepíše s využitím privátního klíče pro AA a odešle podepsaná data do čtečky
4. Čtečka ověří elektronický podpis dat pomocí klíče získaného z DG15 - pokud se podpis podaří ověřit, je pas v pořádku, jinak se může jednat o falzifikát

Aktivní autentizace je náchylná k útoku na soukromí s využitím tzv. challenge sematic (viz bod 2 postupu AA). Pokud je výzva místo náhodného čísla generována tak, aby nesla hodnotu, existuje možnost sledování pohybu držitele pasu, protože v odpovědi na výzvu se pas identifikuje. Z tohoto důvodu AA není implementována v pasech USA a Spolkové republiky Německo a dalších zemí. V Německu byl v nedávné době zaznamenán úspěšný případ kopírování elektronické německého e-pasu, což vzhledem k blízkému zavedení výroby e-pasů ve většině zemí Evropy, vyvolalo silný mediální ohlas.

Poznámka: přehled odkazovaných referencí je uveden v části 2, která vyjde v Crypto-Worldu 11/2006

C. Bezpečnost elektronických pasů

Zdeněk Říha, Masarykova Univerzita a JRC EC Ispra, (zriha@fi.muni.cz)

O nově zaváděných elektronických pasech můžeme slýchat jak ujišťování úřadů, že jsou zcela bezpečné, tak i výroky tzv. hackerů o řadě proveditelných nebo i provedených útoků. Problémy nejčastěji souvisí s detekovatelností pasu (například odpálení bomby) nebo čitelností dat z pasu (a s tím souvisejícím klonováním pasů). Pojďme se v tomto článku podívat na problematiku bezpečnosti elektronických pasů podrobněji. Hned na úvod ale uvedu, že řada útoků na pasy je známa již delší dobu a státy se rozhodly elektronické pasy zavést, neboť rizika s nimi spojená považují za akceptovatelná. To platí například pro útoky klonováním dat, které jsou popsány již v dokumentaci organizace, které je standardizací elektronických pasů pověřena. Přesto byla možnost klonování dat prezentována řadou periodik téměř jako revoluční novinka.

Technologie

Standardizaci pasů na celosvětové úrovni má na starost Mezinárodní organizace pro civilní letectví (ICAO), což je část OSN. Tato organizace vydává (v současné době již v šestém vydání) standard číslo 9303, který popisuje, jak má pas vypadat. Nedávno byly standardizovány i elektronické pasy (samotné vydávání elektronických pasů je však na celosvětové úrovni zatím zcela dobrovolné). Řada vlastností elektronických pasů je volitelných, někdy je možná volba z několika variant. Evropská Unie, která nařizuje členským zemím vydávat elektronické pasy nejpozději od 28. srpna 2006, dále upřesnila některé parametry těchto elektronických pasů vydávaných svými členskými zeměmi.

Elektronický pas se od pasu tradičního liší integrovaným bezkontaktním čipem a logem elektronického pasu na obalu. Čip s anténou bývá nejčastěji vložen buď do vnějších desek pasu nebo do stránky s datovými údaji, která z tohoto důvodu bývá zesílena. U českých pasů je čip vložen do stránky s datovými údaji, která bude přesunuta z posledního listu na začátek pasu a bude tvořena polykarbonátovou vrstvou, do které bude zalit čip a do níž bude také laserem gravitována černobílá fotografie držitele pasu. Čip v pase je bezkontaktní čipová karta splňující ISO 14443 (povolené jsou oba typy – A i B). Tato technologie je schopna přenášet data na vzdálenost 0-10 cm a umožňuje využití relativně komplexních kryptografických čipových karet s paměťovou kapacitou desítek kB. Tím se liší od jiných RFID technologií, které sice komunikují na delší vzdálenosti, neumožňují však o moc složitější operace než pouhé vyslání identifikačního čísla. Na vyšší úrovni se komunikuje klasickým protokolem čipových karet podle ISO 7816-4 (tj. SELECT AID, SELECT FILE a READ BINARY).

Data v elektronickém pase jsou soubory (v terminologii čipových karet elementární soubory) v jednom adresáři (v terminologii čipových karet dedikovaném souboru). Datových souborů je maximálně 16, jsou nazývány DG1 až DG16 (DG jako Data Group – datová skupina). DG1 obsahuje data ze strojově čitelné zóny (tj. jméno, příjmení, číslo dokumentu, vydávající stát, pohlaví, datum narození, datum vypršení platnosti a volitelná data, která v českém případě obsahují rodné číslo), DG2 obsahuje fotografii držitele pasu (ve formátu JPG nebo JPG2000 plus nějaká metadata). DG3 je určena pro otisky prsů, DG4 může obsahovat oční duhovku. Další datové skupiny obsahují dodatečné údaje o držiteli, vydávající instituci nebo pase. Kromě datových skupin obsahuje pas ještě dva soubory s metadaty. Soubor EF.COM obsahuje seznam přítomných datových skupin (plus údaje o použitých verzích) a EF:SOD

digitální podpis dat. Soubory EF.COM, EF.SOD, DG1 a DG2 jsou povinné pro všechny elektronické pasy. V Evropě bude nejpozději od 28. června 2009 povinně ukládána ještě datová skupina DG3. Všechny ostatní datové skupiny jsou volitelné.

Přístup k datům

V základní verzi nejsou data v elektronických pasech z hlediska důvěrnosti nijak chráněna. Na nižší úrovni (ISO 14443) získáme seznam dostupných čipů, jeden z nich vybereme jako aktivní a s tím komunikujeme. Data z pasu získáme výše uvedenými příkazy (SELECT FILE, READ BINARY) bez autentizace. Komunikace není nijak šifrována, takže možný je i odposlech probíhající komunikace.

Takové pasy však vyvolávají řadu debat. Jedním z možných vylepšení je stínění pasu (jeho zabalení do kovového obalu, např. do hliníkového přebalu). Stínění pasu využívají například americké pasy. Takto je možné zabránit nevědomé komunikaci s čipem (např. v kapse). Stínění ale nezabrání odposlechu, jakmile je pas otevřen a komunikace legitimně probíhá. Stínění navíc ztěžuje legitimní komunikaci a při mírném otevření pasu již není účinné.

Jinou možností obrany vůči neautorizovanému čtení je autentizace čtečky[1] a následná šifrovaná komunikace. To poskytuje obranu také vůči odposlechu přenášených dat. Vyřešit je však potřeba skutečnost, že pas musí být čitelný pohraničníky všech zemí světa. Autentizační údaje jim tedy musí být nějak přístupné. Řešení se našlo takové, že autentizační údaje jsou získány hašováním určitých údajů ve strojově čitelné zóně. Takto může přistupovat k datům v pase kdokoliv, kdo otevře pas na stránce s datovými údaji. Předpokládá se tedy, že kdokoliv, kdo má pas v ruce a může v něm číst data, má přístup i k údajům na čipu. Řeší se tak přístup k datům v zavřeném pase v kapse neznámého člověka, ale přístup k datům není omezen pouze na pohraničníky, ale číst data mohou například i hoteliéři apod. Tento způsob ochrany dat v pasech se nazývá základní řízení přístupu (basic access control – BAC) a celosvětově je volitelným ochranným prvkem. Pasy členských zemí EU však musí BAC implementovat povinně. Tedy i české pasy jsou chráněny pomocí BAC.

Základní řízení přístupu brání jak neautorizovanému čtení, tak odposlechu, nevýhodou však je malá entropie dat, ze kterých se odvozují autentizační údaje (viz dále). Základní řízení přístupu také nemůže zabránit detekovatelnosti čipu.

Pokud není čip stíněn, je možné jej detekovat. Nižší komunikační vrstvy podle ISO 14443 nám umožňují získat minimálně identifikátor čipu. Identifikátor čipu je buď náhodně vygenerován při každém resetu (u všech čipů typu B a u některých čipů typy A) nebo fixní po celou dobu života čipu (u některých čipů typu A). V případě fixních identifikátorů je možné sledovat čip (např. jeho pohyb) i v případech, kdy nejsme schopni z čipu získat další data. Identifikátor může prozradit i nějaké další údaje o čipu, příkladem může být samotná délka identifikátoru, ta totiž není jednotná (standard umožňuje několik variant (4, 7 nebo 10 bajtů), ty jsou však u výrobců různě oblíbené).

[1] Nejedná se o klasickou autentizaci čtečky, protože autentizační data nejsou tajná. Jedná se spíše jen o informaci, že čtečka zná určité informace vytištěné v pase. To by mělo prokázat možnost fyzického přístupu k pasu.

Integrita dat a autenticita čipu

Integrita dat je zajištěna digitálním podpisem dat. Digitální podpis je umístěn v souboru EF.SOD a jedná se o klasickou CMS strukturu typu SignedData. Hierarchie PKI je jednoúrovňová. Každý stát má svoji CA (tzv. CSCA – Country Signing CA), která vydává certifikáty složkám, které vydávají pasy (řekněme krajům, to záleží na rozhodnutí každé země) – jedná se o tzv. podepisovače dokumentů (Document Signers). Samotná data v pase jsou podepsána těmito podepisovači dokumentů.

Pro ověření podpisu musíme mít certifikát CVCA příslušné země, ten musíme získat důvěryhodnou cestou od dané země a certifikát konkrétního podepisovače dokumentů, ten se buď nachází přímo v pase (v části certifikátů struktury SignedData) a to je doporučený postup nebo jej musíme získat přímo od dané země podobně jako certifikát CSCA.

Podepsaná data tvoří speciální strukturu obsahující haše všech přítomných DG souborů v pase. Tímto způsobem je možné ověřit integritu každého souboru samostatně (tj. ověříme digitální podpis souboru EF.SOD a na základě zde uvedených hašů kontrolujeme integritu jednotlivých souborů).

Podpisové mechanismy použitelné v elektronických pasech jsou RSA (ve variantách RSASSA-PSS a RSASSA-PKCS1_v15, viz RFC 3447), DSA (viz FIPS 186-2, díky krátkým klíčům nyní nepoužitelné, čeká se na standardizaci algoritmu pro delší klíče) a ECDSA (viz X.62). Použitelné hašovací funkce jsou SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512.

Digitální podpis dat v pase je jedním z klíčových bezpečnostních prvků elektronických pasů, ne-li přímo ten nejdůležitější. Při podepisování dat si země může vybrat podpisové schéma, které jí vyhovuje z hlediska implementace (všechny komponenty však musí používat jen jediné schéma). Při ověřování podpisu je pochopitelně nutné podporovat všechny varianty. Ověřování podpisu je relativně bezproblémová věc, komplikacemi může být velké množství algoritmů, které je třeba implementovat, získávání správných kořenových certifikátů (CSCA) všech zemí (ICAO plánuje adresářové služby pro tento účel), CRL (země musí vydávat minimálně jednou za 90 dnů) a datové skupiny, u nichž jsou možné legitimní změny (typicky DG16 obsahující adresy příbuzných pro případ informování o nehodě držitele) – takové datové skupiny se nepodepisují.

Je zřejmé, že digitální podpis nemůže zabránit vytváření identických kopií dat (včetně souboru EF.SOD s digitálním podpisem). Z toho důvodu není možné spoléhat pouze na data z čipu, ale je třeba při kontrole cestovního dokladu věnovat pozornost i klasickým ochranným mechanismům (bezpečnostní tisk, vodoznak apod.) a souladu vytištěných dat s daty uvedenými v čipu. Zabránit kopírování (klonování) dat však můžeme i za pomoci kryptografie a odolnosti vůči narušení. V takovém případě je v pase uložen asymetrický pár klíčů. Zatímco veřejný klíč je volně čitelný (uložen v DG15 a jako u každé jiné datové skupiny je jeho haš digitálně podepsán), soukromý klíč není z čipu získatelný a je pouze možné ověřit (pomoci algoritmu výzva-odpověď), zda jej má čip k dispozici. Tento postup se nazývá aktivní autentizace a je volitelným prvkem elektronických pasů. Ani EU nestanoví povinnost implementace AA. České pasy však AA implementují (například německé ne).

Dostupnost dat

Zničit čip je možné nejen neúmyslně (teprve praxe spolehlivě ukáže, zda čip opravdu vydrží 10 let platnosti pasu), ale také úmyslně. Čip je možné spolehlivě zničit například v mikrovlnné troubě, ta je však značně výkonná a může pas viditelně poškodit. Na Internetu existují návody, jak vyrobit zařízení, které má dostatečný výkon ke zničení čipu, ale zbytek pasu neponičí [4]. Elektronický pas s nefunkčním čipem by neměl být důvodem přímo k neplatnosti pasu, ale spíše jen signálem k důkladnější kontrole. Konkrétní postup v takovém případě je však věcí státu, který provádí kontrolu. Důvodem k záměrnému zničení čipu může být obava ze vzdálené čitelnosti dat nebo snaha podvodníka s ukradeným pasem o znemožnění využití dat z čipu (například k biometrické verifikaci). Znemožnit čtení dat z čipu je možné také rušením patřičného signálu čtečky.

Základní řízení přístupu (basic access control - BAC)

Základní řízení přístupu je mechanismus bránící čtení dat z čipu bez znalosti autentizačních klíčů. Tyto autentizační klíče jsou odvozeny z dat vytištěných ve strojově čitelné zóně. Konkrétně se jedná o číslo dokumentu, datum narození držitele a datum vypršení platnosti pasu. Všechny tyto údaje se nacházejí na druhém řádku čtecí zóny. Nebyly vybrány zcela náhodně, jsou to právě ty údaje, které obsahují kontrolní číslici (rozpoznání OCR znaků bývá chybové, z tohoto důvodu je preference polí s kontrolní číslici pochopitelná). Tyto tři údaje se v ASCII formě zřetězí (včetně příslušných kontrolních číslic) a hašují algoritmem SHA-1. Z tohoto haše se dalším hašováním odvodí (112 bitové 3DES) klíče pro šifrování a autentizaci MAC. Následně se příkazem GET CHALLENGE získá výzva od čipu a příkazem MUTUAL AUTHENTICATE se čtečka a čip vzájemně autentizují. Dojde k ustavení sdíleného klíče sezení a následná komunikace je zabezpečena Secure Messagingem.

Toto je klasická vzájemná autentizace, která je považována za bezpečnou, pokud jsou klíče tajné. V případě pasů nejde o tajnost klasickou, protože klíče jsou odvoditelné z dat napsaných v pase, nicméně i zde je vhodné zabránit náhodnému uhodnutí klíče. U pasů je však toto mírně problematické, protože data, ze kterých jsou klíče odvozeny, nemají příliš velkou entropii. Ačkoliv teoretické maximum je 58 bitů a v případě alfanumerického čísla dokumentu až 74 bitů, reálné hodnoty jsou o dost nižší. Pojďme se na jednotlivé položky podívat podrobněji:

- datum narození držitele: jeden rok mívá 365 až 366 dnů, teoretické maximum je 100 roků tj. asi 36524 dnů (15,16 bitu entropie). Reálně však můžeme věk držitele odhadnout s předností na 10 let (3652 dnů, 11,83 bitů entropie), často i přesněji.
- datum vypršení platnosti pasu: maximální délka platnosti pasu bývá 10 let (tedy podobně jako výše uvedených přibližně 3652 dnů, 11,83 bitů entropie). U dětí bývá platnost kratší (často 5 let). V nejbližší budoucnosti můžeme využít faktu, že elektronické pasy jsou vydávány jen krátkou dobu. První rok je entropie pod 8 bitů (pokud správně odhadneme, zda je platnost pasu 5 nebo 10 let).Využít je také možné skutečnosti, že pasy jsou vydávány jen v pracovní dny a datum vypršení platnosti přímo souvisí s datem vydání pasu (datum vypršení platnosti bývá určováno jako datum vydání plus X let platnosti). Pracovních dnů bývá v roce jen asi 2/3 kalendářních dnů.
- číslo dokumentu: na číslo dokumentu je ve čtecí zóně vyhrazeno 9 znaků. Pokud je číslo dokumentu kratší, doplní se znaky <, pokud je delší, patřičně se zkrátí. Pokud

číslo dokumentu uvažujeme pouze číselné (a znak <) získáváme 11^9 možností (31,13 bitu entropie), pokud je číslo alfanumerické, je možností až 37^9 (tedy 46,88 bitů entropie). Těchto hodnot bychom však dosáhli, jen pokud by čísla pasů byla zcela náhodná. A tak je tomu málokdy. Pokud však nevíme o číslování pasů dané země vůbec nic (a nebo ani netušíme, o jakou zemi se jedná), jsme v podobné situaci. Pokud však známe určité údaje o číslovacím plánu pasů dané země (nebo všechna platná čísla dokumentů), možností a tím entropie ubývá. Řada zemí čísluje své pasy sekvenčně. Známe-li datum vydání (nebo datum vypršení platnosti), možných čísel pasů není až tak moc. Například Česká republika vydává asi milion pasů ročně, známe-li rok vydání pasu a rozsah čísel pasů v tomto roce, zmenšuje se entropie na přibližně 20 bitů. Známe-li měsíc vydání a rozsah v tomto měsíci, je entropie asi 17 bitů. Podobně můžeme jít až k jednotlivým dnům. Takto detailně asi běžný člověk nebude znát číslování pasů, nicméně nejen insideři, ale například i hoteliéři mohou znát o číslování pasů dost (je možné, že dříve nebo později se podobné informace objeví například na Internetu). V praxi je odhad čísla pasů komplikován tím, že musíme nejprve odhadnout stát vydávající pas, případně ještě typ pasu, neboť různé typy pasů mohou být číslovány separátně.

- Každá z položek je ještě následována kontrolní číslicí. Algoritmus výpočtu kontrolní číslice je však veřejně znám, takže kontrolní číslice nepřináší žádnou novou informaci.

Abychom odhadli celkovou entropii dat můžeme entropii jednotlivých prvků sečíst. To je ovšem korektní jen v situaci, kdy jsou údaje zcela nezávislé. U data platnosti by se dalo diskutovat o tom, že si člověk požádá o doklad v 15 letech a pak jej pravidelně obnovuje. To je sice pravda u občanských průkazů, u pasů tomu tak ale asi moc nebude, takže tento vliv pravděpodobně můžeme zanedbat. Podobně bych neviděl souvislost mezi datem narození a číslem dokumentu. Mezi číslem dokumentu a datem vypršení platnosti však závislost typicky bude. Jen v případě zcela náhodných čísel dokumentů ne a pak můžeme entropii sčítat. U jiných číslovacích plánů už nějaká závislost bude a pak záleží kolik znalostí o tomto plánu máme. V případě značných znalostí může entropie čísla dokumentů značně klesnout. Teoreticky v případě sekvenčních čísel dokumentů, zemí o velikosti ČR, rovnoměrného vydávání pasů po celý rok a detailní znalosti čísel pasů vydávaných ten který den klesá entropie asi na 12 bitů. Celková entropie tak z teoretických 58/74 bitů klesá na přibližně 32 bitů.

Výpočtem entropie jsme se zabývali, abychom se nyní mohli věnovat možným útokům. Komunikace s elektronickým pasem začíná výběrem aplikace ePasu (SELECT AID), potom následuje autentizace a ustavení šifrovacího klíče. Autentizace začíná získáním 8bajtové výzvy z čipu (GET CHALLENGE) a pokračuje odesláním šifrované (a MAC kódem zajištěné) výzvy čtečky (obsahující také výzvu čipu). Pokud je MAC kód v pořádku (a výzva čipu je shodná), odpovídá čip podobně. Při autentizaci se používá statický šifrovací a MAC klíč, který je sdílený mezi čtečkou a čipem (tento je odvozený z dat ve strojově čitelné zóně). Na základě výzev je vypočítán klíč sezení (šifrovací a MAC). Všechny klíče jsou 112 bitové 3DES klíče (detaily viz ISO 7816 nebo [2], tam je příklad komunikace uveden od strany 47). Protože 112 bitů je příliš hodně na útok hrubou silou, můžeme s výhodou využít skutečnosti, že statické autentizační klíče jsou deterministicky odvozeny z informace v pase, která má mnohem menší entropii. Útok hrubou silou tedy můžeme provést s menším množstvím klíčů.

Typy útoků hrubou silou jsou v principu dva. Buďto odposlechneme úspěšnou komunikaci a tu se pak snažíme dešifrovat, nebo se snažíme úspěšně autentizovat vůči čipu a pak s ním komunikovat.

Výhodou odposlechu je možnost data si uložit a off-line je potom analyzovat. Pokud odposlechneme celou komunikaci, můžeme útokem získat všechna přenášená data. Nevýhodou je nesnadnost získání dat odposlechem existující komunikace (tj. komunikace musí probíhat a my ji musíme odposlechnout).

Nejprve získáme výzvu čipu, ta je přenášena nešifrovaně. Pak analyzujeme příkaz MUTUAL AUTHENTICATE zasílaný čtečkou čipu. Hrubou silou zkoušíme všechny smysluplné kombinace údajů ze strojově čitelné zóny, tyto hašujeme (dvakrát, viz detailní popis protokolu např. v [2]) abychom získali šifrovací klíč (MAC klíč nutně nepotřebujeme) a tímto zkoušíme dešifrovat datovou část příkazu a ověřujeme, zda se dešifrovaná výzva čipu (9.-16. bajt) shoduje s nešifrovaně poslanou výzvou (na toto nám stačí dešifrovat bajty 9-16 a xorovat s bajty 1-8 šifry (jedná se o CBC mód)). Pokud se výzva neshoduje, pokračujeme v prohledávání stavového prostoru, pokud se výzva shoduje, můžeme ještě pro kontrolu vypočítat MAC klíč a ověřit MAC příkazu, dále dešifrujeme odpověď čipu, abychom získali všechny výzvy a mohli tak vypočítat klíč sezení, pomocí kterého můžeme dešifrovat následnou komunikaci. Pro každý testovaný klíč musíme provést dvakrát SHA-1 hašování a jednou 3DES dešifrování. Alternativní útok může počítat MAC klíče a kontrolovat, zda má APDU příkaz odpovídající MAC kód. Pro každý testovaný klíč pak musíme provést dvakrát SHA-1 hašování, čtyřikrát DES šifrování a jedno 3DES šifrování[2]. Takový útok není rychlejší, ale může být výhodný v situaci, kdy máme k dispozici pouze odposlechnutá data ze čtečky (odposlouchávat čtečku je podstatně jednodušší, než odposlouchávat odpověď karty). V takovém případě můžeme získat statické klíče pouze na základě odchycených dat ze čtečky, pro přečtení dat se však musíme vrátit k pasu a data přečíst (klíče již k dispozici máme).

Jeden výpočet klíče z autentizačních dat, dešifrování dat a porovnání výzvy trvá na běžném počítači asi 1 mikrosekundu. Procházení prostoru autentizačních dat o velikosti 2^{32} tak zabere něco přes hodinu. Marc Witteman ve svém příspěvku [5] ukázal možnost provedení takového útoku vůči holandským pasům. Ve svém útoku využil dodatečných informací o závislosti čísla dokumentu na datu expirace a znalosti kontrolní číslice.

Jak již bylo zmíněno, odposlech existující komunikace není snadný. Zamýšlený dosah zařízení splňujících ISO 14443 je 0-10 cm. To sice neznamená, že odposlech na delší vzdálenost není možný, při odposlechu však útočník brzy narazí na problém poměru šumu a signálu. Zatímco signál čtečky je silný a zachytitelný na delší vzdálenosti, při odposlechu dat z čipu (přenášených pomocí zátěžové modulace) se bojuje o každý centimetr.

On-line útok vůči čipu prochází stavový prostor stejně, jedno ověření autentizačních dat však trvá déle, protože jednak musíme komunikovat s čipovou kartou, jednak je potřeba vždy vypočítat také MAC klíč a kód. Jedno ověření trvá u běžné komerční čtečky řádově dvě desítky milisekund, útok tak je asi 10 000 x pomalejší než off-line útok.

---

[2] Děkuji Marcu Wittemanovi za diskusi v této oblasti.

Autorův pokus o program pro off-line i on-line útoky můžete najít na http://www.fi.muni.cz/~zriha/bac . Program není speciálně optimalizovaný, test jednoho klíče trvá skutečně asi jednu mikrosekundu, režie programu pro generování správných kombinací dat a výpočtu kontrolní číslice je však významně vyšší. U off-line útoků program neřeší odposlech dat a očekává odchycená data v souborech.

Aktivní autentizace

Cílem aktivní autentizace je ověřit, zda je čip v pase autentický. Pomocí protokolu výzva odpověď se ověřuje, zda pas má k dispozici správný soukromý klíč. Asymetrický pár klíčů pro aktivní autentizaci je specifický pro každý pas. Protokol výzva-odpověď je založený na ISO 9796-2. Čtečka generuje 8 bajtovou výzvu a tu posílá čipu s příkazem INTERNAL AUTHENTICATE. Čip generuje další náhodnou část a obě části hašuje. Svoji náhodnou část a haš (spolu s hlavičkou a patičkou) podepíše svým soukromým klíče. Výsledek posílá čtečce. Ta digitální podpis ověří. Za předpokladu odolnosti vůči narušení čipu, správnosti implementace, odolnosti vůči útoků postranními kanály apod. je výsledkem bezpečné ověření autenticity čipu.

V praxi je aktivní autentizace komplikována faktem, že ne všechny implementace v čipu se drží faktu, že odpověď má být vytvořena podle ISO 9796-2 schématu 1. Může se pak stát, že odpověď není správně interpretována a autentizace selže.

Zajímavý je i útok vůči soukromí, kdy výzva, která se posílá k pasu k podepsání, není zcela náhodná, ale má určitou sémantiku, například kóduje čas a místo. Pak může nějaká země uchovávat výzvy a odpovědi jako důkaz o tom, že se daný člověk nacházel v daném čase na určitém místě. V praxi však takový důkaz musí čelit faktu, že pas podepíše kdekoliv a kdykoliv jakoukoliv výzvu a vypovídací hodnota odpovědí je tedy malá. I tak je ale existence tohoto útoku důvodem proč Německo ve svých pasech aktivní autentizaci neimplementovalo.

Brzy si zřejmě uvědomíme, že spolu s pasem jsme vlastně dostali i výkonnou čipovou kartu. Využití pro digitální podepisování dokumentů je však viditelně nebezpečné, neboť pas podepisuje vše bez dodatečné autentizace např. PINem (nehledě na fakt, že použitý protokol výzva-odpověď není vhodným podpisovým schématem). Využití pro autentizaci uživatele např. při přihlašování k počítači však už může být podstatně zajímavější.

Závěr

Ukázali jsme si, že elektronické pasy jsou vybaveny bezpečným nosičem dat, obsahujícím údaje o držiteli a vydávající instituci. V základní verzi jsou data chráněna „jen“ digitálním podpisem, volitelně je však možné chránit přístup k datům, případně zajistit autenticitu čipu.

Bez účinného stínění čipu je možné i s dodatečnými ochrannými mechanismy detekovat existenci čipu. To může vést k řadě útoků, reálně však budete podstatně snadněji vysledovatelní díky vašemu mobilnímu telefonu.

Ačkoliv entropie dat využitých pro odvození klíče je značně nižší než délka výsledného klíče, jsou v praxi realizovatelné útoky omezeny nesnadností získání odposlechnutých dat u offline útoků a pomalostí komunikace u on-line útoků. Předpokládáme-li, že při pohraniční kontrole

je typicky držitel pasu vzdálen asi 50 cm od pohraničního úředníka a ostatní osoby asi další 1 metr a vezmeme-li v úvahu velikost současných odposlouchávacích zařízení, nemusí být odposlech dat nejsnazším útokem pro získání dat uložených v čipu. Při on-line útocích nemusí být náročné dostat se do dostatečné vzdálenosti od pasu (s využitím velké antény ukryté v kufru to může být až 40 i 50 cm [3]), problémem však je pomalá rychlost komunikace, což omezuje počet pokusů o autentizaci, které můžeme v rozumném čase provést.

Je dobré si také uvědomit, že BAC neomezuje přístup k datům těm subjektům, kteří z něj mohou přečíst údaje ze strojově čitelné zóny. Necháte-li tedy pas na recepci hotelu nebo jiné instituce, BAC vaše data neochrání. Na druhou stranu se v elektronické části pasu zatím nenachází moc jiných informací, než které jsou tam tak jak tak vytištěné. O možnostech zneužití digitálně podepsaných dat a kvalitních fotografií ke krádežím identit se však již spekuluje…

Aktivní autentizace je protokol ověřující autenticitu čipu. Možné útoky vůči němu mohou směřovat proti odolnosti pasu vůči narušení nebo využívat postranních kanálů.

Na závěr je možné konstatovat, že elektronická část elektronického pasu sice má svá slabá místa, ale zcela perfektní není žádná technologie. Navíc je třeba si uvědomit, že bezpečnost pasu nezáleží jen na elektronické části, ale také na částech ostatních (tiskové a jiné bezpečnostní techniky). Elektronický podpis dat zcela jistě zvyšuje bezpečnost těchto cestovních dokladů. Otázkou je, zda tato dodatečná bezpečnost stojí za nutné náklady na zavedení této technologie do praxe. Na takovou otázku mi však odpovídat nepřísluší.

A co otisky prstů?

Zmínil jsem, že nejpozději od 28. června 2009 se budou v EU do pasů ukládat i otisky prstů (DG3). Tyto však budou chráněny zcela jiných mechanismem. O tomto tzv. „rozšířeném řízení přístupu“ si povíme příště.

Poznámka

Názory, zde uvedené, jsou soukromé názory autora a nemohou být považovány za oficiální stanovisko Evropské komise.

Odkazy

[1] ICAO TAG MRTD/NTWG: Biometrics Deployment of Machine Readable Travel Documents, version 2.0. Včetně příloh A-J, http://www.icao.int/mrtd/download/technical.cfm
[2] ICAO TAG MRTD/NTWG: PKI for Machine Readable Travel Documents offering ICC read-only access v1.1, http://www.icao.int/mrtd/download/technical.cfm
[3] Kirschenbaum, I., Wool, A. How to Build a Low-Cost, Extended-Range RFID Skimmer, http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html
[4] MiniMe (pseudonym), Mahajivana (pseudonym): RFID-Zapper, http://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)
[5] Witteman, M. Attacks on Digital Passports, WhatTheHack, http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf

D. Říjnové akce – pozvánka (PR)

1) MFF UK – zve všechny zájemce na 3 přednášky prof. Serge Vaudenay (Security and Cryptography Laboratory)

http://www.karlin.mff.cuni.cz/~tuma/nciphers.html

Francouzský kryptolog **Serge Vaudenay** (http://en.wikipedia.org/wiki/Serge_Vaudenay , vedoucí Security and Cryptography Laboratory of the Swiss Federal Institute of Technologies) navštíví Katedru algebry MFF UK v Praze ve dnech 16.-20.10.2006. Během svého pobytu přednese tři přednášky, vždy v budově Sokolovská 83, Praha 8 (u stanice metra Křižíkova).

- Pondělí 16.10. v 17,20, posluchárna K1
  SSL security (how SSL works and the 2003 attack)

- Úterý 17.10 v 17,20, posluchárna K1
  TCHo, a new public-key cryptosystem based on the problem of finding a multiple of low weight and degree of a given polynomial

- Středa 18.10. v 17,20, posluchárna K3 (pozor - jiná posluchárna)
  Privacy in RFID

2) BIST GigaCon 2006

Tým Software-Konferencje srdečně zve k účasti na konferenci BIST GigaCon 2006 - Bezpečnost a spolehlivost informačních systémů, která se koná v ČR pod záštitou Ministerstva informatiky.
Konference se zabývá nejnovějšími řešeními a technologiemi, která zajišťují spolehlivost informačních systémů.
Konference BIST GigaCon 2006 proběhne 23.-24. října v Praze v Hotelu Pyramida.

Registrace je zdarma.
Více informací a přihlašovací formulář na http://www.bist.gigacon.org/ .

3) IT Underground

Ani nejlepší antivirové programy neochrání vaši firmu před počítačovými hackery! Chcete se dozvědět, jak zajistit bezpečné fungování vašich informačních systémů? Opravdu je váš Linux čistý? Víte už všechno o bezpečnosti Ajaxu? Slyšeli jste o Bluebag?

Přijeďte do Varšavy a využijte příležitost mluvit s předními odborníky jako jsou Fyodor Yarochkin, Saumil Shah anebo Claudio Merloni!

IT Underground se koná 26.-27. října 2006 ve Varšavě.
Podrobnosti najdete na http://www.itunderground.org

E. O čem jsme psali v říjnu 1999 – 2005

Crypto-World 10/1999

Crypto-World 10/2000

Příloha : ZoEP.htm

Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

Crypto-World 10/2001

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)
(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 10/2002

Crypto-World 10/2003

Crypto-World 10/2004

Příloha : J.Pinkava - Hashovací funkce v roce 2004 , hash_2004.pdf

Crypto-World 10/2005

Příloha : Další informace k článku V.Klímy - prilohy.zip (53 kB)
(Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

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

3. Redakce

E-zin Crypto-World

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

4. Spojení (abecedně)

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