Elektronický cestovní pas: autentizace

V případě pasu je velmi důležité zajistit, aby osobní údaje v něm uložené nebylo možné neautorizovaně měnit. K tomu slouží takzvaná pasivní autentizace, která je jediným celosvětově striktně povinným mechanismem. Některé státy včetně České republiky se navíc rozhodly zavést i autentizaci aktivní, která brání vytváření neautorizovaných kopií pasů.

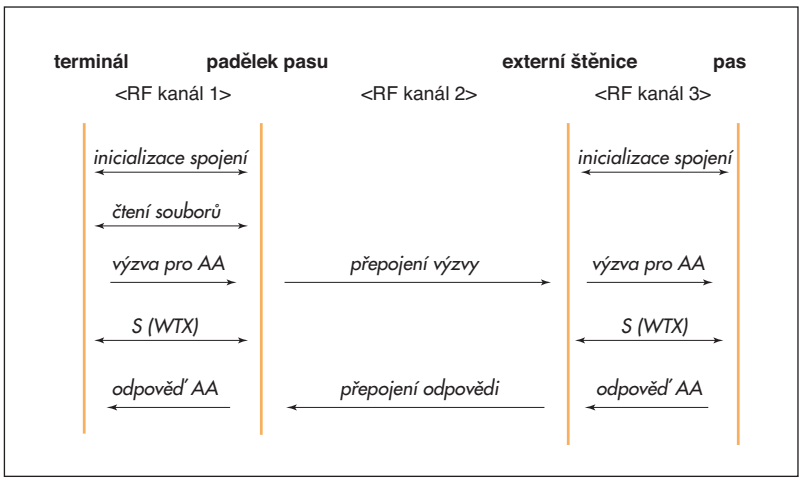
Autentizace původu dat

Mechanismus pasivní autentizace je realizován jako digitální podpis datových souborů označovaných DG1 až DG15, což jsou soubory nesoucí aplikační data pasu (zejména osobní údaje). Více o jejich náplni a mapování na elementární soubory podle ISO 7816 viz [1]. Na českých pasech jsou nyní přítomny jen DG1 (kopie strojově čitelné zóny pasu), DG2 (biometrická fotografie držitele) a DG15 (veřejný klíč aktivní autentizace). DG3 s otiskem palce přibude do 28. 6. 2009 a bude vyžadovat rozšířené řízení přístupu. Podpisové schéma u českých pasů vychází z RSA s délkou modulu 2048 bitů a využívá perspektivní kódování EMSA-PSS podle PKCS#1. Datové struktury jsou uloženy v běžném formátu CMS podle RFC 3852. Podpis na našem pasu pocházel od Státní tiskárny cenin, jejíž certifikát vydala národní autorita Ministerstva vnitra ČR, která používá RSA s modulem 3072b. V jiných státech je klíčové hospodářství obdobné, certifikáty národních autorit jsou vyměňovány přes diplomatické služby.

Aktivní autentizace čipu

Pasivní autentizace z principu nemůže zabránit vytvoření elektronicky identické kopie pasu. Stačí soubory podepsaných dat jednoduše překopírovat včetně souboru s jejich podpisem. Proto byl coby doplňkový mechanismus navržen a v českých pasech (narozdíl například od německých) i implementován jednoduchý protokol výzva-odpověď, který přímočarému kopírování brání. Německu se patrně nelíbila skutečnost, že záznam výzvy a správné odpovědi může sloužit jako jistý druh důkazu přítomnosti pasu na nějakém místě. Za svou snahu chránit soukromí občanů však Německo zaplatilo silnou medializací „objevu“, že tamní pas lze okopírovat. Podstatou diskutovaného protokolu, jehož volání u pasů zemí EU podléhá BAC (viz ST 4/2007), je podpisové schéma RSA podle standardu ISO 9796-2. Veřejný klíč je uložen v datovém souboru DG15 zmíněném výše. Soukromý klíč je uložen ve skrytém souboru (u nás asi EF 0013), jehož externí čtení pas nedovoluje. Dále popsaný protokol umožňuje terminálu ověřit, že pas zná správný klíč do páru s klíčem z DG15, aniž by se přitom jeho hodnotu dozvěděl.

Protokol zahajuje terminál 8B výzvou *V*. Pas vygeneruje náhodné číslo *U* v délce 106 bajtů a vypočte hašový kód w=SHA-1($U||V$), který zformátuje do řetězce m=6A$||U||w||$BC v délce 128 bajtů (délka modulu RSA u pasu v našich experimentech byla 1024 bitů). Na něj je aplikována podpisová transformace RSA a výsledek $s=m^d \bmod N$, kde N je modul a d soukromý exponent, je odeslán terminálu, který jej zřejmým způsobem ověří (detaily viz ISO 9796-2).



Obr. 1 Přepojovací útok na aktivní autentizaci (AA)

Pomineme-li postranní kanály, obrana vůči nimž je asi výrobním tajemstvím, není v současné době znám matematický postup umožňující uvedený protokol prolomit. Analýza komunikačního protokolu však odhalila jistou technickou slabinu umožňující přepojovací útok ilustrovaný na *obr. 1*. Jádrem slabiny je *S*-blok přenosového protokolu *WTX* (viz ISO 14443-4), kterým pas žádá terminál o prodloužení doby čekání na odpověď. Náš pas konkrétně požadoval prodloužení na 4949 ms, což byl 16násobek běžné doby. Pokud terminál tuto dobu nepotvrdil, pas spolupráci vždy ukončil. Předpokládáme proto, že i terminály na hranicích musí *S*(*WTX*) korektně zpracovat a téměř pětisekundové čekání akceptovat. Náš pas byl přitom obvykle schopen odpovídat už za méně než 950 ms. Při zhruba hraniční intenzitě pole pak za méně než 1250 ms (zpomalením výpočtu si čip asi šetří energii). Vzniklou časovou rezervu může útočník využít k předání výzvy kanálem 2 do zařízení nazvaného externí štěnice, které je v blízkosti originálu a požádá ho o správnou odpověď. Originál ji štěnici poskytne dostatečně rychle na to, aby byla kanálem 2 zpět přes padělek dopravena včas do terminálu. Ostatní požadavky padělek nepřepojuje, neboť je umí obsloužit lokálně (má kopie souborů DG). Hypoteticky by tak na řádný pas, který byl přes noc uložen v hotelové recepci, mohl kdosi překročit státní hranice, aniž by se originál pohnul z místa, kde si ho ráno nic netušící majitel vyzvedne. Realizace kanálů 1 a 2 ovšem není úplně jednoduchá, padělek musí totiž stále mít vizuální podobu pasu a klasické ochranné prvky. Nicméně fyzika jisté cesty nabízí, například v již zmíněné technice emulace postranních pásem (viz ST 1/2007). Pas, který by útočník držel v ruce, by pak vůbec nemusel nějaký čip obsahovat. Místo něho by totiž veškerou elektronickou komunikaci s terminálem na hranicích obstaralo z dostatečné vzdálenosti (například z auta, viz ST 3/2007) zcela jiné zařízení, které již podobu pasu mít rozhodně nemusí. To by pak zajistilo i navázání kanálu 2 se štěnicí.

Závěr

Digitální podpisy nabízejí elektronickým částem nových pasů analogické ochranné prvky jako tiskařská technologie částem „papírovým“. Při ověřování dokladu by se zatím podle našich informací měly kontrolovat všechny dostupné markanty (elektronické i tištěné). Časem se však nejspíš bude postupně přecházet na levnější a rychlejší kontrolu pouze elektronické části. Do té doby je ovšem žádoucí ošetřit všechny takové prozatím nevýznamné slabiny, jako jsme ukázali výše.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technologies, ICAO, ver. 1.7, 2004

[2] PKI for Machine Readable Travel Documents offering ICC Read-Only Access, IACO, ver. 1.1, 2004

[3] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz