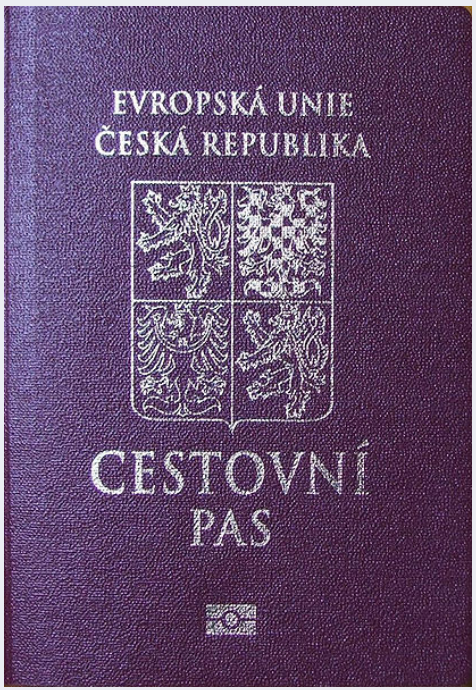
Elektronický cestovní pas

L'ubomíra Balková

Úvod do kryptologie

13. května 2010



- pasová kontrola
  - je pas originál a ne padělek? nebyl neautorizovaně modifikován?
    ochranné prvky: speciální papír, vodoznak, ochranný kovový proužek, speciální barvy, mikrotisk, prvky viditelné pouze pod UV;
    pasivní autentizace
  - odpovídá podoba držitele fotce?
    biometrie
  - má osoba právo překročit hranici? není stíhána?
    databáze Interpolu
  - nejde o odcizený či ztracený pas?
    databáze Interpolu

- pasová kontrola
  - je pas originál a ne padělek? nebyl neautorizovaně modifikován?
    ochranné prvky: speciální papír, vodoznak, ochranný kovový proužek, speciální barvy, mikrotisk, prvky viditelné pouze pod UV;
    pasivní autentizace
  - odpovídá podoba držitele fotce?
    biometrie
  - má osoba právo překročit hranici? není stíhána?
    databáze Interpolu
  - nejde o odcizený či ztracený pas?
    databáze Interpolu
- dlouho jedinou automatizací strojově čitelná zóna s digitalizací 2 řádků s osobními údaji (88 znaků - jméno, příjmení, datum narození)
- ICAO (Mezinárodní organizace pro civilní letectví) - přidání čipu
- EU - povinné zavedení čipů do pasů pro všechny členské státy: ČR od 1. září 2006, otisk prstu od 1. dubna 2009

- standard ICAO 9303 z roku 2003 využívá technologie bezkontaktních čipových karet, asymetrické kryptografie a do jisté míry i biometrie

- standard ICAO 9303 z roku 2003 využívá technologie bezkontaktních čipových karet, asymetrické kryptografie a do jisté míry i biometrie
- čipové karty
  - včetně antény integrovány v papírovém obalu pasu
  - nevyžadují kontakt se čtečkou (0-10 cm)
  - používají rychlý komunikační protokol ISO 14443
  - disponují relativně velkou pamětí (desítky kB) i rychlými procesory včetně kryptografických koprocesorů
  - patří mezi RFID zařízení (Radio Frequency Identification) = společný název pro technologie přenášející data pomocí elmg pole
    - ★ aktivní - vlastní zdroj energie, komunikace na větší vzdálenost
    - ★ pasivní - zdroj energie nemají, odkázána na energii získanou indukcí z elmg pole generovaného snímačem

- je pas originál a ne padělek?

- je pas originál a ne padělek?
- data v el. pasu musí být digitálně podepsána vydávající institucí $\Rightarrow$ ani vynikající padělek nemůže bez patřičného soukromého klíče vytvořit správný digitální podpis padělaných dat
- povinná součást el. pasů
- nemůže zabránit vytváření přesných kopií dat (tzv. klonování) $\Rightarrow$ biometriky a aktivní autentizace

- každý stát vytváří svou národní certifikační autoritu, která podepíše klíče autorit vydávajících dokumenty (národní autorita Ministerstva vnitra ČR - RSA 3072 bitů)
- tyto autority pak podepisují data v el. pasech (např. Státní tiskárna cenin - RSA 2048 bitů)
- 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
- kompromitace klíče neznamená automatickou neplatnost VŠECH dokumentů podepsaných tímto klíčem, ale jen zvýšenou pečlivost při kontrole takových dokumentů

- jde o neautorizovanou kopii pasu?

- jde o neautorizovanou kopii pasu?
- čip obsahuje asymetrický klíč, který nelze přečíst, snímač pouze zjistí, zda má čip takový klíč k dispozici
- součástí dat uložených na čipu a digitálně podepsaných vydávající autoritou je veřejný klíč čipu
- 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 nemůže získat soukromý klíč 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)

- jde o neautorizovanou kopii pasu?
- čip obsahuje asymetrický klíč, který nelze přečíst, snímač pouze zjistí, zda má čip takový klíč k dispozici
- součástí dat uložených na čipu a digitálně podepsaných vydávající autoritou je veřejný klíč čipu
- 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 nemůže získat soukromý klíč 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)
- aktivní autentizace dobrovolná (české pasy ano, německé ne)

- systém, který umožní přístup k datům komukoliv, kdo je schopen číst údaje ze stránky s osobními údaji
- EU v roce 2005 - povinné základní řízení přístupu (Basic Access Control, BAC)
- algoritmus BAC: řetězec z čísla pasu, data narození držitele a data vypršení platnosti pasu (všechny 3 údaje včetně kontrolních číslic) hašován funkcí SHA-1 pro získání dvou 3DES klíčů $\Rightarrow$ využití k autentizaci a ustavení společného klíče pro následnou komunikaci
- nevýhoda BAC: malá entropie v datech pro autentizaci, teoretické maximum je asi 56 bitů:
  - datum narození z období max. 100 let - asi 15 bitů,
  - datum platnosti max. 10 let - asi 11 bitů,
  - 9 číslic čísla pasu - asi 30 bitů,

  ale všechny hodnoty nejsou stejně pravděpodobné a se znalostí číslovacího plánu pasů klesá entropie na cca. 35 bitů $\Rightarrow$ tzv. off-line útok založený na odposlechu úspěšné komunikace

- systém, který umožní přístup k datům komukoliv, kdo je schopen číst údaje ze stránky s osobními údaji
- EU v roce 2005 - povinné základní řízení přístupu (Basic Access Control, BAC)
- algoritmus BAC: řetězec z čísla pasu, data narození držitele a data vypršení platnosti pasu (všechny 3 údaje včetně kontrolních číslic) hašován funkcí SHA-1 pro získání dvou 3DES klíčů $\Rightarrow$ využití k autentizaci a ustavení společného klíče pro následnou komunikaci
- nevýhoda BAC: malá entropie v datech pro autentizaci, teoretické maximum je asi 56 bitů:
  - datum narození z období max. 100 let - asi 15 bitů,
  - datum platnosti max. 10 let - asi 11 bitů,
  - 9 číslic čísla pasu - asi 30 bitů,

  ale všechny hodnoty nejsou stejně pravděpodobné a se znalostí číslovacího plánu pasů klesá entropie na cca. 35 bitů $\Rightarrow$ tzv. off-line útok založený na odposlechu úspěšné komunikace
- řešení: více náhodnosti v sériových číslech pasů $\Rightarrow$ rozšířené řízení přístupu (Extended Access Control, EAC)

- RFID lze vzdáleně detekovat $\Rightarrow$ zloděj ví, v čí kabelce je pas
- i bez přístupu k datům na čipu lze zjistit:
  - číslo čipu $\Rightarrow$ sledování konkrétní osoby
  - výrobce a typ čipu, a tedy stát (nestandardní chybové návratové kódy) $\Rightarrow$ zneužití teroristy (bomba, která se aktivuje, je-li v blízkosti Američan)

- RFID lze vzdáleně detekovat $\Rightarrow$ zloděj ví, v čí kabelce je pas
- i bez přístupu k datům na čipu lze zjistit:
  - číslo čipu $\Rightarrow$ sledování konkrétní osoby
  - výrobce a typ čipu, a tedy stát (nestandardní chybové návratové kódy) $\Rightarrow$ zneužití teroristy (bomba, která se aktivuje, je-li v blízkosti Američan)
- obrana: Faradayova klec = kovový obal čipu (např. hliníkový přebal) $\Rightarrow$ čip nelze detekovat ani s ním komunikovat, dokud pas nevyndáme z obalu

běžný souborový systém čipových karet

- adresáře = dedikované soubory DF
- soubory = běžné soubory EF
- *EF.COM* - vyhrazen pro metadata (verze formátu dat a seznam přítomných datových skupin)
- $EF.SO_D$ - obsahuje digitálně podepsané haše souborů
- ostatní soubory obsahují jednotlivá data rozdělena do skupin Data Groups DG
  - DG1 - strojově čitelná zóna
  - DG2-7 - biometrické údaje (portrét v JPEG, otisk prstu, oční duhovka, podpis)
  - DG8-10 - popisují bezpečnostní prvky (papírové části) pasu, formát dat však zatím není standardizován
  - DG11 - dodatečná data o držiteli
  - DG12 - data o vydavateli pasu
  - DG13 - pro interní použití vydávajícího státu
  - DG14 - pro rozšířené řízení přístupu
  - DG15 - veřejný klíč pro aktivní autentizaci
  - DG16 - adresy příbuzných pro podání zprávy v případě nehody