B. Bezpečnost elektronických pasů, část II.

Zdeněk Říha, Masarykova Univerzita a JRC EC Ispra, (zriha@fi.muni.cz)
Petr Švenda, Masarykova Univerzita, (xsvenda@fi.muni.cz)
Václav Matyáš, Masarykova Univerzita, (matyas@fi.muni.cz)

V prvé části [4] jsme diskutovali vlastnosti elektronických pasů první generace, tedy těch pasů, které jsou vydávány v současné době a které obsahují biometrická data jen ve formě snímků obličeje držitele (uložených v DG2). Biometrické systémy založené na srovnávání obličejů jsou však značně chybové a pro přesvědčivější a přesnější verifikaci (případně identifikaci[1]) osob je nutné využít jiných (silnějších) biometrických technologií. Standardy organizace ICAO v oblasti elektronických pasů podporují ukládání otisků prstů (DG3) a snímků očních duhovek (DG4). Jejich uložení v pasech je zatím na celosvětové úrovni dobrovolné. Evropská komise však ve svém rozhodnutí K(2005) 409 rozhodla, že nejpozději od 28. června 2009 musí členské státy ukládat do elektronických pasů i otisky prstů ve formátu WSQ (ztrátová komprese optimalizovaná pro snímky otisků prstů).

Biometrická data ve formě otisků prstů nebo snímků duhovek jsou považovány za citlivější údaje než snímky obličejů, a to z důvodu jejich podstatně přesnějších identifikačních možností. Standardy ICAO proto doporučují dodatečná ochranná opatření pro přístup k těmto citlivým datům a rozhodnutí Evropské komise, které nařizuje ukládání otisků do elektronických pasů, činí ochranná opatření (tzv. rozšířené řízení přístupu) povinnými. Jak však tato ochranná opatření vypadají? Standardy ICAO jsou v této oblasti značně vágní a detaily nechávají na jednotlivých státech. Jen jako příklad uvádějí šifrování dat nebo rozšířené řízení přístupu pracující na stejném principu jako základní řízení přístupu s tím, že symetrický autentizační klíč je tajný [1]. V některých dokumentech zmiňují dokumenty ICAO i rozšířené řízení přístupu založené na PKI, žádné detaily však nejsou rozpracovány. Prvotní rozhodnutí Evropské komise vyžadující ochranu citlivých dat v pasech (K(2005) 409) žádné bližší detaily o rozšířeném řízení přístupu neuvádí, další rozhodnutí Evropské komise v této oblasti (K(2006) 2909) se jen odkazuje na technickou zprávu německého BSI [3]. Tato technická zpráva od té době doznala několika změn a řada detailů protokolu se stále diskutuje.

Pojďme se nyní podívat na jednotlivé teoretické možnosti ochrany citlivých biometrických dat v elektronických pasech. Nejdříve krátce zmíníme dva fundamentální přístupy k celému problému: on-line a off-line přístup. Principielním rozdílem mezi základním řízením přístupu a dodatečnou ochranou citlivých biometrických dat je okruh autorizovaných subjektů, které mají mít přístup k daným datům. Zatímco u základních dat uložených v elektronických pasech je nutné umožnit přístup pohraničníkům všech zemí včetně těch nepřátelských a klíč tak nemůže být skutečně utajen (a u základního řízení přístupu je autentizační klíč v podstatě vytištěn v pase, viz minulý díl), u ochrany citlivých biometrických údajů je okruh subjektů s přístupem značně omezen a tak je možné přístupové klíče lépe chránit a umožnit přístup právě cílové skupině autorizovaných subjektů. Tuto skupinu navíc definuje právě vydavatel dokumentu. Pro přístup k citlivým biometrickým datům jsou tedy nutná tajná autentizační

[1] Jak státy naloží s biometrickým daty získanými pro uložení do pasu je jejich rozhodnutí, na celoevropské úrovni však žádná centrální databáze nevzniká. Česká republika otisky prstů po jejich uložení v pase po krátké době z ostatních úložišť maže, otisky prstů tak lze využít pouze k verifikaci držitele pasu, identifikace osob není možná.

data a nejrůznější metody ochrany biometrických dat v pasech se vlastně zabývají správou těchto tajných klíčů. V principu existují dvě metody správy tajných klíčů a podle typu přístupu ke klíči se nazývají on-line a off-line metody.

V případě on-line režimu jsou tajné klíče (ať už tajné symetrické nebo soukromé asymetrické) umístěny na centrálním serveru (nebo několika málo serverech). Výhodou je relativně snadná ochrana těchto klíčů, neboť chránit je třeba jen několik takových lokalit a při budování takovýchto centrálních bodů je možné s výhodou využít již existujících zabezpečených lokalit. Nevýhodou je nutnost on-line připojení všech inspekčních systémů. To znamená nejen zvýšené náklady na připojení všech míst, kde se budou pasy kontrolovat (navíc v případě některých vzdálených lokalit to může být až neřešitelný problém (například některé ostrovy)), ale také kompletní závislost na tomto připojení. V případě výpadku připojení inspekčního systému k centrálnímu serveru s klíčem nemá inspekční systém žádnou možnost čtení citlivých biometrických dat z pasů. Je zřejmé, že výpadky připojení mohou být způsobeny i úmyslně a připojení je pak kritickým prvkem celého systému. V případě off-line systémů jsou všechny nutné tajné klíče uloženy v každém inspekčním systému, což znamená nezávislost na centrálním systému, ale problém s ochranou tajných klíčů na velkém množství míst (a zvýšenou možnost kompromitace klíčů). Možné jsou i kombinace obou přístupů, pak se kombinují výhody i nevýhody obou přístupů.

Pojďme se nyní podívat na možné principy ochrany citlivých biometrických dat v pasech.

Symetrické metody

V případě využití symetrických šifrovacích metod můžeme buďto data v pase ukládat nešifrovaně a přístup k nim vázat na autentizační schéma založené na symetrické šifře nebo data šifrovat, ukládat šifrovaně a pak se již nestarat o přístup k nim.

Symetrický klíč musí být jiný pro každý pas, klíče mohou být buďto zcela náhodné nebo odvozené z hlavního klíče pomocí nějakého diversifikačního algoritmu (například zašifrováním čísla dokumentu pomocí hlavního klíče získáme klíč specifický pro tento pas). V každém případě potřebujeme minimálně jeden klíč pro každý stát, pravděpodobněji jeden klíč pro každého vydavatele pasu (např. kraje, ambasády apod.) a klíč by měl být pravidelně (např. měsíčně, ročně) aktualizován (pro aktuálně vydávané pasy). Inspekční systém pak musí mít přístup ke všem klíčům nutným pro přístup ke všem platným pasům (tj. až deset let) řady zemí. U off-line systémů se jedná o velké množství velice citlivých klíčů, které by musely být ukládány v každém inspekčním systému a kompromitace byť i jediného inspekčního systému by znamenala okamžitý i budoucí přístup útočníka k biometrickým údajům všech pasů platných v době krádeže. U on-line systémů jsou klíče dobře fyzicky chráněny, chránit je však nutné i přístup k centrálnímu systému, v případě incidentu s neautorizovaným přístupem k serveru je však zotavení snadné – stačí ukončit možnost neautorizovaného využití sítě.

Výhodou symetrické autentizace nebo šifrování jsou malé nároky na výpočetní sílu čipu v pase. Symetrická autentizace je součástí základního řízení přístupu (BAC), rozšířené řízení přístupu by pak bylo zcela stejné, jen založené na klíči, který je skutečně tajný. V případě ukládání šifrovaných dat nejsou nároky na čip žádné, neboť pro pas jsou šifrovaná data transparentní a přístup k nim nemusí nijak řídit. V případě, kdy jsou tajné klíče udržovány v tajnosti (což však není triviální), je takové řešení bezpečné.

Nevýhodou je velké množství klíčů, které je třeba uchovávat v tajnosti (u off-line řešení dokonce na každém koncovém inspekčním systému). Tajné klíče navíc mají dlouhou dobu platnosti/použitelnosti a není možné je revokovat (neboť se nacházejí ve velkém množství pasů). Získání takových klíčů znamená přístup ke všem dosud vydaným pasům. Bezpečnostní nevýhodou šifrovaně ukládaných dat bez ochrany řízením přístupu je možnost získání šifrovaných dat a provádění off-line útoků (třeba i paralelních), což je samozřejmě podstatně mocnější zbraň než provádění on-line útoků na autentizaci vůči pasu. Při vhodně zvolené délce šifrovacího klíče a šifrovacího algoritmu by to však neměl být problém tak jako tak.

Asymetrické přístupy

Jinou možností je provést autentizaci čtečky pomocí autentizace založené na PKI. Cílem je limitovat počet tajných (soukromých) klíčů na straně čtečky a limitovat možnost zneužití těchto klíčů v případě jejich kompromitace. Ačkoliv možností, jak implementovat rozšířené řízení přístupu pomocí PKI, by mohlo být více, budeme se zde držet návrhu německého BSI [3].

Podle tohoto návrhu (pro tzv. autentizaci terminálu) každá země zřídí CV (Country Verifying) certifikační autoritu, která bude vydáváním certifikátů určovat kdo (které jiné země) bude mít přístup k citlivým biometrickým datům této země. Certifikát této autority je uložen v pase a je počátečním bodem (kořenovým certifikátem) řízení přístupu. Dále země, které budou chtít přistupovat k citlivým biometrickým údajům (ať už ve vlastních pasech nebo pasech jiných zemí), musí zřídit DV (Document Verifier) certifikační autoritu. Ta získá certifikát od všech zemí, které ji dovolí přistupovat k datům v jimi vydávaných pasech. Tato DV CA pak bude vydávat certifikáty koncovým entitám přistupujícím k biometrickým datům (tzv. inspekčním systémům – IS).

V pase je pak uložen CVCA certifikát vydávající země (např. ČR). Pokud čtečka (například italská) chce přesvědčit pas o tom, že je autorizovaná pro přístup k citlivým biometrickým datům, musí ukázat certifikát DV (v našem případě Itálie) podepsaný správnou vydávající CVCA (tedy českou) a svůj IS certifikát (pro toto konkrétní zařízení) podepsaný DV certifikační autoritou (v našem příkladě italskou). Jakmile pas celý tento certifikační řetěz ověří, musí ještě zjistit, zda inspekční systém (čtečka) má k dispozici soukromý klíč, jehož veřejná část je certifikována. To se provede pomocí protokolu výzva-odpověď. Pokud toto vše proběhne v pořádku, může následně čtečka přistupovat k citlivým biometrickým datům (tedy DG3 a/nebo DG4).

Výše uvedený postup je mírně komplikován aktualizacemi CVCA certifikátů, pro které se vydávají tzv. linkovací certifikáty (pokud má pas uložen starý CVCA certifikát, je třeba nejprve předložit (a v pase verifikovat) překlenovací linkovací certifikáty). Kromě autentizace terminálu německý návrh dále zavádí autentizaci čipu, která jednak odstraňuje nevýhodu malé entropie BAC (a tedy dešifrovatelnosti komunikace), neboť výsledkem je nový šifrovaný kanál, a jednak také nahrazuje aktivní autentizaci, neboť při ní je ověřen přístup k čipu k tajné informaci (jejíž veřejná část je uložena v DG14 a je tedy součástí digitálního podpisu dat v pase). Pojďme se nyní podívat na jednotlivé protokoly podrobněji.

Autentizace čipu

Inspekční systém získá z čipu pasu veřejnou část Diffie-Hellman (podporovaný je klasický DH podle PKCS #3 a DH založený na eliptických křivkách podle ISO 15946) klíčového páru spolu s doménovými parametry (uloženo v DG14). Dále inspekční systém vygeneruje svůj dočasný (právě pro jedno sezení platný) DH pár klíčů (se stejnými doménovými parametry jako klíč čipu) a pošle jej čipu (příkazem Manage Security Environment – Set for Computation – Key Agreement Template). Jak čip, tak i inspekční systém nyní na základě údajů, které mají k dispozici, mohou odvodit sdílené tajemství. Toto tajemství se využije ke konstrukci klíče (resp. klíčů – pro šifrování a MAC) sezení, který bude použit pro zabezpečení následné komunikace přes Secure Messaging (a SSC (Send Sequence Counter – čítač zpráv použitý pro zabránění přehrání zpráv) se nyní nuluje). Znalost správného klíče se tedy potvrdí možností následné úspěšné komunikace.

Výsledkem je ustavení nového šifrovacího kanálu (odstraňuje se tak nedostatečnost BAC) a autentizace čipu (nahrazuje se tak aktivní autentizace, pas však přesto může aktivní autentizaci podporovat, aby bylo možné ověřit autenticitu čipu i na systémech, které nejsou kompatibilní s rozšířeným řízením přístupu a podporují pouze protokoly standardizované organizací ICAO).

Autentizace terminálu

Během autentizace terminálu musí čtečka (inspekční systém) přesvědčit čip v pase, že je autorizována pro přístup k citlivým biometrickým datům. Počáteční bod důvěry je certifikát CVCA, který je do pasu nahrán při jeho personalizaci. Při autentizaci terminálu musí čtečka pasu předložit certifikační řetěz, začínající certifikátem CVCA v pase uloženým a končícím certifikátem inspekčního systému (odesílá jej příkazy Manage Security Environment – Set for verification – Digital Signature Template a Perform Security Operation – Verify Certificate). Tento certifikační řetěz může v případě potřeby obsahovat i linkovací certifikáty, v takovém případě pas (po jejich ověření) aktualizuje CVCA certifikát za nový (vzhledem k možnému překrytí časové platnosti CVCA certifikátů mohou v jeden okamžik být platné i dva CVCA certifikáty, v takovém případě jsou jako aktuální uloženy oba). Ostatní certifikáty (tedy certifikát pro DV vydaný CVCA a pro IS vydaný DVCA) jsou po ověření ukládány jen dočasně a slouží pouze k ověření celého certifikačního řetězce. V případě úspěšného ověření řetězce pas získá veřejný klíč inspekčního systému a jeho přístupová práva. Ta jsou v současném návrhu pouze dvě a to přístup k DG3 (otisky prstů) a DG4 (oční duhovka). Výsledná práva se získají jako bitové AND těchto práv v celém certifikační řetězci.

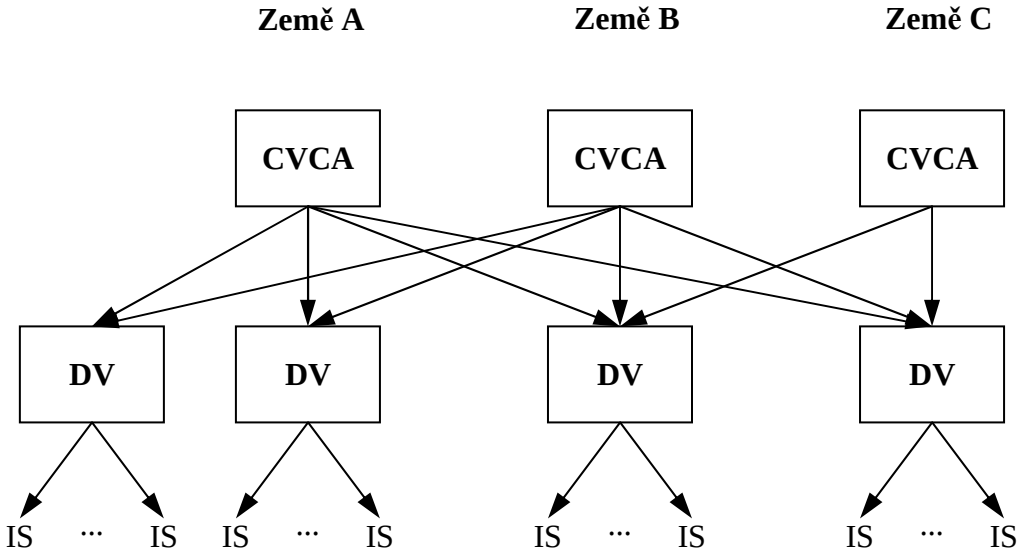
Po získání veřejného klíče inspekčního systému je třeba ověřit, zda inspekční systém má přístup k odpovídajícímu soukromému klíči. To provedeme pomocí protokolu výzva-odpověď. Nejprve inspekční systém získá 8-bajtovou náhodnou výzvu (příkazem GET CHALLENGE), tu digitálně podepíše (podepisuje ve skutečnosti zřetězené číslo pasu, náhodné číslo čipu a haš dočasného DH klíče čtečky (z předchozí autentizace čipu)) a příkazem EXTERNAL AUTHENTICATE posílá čipu k verifikaci. Pokud proběhne verifikace úspěšně, je čtečka autentizována a může přistupovat k DG3 nebo DG4 podle vypočítaných přístupových práv. Předpokladem autentizace terminálu je provedená

autentizace čipu. Autentizace terminálu není povinným prvkem komunikace s pasem. Pokud nezamýšlíme číst z pasu citlivá biometrická data, můžeme autentizaci čtečky vynechat.

Pro autentizaci terminálu jsou podporována následující schémata: RSASSA-PKCS#1_v15 (v kombinaci s SHA-1 a SHA-256), RSASSA-PSS (v kombinaci s SHA-1 a SHA-256) a ECDSA (v kombinaci s SHA-1, SHA-224 a SHA-256). Teoreticky je možné pro jeden pár klíčů vydat certifikáty různých CVCA, DV a tím minimalizovat celkový počet párů klíčů a certifikátů. Různé pasy/CVCA však mohou využívat jiných podpisových schémat a tak teoretický maximální počet klíčů, který může být umístěn na inspekčním systému je dán počtem povolených schémat, tedy 7.

Protože výpočetní síla čipových karet je omezená, jsou místo klasických X.509 certifikátů používány certifikáty zjednodušené, tzv. kartou verifikovatelné (card verifiable – CV) certifikáty. Zajímavé je ověřování časové platnosti certifikátů. Čip totiž nemá vlastní hodiny a tak jediné, co mu zbývá, je využít datum vydání certifikátů. Pokud čip úspěšně ověří platnost certifikátu vydaného určitého dne, ví, že toto datum už jistě nastalo, a může tak aktualizovat svůj časový odhad na tuto hodnotu (tedy pokud je novější, než hodnota dosud uložená). Je zřejmé, že pokud by nějaká CV CA nebo DV CA vydala (ať už omylem, cíleně nebo jako výsledek nějakého útoku) certifikát s datem vydání v budoucnosti, pas by pak odmítal i aktuální certifikáty a byl tak prakticky nepoužitelný. Z důvodu rizika takových útoků se pro aktualizaci interního odhadu data používají pouze CVCA, DV a domácí IS certifikáty.

PKI



Jak již bylo zmíněno, zřizuje každá země CV CA a ta pak určuje, které jiné země budou mít přístup k datům v pasech vydávaných touto zemí. Každá země, která chce přistupovat ke chráněným datům, musí zřídit DV CA a požádat CV CA všech zemí, k jejichž chráněným datům chce přistupovat, o vydání certifikátu touto CV CA pro DV CA. DV CA pak vydává certifikáty jednotlivým inspekčním systémům, kterých mohou být například desítky až tisíce. Pokud se někdo neautorizovaně zmocní inspekčního systému, může pomocí něho číst data z chráněných pasů a to z pasů zemí, pro které daná DV CA získala certifikát od CVCA a po dobu platnosti certifikátu tohoto inspekčního systému (resp. u málo používaných pasů, které

nemají uloženu příliš přesnou aproximaci data i později). Doba, na kterou jsou vydávány certifikáty inspekčním systémům, je tedy jedním z klíčových parametrů bezpečnosti celého systému. Je zřejmé, že čím kratší je tato doba, tím menší užitek bude mít útočník z ukradených či jinak neautorizovaně získaných inspekčních systémů. Konkrétní doba platnosti certifikátů bude záviset na domluvě jednotlivých CA, například doba platnosti certifikátu pro DV CA vydaného CV CA by mohla být roční a doba platnosti IS certifikátů vydávaných DV CA by mohla být měsíční nebo týdenní. Pomocí řešení založeného na on-line přístupu by bylo možné se vyvarovat problémů s ukradenými inspekčními systémy (ať už přesměrováním autentizace nebo aktuálními CRL), toto však nebylo akceptovatelné pro všechny země EU, neboť ne všechna inspekční místa lze vždy spolehlivě propojit on-line s centrem. Z tohoto důvodu je v EU zvažován off-line systém, kde každé inspekční zařízení může mít k dispozici svůj pár klíčů a jemu odpovídajících certifikátů. S CRL se v diskutovaném schématu nijak nepočítá. I přesto je však možné například na úrovni země implementovat on-line režim tak, že inspekční systém má daná země vlastně jen jeden a všechna kontrolní místa s přístupem ke chráněným datům jsou vybavena terminály, které svoje požadavky na autentizaci on-line přesměrují na centrální inspekční systém. Takové řešení pak má klasické výhody a nevýhody centrálního on-line přístupu (tj. snadnější ochrana tajných klíčů, ale závislost na připojení). Vzhledem k faktu, že bezpečnost systému jako celku je dána nejslabším článkem, může být při off-line přístupu problematická například ochrana klíčů na vzdáleném ostrově.

Mezi nevýhody takto definovaného rozšířeného řízení přístupu patří především zneužitelnost ukradeného inspekčního systému (samozřejmě záleží na detailech ochrany klíčů) po dobu platnosti certifikátu pro tento IS (řešení tohoto problému by vyžadovalo kompletní on-line přístup) a značně náročná (jak finančně, tak i organizačně) režie související s použitým PKI.

Celosvětová interoperabilita v oblasti rozšířeného řízení přístupu není nutná, neboť citlivá data by měla být přístupná jen na základě vzájemných dohod států a je na těchto státech, aby se domluvily na technických detailech v rámci mantinelů stanovených standardy ICAO. Lídrem v oblasti EAC je v současné době EU, která navrhla (vlastně německé BSI) protokol pro EAC a diskutuje jeho detaily tak, aby členské země mohly nejpozději od 28. června 2009 začít ukládat otisky prstů do pasů a chránit je pomocí rozšířeného řízení přístupu. Rozhodnutí Evropské komise o povinnosti ukládat otisky prstů, a tyto chránit pomocí EAC, se odkazuje na technickou zprávu BSI, ta však není v některých detailech zcela jednoznačná. Úkol detailněji specifikovat případné problematické body má tzv. Výbor podle článku 6 (Article 6 committee podle čísla článku, kterým byl zřízen – původně ke stanovení společného postupu v oblasti víz) a ten pro svá rozhodnutí využívá doporučení skupiny BIG (Brussels Interoperability Group), která pravidelně zasedá a řeší aktuální otázky v oblasti elektronických pasů. Ve dnech 6. a 7 prosince 2006 proběhl v italské Ispře workshop, jehož součástí byl první test interoperability. Ačkoliv výsledná interoperabilita jednotlivých národních implementací zdaleka ještě nebyla 100%, pomohl test identifikovat problematická místa v implementacích a na ta se dále soustředit (jedná se o formáty jednotlivých polí, chybějící podpora některých kryptografických algoritmů, APDU s rozšířenou délkou pro příkazy verifikace certifikátu, kde velikost certifikátu přesahuje 260 bajtů apod.).

Dá se očekávat, že pokud se tento protokol úspěšně osvědčí v EU, bude použit i v jiných zemích, případně, že se stane základem pro diskuze ohledně možností zápisu dalších dat na čip (víza, záznamy o přechodech hranic a oprávnění k automatickému přechodu hranic).

Interoperabilita ovšem nespočívá jen v technických detailech, ale také v oblastech důvěry, ochrany citlivých klíčových dat a jiných organizačních záležitostech. Aby se usnadnila vzájemná certifikace CV certifikačních autorit a DV certifikačních autorit jednotlivých členských zemí, vzniká na evropské úrovni certifikační politika, která by měla být minimální (ve smyslu, toto je minimální bezpečnost, která je vyžadována), resp. maximální (tj. země by neměly od ostatních vyžadovat více) požadavky na certifikační politiky DV certifikačních autorit.

Pro začátek se předpokládá, že chráněná biometrická data budou přístupná pouze navzájem mezi zeměmi EU. V diskuzích se však objevují i Spojené státy americké, Kanada a Austrálie jako další možné země zapojené do evropského systému rozšířeného řízení přístupu. Při pohledu na strukturu PKI však vidíme, že je na jednotlivých členských zemích, aby rozhodly, které jiné země budou mít přístup k údajům v jimi vydávaných pasech.

Ačkoliv autentizace čipu nahrazuje aktivní autentizaci a zlepšuje bezpečnost i pro Secure Messaging, probíhá autentizace čipu a terminálu protokoly, které zatím nebyly standardizovány organizací ICAO. Proto to jsou protokoly, které budou využity jen v těch kombinacích, kdy pas i inspekční systém dané protokoly podporují. Pokud pas (např. pasy první generace) nebo inspekční systém (např. ne-EU systém, nebo i EU systém na méně významném přechodu) protokol nepodporují, je nutné využít klasické protokoly standardizované v 9303 (tedy přímé čtení, BAC a AA). Je také možné, že některé země (mimo EU) nebudou otisky prstů nebo oční duhovky považovat za citlivá data a datové skupiny DG3 a DG4 tedy v jejich pasech nebudou nijak dodatečně chráněny.

Poznámka

Názory, zde uvedené, jsou soukromé názory autorů a nemohou být považovány za oficiální stanovisko Evropské komise, kde jeden z autorů pracuje ve Společném výzkumném středisku (JRC) v italské Ispře.

Odkazy

[1] ICAO NTWG: PKI for Machine Readable Travel Documents
Offering ICC Read-Only Access V1.1, http://www.icao.int/mrtd/download/technical.cfm .

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

[3] BSI: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.0, TR-03110,
http://www.befreite-dokumente.de/eingereichte-akten/tr-03110-eac-1.0/.

[4] Říha, Z.: Bezpečnost elektronických pasů, Crypto-World 10/2006, str. 19-26,
http://crypto-world.info/casop8/crypto10_06.pdf