Elektronické pasy

Zdeněk Říha, FI MU

Od září letošního roku dostávají občané ČR do rukou zcela nové typy cestovních dokladů. Jedná se o tzv. elektronické pasy, u nichž byla uplatněna řada moderních technologií z oblasti informatiky a výpočetní techniky. Pojďme se podívat na naše nové elektronické pasy podrobněji.

1 Úvod

Cestovní pas je identifikační doklad, který slouží především k překračování hranic. Při hraniční kontrole se kontroluje, jednak zda pas je opravdu originál (ne padělek) a nebyl neautorizovaně modifikován, jednak zda podoba držitele přibližně odpovídá fotografii v pase (pas patří jeho držiteli). Dále je možné kontrolovat právo osoby překročit hranice (zda dotyčná osoba např. nebyla obviněna nebo odsouzena) a hledat tak patřičné záznamy v databázích (například Interpol provozuje databázi ukradených a ztracených pasů). Ruční přepisování údajů z pasu je však pomalé a relativně chybové, proto je výhodné získat některé údaje z pasu automatizovaně.

Dlouhou dobu byla jedinou automatizací strojově čitelná zóna, které umožňovala pomocí počítačového rozpoznání znaků digitalizovat 2 řádky na straně s osobními údaji, které obsahují základní informace jako jméno, příjmení a datum narození. Nedávno však bylo na úrovni ICAO (Mezinárodní organizace pro civilní letectví) standardizováno rozšíření pasů o čip [4]. I když na celosvětové úrovni zatím nebylo o povinném zavedení čipů do pasů rozhodnuto, Evropská Unie určila, že všechny členské státy musí zavést pasy s čipem nejpozději 28. srpna 2006. Z toho důvodu jsou tyto pasy od září vydávány i u nás. V dalších částech článku popíšeme, jaké technologie jsou u elektronických pasů využity.

2 Elektronické pasy

Při kontrole pasu je třeba ověřit, zda se jedná o originál cestovního dokumentu vydaný patřičnou autoritou, a že dokument nebyl od vydání neoprávněně pozměněn. Z tohoto důvodu je pas chráněn vůči snadnému padělání, a obsahuje celou řadu ochranných prvků, které je při použití běžně dostupných technologií obtížné napodobit. Mezi klasické ochranné prvky patří speciální papír, vodoznak, ochranný kovový proužek, speciální barvy, mikrotisk, prvky viditelné pouze pod ultrafialovým světlem apod.

Protože množství dat v MRZ (strojově čitelné zóně) je velmi malé (88 znaků) a jejich jediným bezpečnostním prvkem je kontrolní kód, hledaly se nové způsoby uložení dat pro automatizované zpracování. Nová verze standardu ICAO 9303 z roku 2003 využívá technologie bezkontaktních čipových karet, asymetrické kryptografie a do jisté míry i biometrie.

Nové pasy vybavené bezkontaktními čipy se nazývají *elektronické pasy*. Čip včetně antény je obvykle integrován v papírovém obalu pasu (možná jsou však i jiná umístění).

Bezkontaktní čipové karty nevyžadují kontakt se čtecím zařízením, používají rychlé komunikační protokoly, a moderní čipy disponují jak relativně velkou pamětí (desítky kB) tak i rychlými procesory včetně kryptografických koprocesorů. Pro použití v elektronických pasech byl organizací ICAO vybrán protokol ISO 14443 [3], který umožňuje komunikaci na předpokládanou vzdálenost 0-10 cm. Standard připouští dva druhy zařízení, označují se typem A nebo B a liší se v řadě technických parametrů včetně komunikačního protokolu. Pro použití v elektronických pasech je možné použít kterýkoliv z těchto typů.

Bezkontaktní čipy patří mezi tzv. RFID zařízení. RFID (Radio Frequency Identification) je společný název pro technologie přenášející data pomocí elektromagnetického pole. V oblasti RFID existuje celá řada standardů; liší se především použitou frekvencí a vzdáleností, na kterou jsou zařízení schopna komunikovat. V principu existují dvě kategorie RFID zařízení: aktivní a pasivní. Aktivní zařízení mají vlastní zdroj energie a mohou tak komunikovat na delší vzdálenost a používat komplikovanější procesory. Pasivní zařízení naopak žádný vlastní zdroj energie nemají, a jsou tak odkázána na energii získanou indukcí z elektromagnetického pole generovaného snímačem. Vzhledem k omezené době životnosti

baterií napájejících aktivní RFID zařízení a naopak relativně dlouhé době platnosti pasů (10 let) připadají pro využití v pasech v úvahu pouze pasivní RFID čipy.

Data nacházející se v elektronickém pasu musí být *digitálně podepsána* vydávající institucí. Toto je významný bezpečnostní prvek, neboť i v případě, kdy padělatel bude mít k dispozici nejmodernější technické vybavení pro vytištění a personalizaci pasu (a tyto technologie jsou opravdu stále dostupnější), nebude moci bez patřičného soukromého klíče vytvořit správný digitální podpis padělaných dat. Tento způsob ochrany dat digitálním podpisem se nazývá *pasivní autentizace* a je povinnou součásti všech elektronických pasů. Pasivní autentizace však nemůže zabránit vytváření přesných kopií dat (tzv. klonování); pro zabránění takovému jednání je možné využít další mechanismy (biometriky a aktivní autentizaci, viz dále). Hierarchie infrastruktury veřejných klíčů je jednoúrovňová [2]. Každý stát vytváří svou národní certifikační autoritu, která podepíše klíče autorit vydávajících dokumenty – tyto autority pak podepisují data v elektronických pasech. Pro zpřístupňování certifikátů jednotlivých autorit vydávajících dokumenty vytvoří ICAO speciální infrastrukturu. Řešit je třeba i CRL (seznamy odvolaných certifikátů), ty vydávají státy maximálně jednou za 90 dnů, v případě incidentu (tj. prozrazení soukromého klíče) musí CRL distribuovat do 48 hodin (CRL se mezi státy distribuují primárně bilaterálně, sekundárně opět pomocí infrastruktury ICAO). Zajímavý je i fakt, že kompromitace klíče neznamená automatickou neplatnost VŠECH dokumentů podepsaných tímto klíčem, ale jen implikuje zvýšenou pečlivost při kontrole takových dokumentů.

Elektronické pasy mají však i své *nevýhody a rizika* [6]. Ty většinou souvisejí s využitím bezkontaktní technologie přenosu dat. Předně je možné vzdáleně detekovat existenci pasivního RFID čipu, aniž bychom s ním museli nějak komunikovat. Takto může například zloděj zjistit, že v něčí kabelce se nachází RFID a zaměřit se právě na tuto kabelku. Za druhé lze i bez přístupu k datům na čipu zjistit některé informace o použitém čipu samotném. Například antikolizní algoritmy umožňují zjistit číslo čipu ještě dříve, než začneme s čipem komunikovat. Podobně se dá podle některých nestandardních chybových návratových kódů zjistit výrobce nebo typ čipu, a tím pravděpodobně i stát vydávající pas. Takovou informaci pak mohou například zneužít teroristé při konstrukci bomby, která se sama aktivuje, bude-li v blízkosti osoba s pasem vydaným určitou zemí nebo určitou množinou zemí. Nebo může být možné sledovat na základě čísla čipu konkrétní osobu. Obě tyto nevýhody (tj. zjištění existence RFID a jeho čísla) je možné eliminovat využitím tzv. Faradayovy klece neboli umístěním čipu do kovového obalu – například hliníkového přebalu. Takto nebude možné čip detekovat ani s ním nijak komunikovat, dokud pas nevyndáme z tohoto obalu (v případě kovového přebalu pasu dokud jej neotevřeme). Takovýto obal ale nemůže zabránit neautorizovanému odposlechu, jakmile ke komunikaci dojde.

Pokud elektronický pas nevyužívá dodatečných ochranných mechanismů (jejich použití však není celosvětově povinné), lze data z elektronického pasu přečíst bez jakékoliv autentizace, komunikace mezi čtečkou a čipem není šifrovaná. Z důvodu velkých obav z nepozorovatelného neautorizovaného čtení dat z čipu v pasu bylo třeba implementovat nějaký způsob řízení přístupu k datům. Protože však základní data musí být čitelná pohraničními úředníky libovolného státu (včetně těch nepřátelských), bylo by opravdu těžké implementovat systém správy tajných (šifrovacích nebo autentizačních) klíčů tak, aby zmínění úředníci (případně jiné autorizované složky) mohli data z pasu získat, ale nikdo jiný ne. Proto bylo rozhodnuto implementovat systém, který umožní přístup k datům komukoliv, kdo je schopen přečíst některé údaje ze stránky s osobními údaji. Protože autentizace vyžaduje znalost těchto údajů z pasu a tyto údaje je možné získat až po otevření pasu, dá se předpokládat, že úspěšnou autentizací projde pouze ten, kdo má pas v ruce (tedy pouze s vědomím držitele pasu). Konkrétně to vypadá tak, že se vezme číslo pasu, datum narození držitele a datum vypršení platnosti pasu (všechny 3 údaje včetně kontrolních číslic) a tento řetězec se hašuje funkcí SHA-1 pro získání dvou 3DES

klíčů, které se využijí na autentizaci a ustavení společného šifrovacího klíče, kterým je zabezpečena následná komunikace. Takto je celá komunikace chráněna i proti odposlechu. Tento způsob zabezpečení přístupu k datům na čipu se nazývá *základní řízení přístupu* (Basic Access Control, BAC) a podle rozhodnutí Evropské komise K(2005) 409 je jeho implementace povinná u všech pasů vydávaných členskými zeměmi. Tedy i české pasy jsou takto chráněny.

Nevýhodou tohoto základního řízení přístupu je malá entropie v datech, která jsou použita pro autentizaci. Ačkoliv teoretické maximum je asi 56 bitů (datum narození z období max. 100 let, tj. asi 15 bitů, datum platnosti max. 10 let, tj. asi 11 bitů, 9 číslic čísla pasu, asi 30 bitů) případně až 73 bitů u alfanumerických čísel dokumentů, nejsou všechny hodnoty stejně pravděpodobné a díky dodatečným znalostem je možné provést útok podstatně úspěšněji než jen náhodným zkoušením všech možností. Zvláště znalost rozsahu čísel pasů může útok značně zrychlit. Se znalostí číslovacího plánu pasů a dalším omezením rozsahu testovaných hodnot klesá entropie na přibližně 35 bitů. To je sice stále hodně na provedení on-line útoku vůči pasu (tj. zkoušením všech možností při skutečné komunikaci s čipem pasu), pokud se nám však podaří odposlechnout úspěšnou komunikaci, můžeme později provést off-line útok, při kterém se nám podaří získat klíč, kterým byla šifrována komunikace, a tak dešifrovat obsah přenášených dat. Pro znesnadnění takových útoků je možné vnést do sériových čísel pasů více náhodnosti.

Využití digitálního podpisu pro ochranu integrity dat ještě neznamená, že útočník nemůže přečíst všechna data včetně relevantních podpisů a vytvořit čip, do kterého uloží právě tato data. Zabezpečení pasu klasickými bezpečnostními prvky (tiskové technologie apod.) a kontrola, zda data uložená na čipu korespondují s daty vytištěnými v MRZ, stále hrají svoji roli. To však pořád nezabrání kompletním kopiím pasů včetně vytištěných údajů. Proti tomuto útoku mohou být elektronické pasy vybaveny technologií, která se nazývá *aktivní autentizace*. V čipu pasu je bezpečně uložen soukromý asymetrický klíč. Tento klíč čip nikdy neopustí (neexistuje příkaz pro přečtení klíče), snímač se pouze může přesvědčit, zda čip má tento klíč k dispozici. Součástí dat uložených na čipu a digitálně podepsaných vydávající autoritou je veřejný klíč čipu (datová skupina 15). Snímač tento klíč přečte a pomocí protokolu výzva-odpověď (konkrétně snímač posílá náhodné číslo, které čip pasu doplní další náhodnou částí a digitálně podepíše) si ověří, zda čip má k dispozici soukromý klíč odpovídající klíči veřejnému. Padělatel tedy nemůže vytvořit kompletní kopii čipu, neboť z původního čipu nemůže získat soukromý klíč. Nemůže ani vytvořit nový pár klíčů, neboť veřejný klíč musí být digitálně podepsán vydávající autoritou (verifikace digitálního podpisu veřejného klíče je tedy důležitým prvkem aktivní autentizace). Nemožnost vyčíst soukromý klíč z čipu je samozřejmě založena na předpokladu dostatečné odolnosti čipu vůči narušení. Pokud by čip nebyl dostatečně odolný a soukromý klíč by bylo možné přečíst, pak by bylo možné vytvářet přesné kopie čipu a ani aktivní autentizace by nemohla odhalit, že se jedná o kopii. Celosvětově i v EU je implementace pouze dobrovolná. České pasy však aktivní autentizaci implementují.

3 Biometrické pasy

Kromě samotného zabezpečení pasu je třeba zjistit, zda pas opravdu patří osobě, která jej předkládá. Tedy zabránit zneužití ukradených a ztracených pasů. Právě z tohoto důvodu je součástí osobních údajů i fotografie držitele. Podobnost držitele s fotografií je typicky prováděna „manuálně“ pohraniční kontrolou, která mívá v porovnávání aktuální podoby s podobenkou jak výcvik tak i zkušenost. Přesto je značná možnost zneužití pasu podobnou osobou. Známá je skutečnost, že lidé těžko rozpoznávají osoby jiné rasy než vlastní (např. Asiaté mají problémy s odlišením Evropanů, Evropané s Afričany apod.).

Uložení biometrických dat do identifikačních dokumentů není úplná novinka, i současné pasy obsahují podpis a fotografii držitele. Před rozšířením fotografických technik (tj. již velmi dávno) pasy obsahovaly slovní popis držitele a v některých obdobích bývaly součástí identifikačních dokumentů i otisky prstů. Co je však nové, je

možnost *automatické verifikace osoby pomocí biometrických technologií* a díky digitálnímu podpisu i vazba biometrických dat na ostatní údaje v pasu.

Možnost biometrické verifikace je významným bezpečnostním faktorem elektronických pasů vybavených biometrickými daty. Ačkoliv fotografii držitele je možné porovnat s osobou předkládající pas i manuálně, automatická biometrická verifikace je přesnější a může být provedena i bez přítomnosti kontrolních orgánů. Zásadní nevýhodou biometrické verifikace založené na srovnávání obličeje je její značná chybovost (ale i tak bývá automatizovaná verifikace přesnější než manuální). V případě řízených světelných podmínek může chybovost (ve smyslu odmítání oprávněných držitelů – FRR) dosáhnout asi 10 % (při 1 % pravděpodobnosti neoprávněného přijetí – FAR). V případě, kde světelné podmínky není možné optimalizovat pro biometrický systém, může chybovost dosáhnout až 50 % [1]. Je zřejmé, že při takové chybovosti není možné každou osobu, která není úspěšně autentizována, důkladně prověřovat. Výhoda využití biometrik tedy vyzní především v případě využití otisků prstů nebo očních duhovek. Přesnost dosahovaná u těchto biometrických technologií je řádově vyšší (FRR kolem 0,5% při FAR 0,1% pro otisky prstů) [1].

Elektronické pasy, které obsahují biometrická data se nazývají *biometrické pasy*. Pro celosvětovou použitelnost je nutné uložit do čipu tvář držitele. Další biometrické charakteristiky (v úvahu připadají pouze otisky prstů nebo snímky oční duhovky) jsou nepovinné, a rozhodnutí, zda je do čipu ukládat nebo ne, je věcí vydávajícího státu. Členské země EU však na základě nařízení Rady (ES) č. 2252/2004 a následných rozhodnutí evropské komise musí začít vydávat biometrické pasy s tváří držitele nejpozději od 28. srpna 2006, s otiskem prstu pak od 28. června 2009. Otisky prstů musí být chráněny mechanismem rozšířeného řízení přístupu (Extended Access Control – EAC). Evropské EAC je však zatím pouze ve fázi návrhu a diskuzí. Podstatou EAC je omezit přístup k citlivým biometrickým datům pouze na pohraniční kontroly (a další autorizované instituce) přátelských zemí, pro začátek pouze zemí EU. České elektronické pasy „první generace“ vydávané od září 2006 obsahují pouze fotografii držitele. Otisky prstů budou do pasů v souladu s evropskou legislativou ukládány až později.

Na skutečnost, zda lze za „pravá“ biometrická data považovat i pouhou fotografii držitele ve formátu JPG/JPG2000, panují různé názory, a podle toho pak termín biometrické pasy buď zahrnuje nebo nezahrnuje současné pasy s pouhou fotografií obličeje. V každém případě je však čip v pase pouhým bezpečným nosičem dat a nemá žádné speciální biometrické vlastnosti. Zajímavý je také fakt, že ačkoliv vydávání elektronických pasů je pro země EU povinné, skutečné využívání čipů na hranicích není zatím nijak upraveno a řada zemí zatím čipy nijak využívat nemíní.

4 Data v pasech

Struktura dat na čipu vychází z běžného souborového systému čipových karet, kde se adresáře nazývají dedikované soubory (DF) a běžné soubory tzv. elementární soubory (EF) [5]. Data jsou uložena v řadě souborů ve společném adresáři. Jeden soubor (EF.COM) je vyhrazen pro metadata (verze formátu dat a seznam přítomných datových skupin), jeden soubor ($EF.SO_D$) obsahuje informace o zabezpečení (digitálně podepsané haše všech souborů) a ostatní soubory jsou určeny pro samotná data, která jsou rozdělena na jednotlivé datové skupiny (Data Groups, DG).

V DG1 je uložena strojově čitelná zóna, podobně jako je vytištěna i v pase. V DG2-7 mohou být uloženy biometrické údaje (portrét, otisk prstu, oční duhovka, podpis). DG8-10 popisují bezpečnostní prvky (papírové části) pasu, formát dat však zatím není standardizován. DG11 obsahuje dodatečné data o držiteli a DG12 data o vydavateli pasu. DG13 je určeno pro interní použití vydávajícího státu. DG14 je rezervováno pro další použití (v podstatě již bylo přiděleno pro rozšířené řízení přístupu), DG15 obsahuje veřejný klíč pro aktivní autentizaci. V DG16 mohou být uloženy adresy příbuzných pro podání zprávy v případě nehody.

5 České pasy

Evropský termín 28. srpna 2006 na zavedení elektronických pasů se snímkem tváře držitele se vztahuje i na Českou republiku. Využity jsou čipy P5CT072 firmy Philips (72kB EEPROM paměti) s OS Axalto AXSEAL. Pasy obsahují povinné datové skupiny DG1 (strojově čitelná zóna) a DG2 (snímek obličeje). Snímek držitele bude ukládán pravděpodobně ve formátu JPG (finální rozhodnutí nebylo v době psaní článku známo) bez dodatečných biometrických dat. V souladu s evropskými požadavky jsou data chráněna pomocí základního řízení přístupu. České elektronické pasy však budou implementovat i aktivní autentizaci (veřejný klíč je uložen v DG15). Otisky prstů (a s nimi související rozšířené řízení přístupu) zatím nejsou využívány. Po personalizaci čipu je čip uzamknut a žádná další modifikace dat není možná (ani ze strany vydávající instituce).

6 Závěr

Hlavní výhodou elektronických resp. biometrických pasů je jejich vyšší bezpečnost. Tato vyšší bezpečnost se však projeví až v delším horizontu, neboť potrvá nějakou dobu, než budou hraniční přechody vybaveny odpovídající verifikační technologií. Navíc lze očekávat, že se padělatelé soustředí na starší pasy, jejichž platnost nebyla zavedením elektronických pasů omezena, a na pasy států, které elektronické pasy zatím vydávat nebudou. Je také pravděpodobné, že nebude možné biometricky verifikovat všechny osoby překračující státní hranice, ale pouze náhodné (nebo jinak vybrané) případy, lety apod. V každém případě bude padělání elektronických pasů ztíženo a u biometrických pasů bude těžší i jejich zneužití po nalezení/ukradení, což je dobrá zpráva nejen pro vládní instituce, ale i všechny držitele pasů.

Mezi nevýhody elektronických pasů patří především vysoké náklady na zavedení patřičné technologie (jak na vydávání pasů tak i na kontrolu pasů a osob) a problémy související s možným narušením soukromí držitelů (vzdálená čitelnost dat, ukládání biometrických dat).

Protože současné elektronické pasy jsou navrženy tak, aby byly čitelné na celém světě, stačí k přečtení a zobrazení dat libovolná kompatibilní čtečka, patřičné softwarové vybavení a některé údaje ze strojově čitelné zóny. Bezkontaktní čtečku čipových karet máme k dispozici i na FI v Laboratoři bezpečnosti a aplikované kryptografie (LaBAK). Chcete-li si tedy ověřit jaká data se nacházejí ve vašem elektronickém pase, zastavte se v naší laboratoři (místnost C517).

Poznámka na závěr: Článek byl připraven s použitím [7]. Názory v něm uvedené jsou soukromými názory autora a nemohou být považovány za oficiální stanovisko Evropské komise, kde autor v současné době působí v Joint Research Center, Ispra.

Literatura

[1] G. M. Ezovsky: Biometric Passports: Policy for International and Domestic Deployment. Journal of Engineering and Public Policy. Vol. 9, 2005.

[2] ICAO, MRTD: PKI for Machine Readable Travel Documents offering ICC Read-Only Access

[3] ICAO: ICAO 9303 specification. Včetně Supplement – 9303, 2005-4 V3.0

[4] ICAO TAG MRTD/NTWG: Biometrics Deployment of Machine Readable Travel Documents, version 2.0. Včetně příloh A-J, `http://www.icao.int/mrtd/download/documents/`

[5] ICAO: Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technologies, V 1.7, `http://www.icao.int/mrtd/download/documents/`

[6] Ari Juels, David Molnar, David Wagner: Security and Privacy Issues in E-passports

[7] Zdeněk Říha, Ioannis Vakalis: Elektronické pasy. Data Security Management, ročník X, číslo 3, ISSN 1211-8737, 2006. □