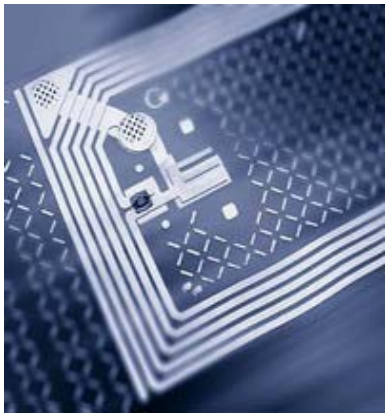
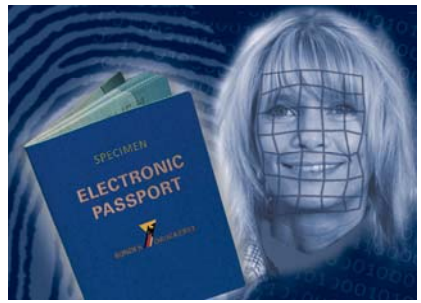
Autentizace v příkladech



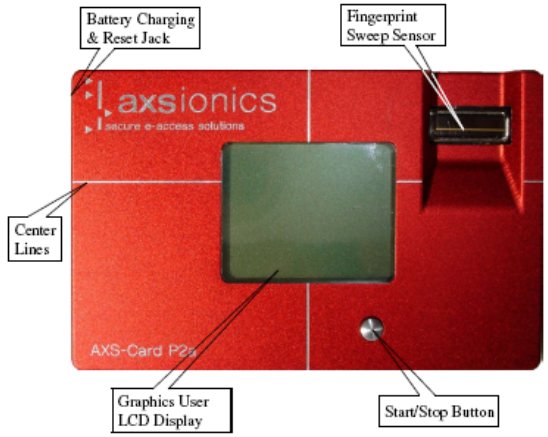
Masarykova univerzita
Fakulta informatiky

Honza Krhovják
Vašek Matyáš
Zdeněk Říha



HW tokeny a jejich využití

- Uchovávání citlivých dat
  - zejména kryptografické klíče
  - údaje nezbytné pro využívání předplacených služeb
    - přihlášení do GSM sítě, dekódování satelitního signálu
- Autentizace uživatelů
  - vstup do zabezpečené místnosti
  - přihlašování do operačního systému
  - přihlašování do e-bankovnictví
  - autorizace bezhotovostní platby
  - výběr hotovosti z bankomatu



- Identifikace uživatelů
  - elektronické dokumenty (pasy, řidičské průkazy, atd.)

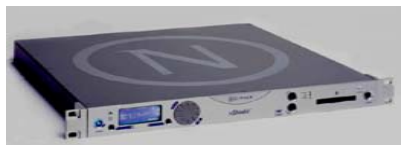
Autorizace finančních transakcí

- Typicky dvoufaktorová autentizace
  - použití tokenu (karta s magnet. proužkem, čipová karta)
  - použití biometriky nebo znalosti
    - peněžní bankomaty – PIN
    - bezhot. platba z místa prodeje – podpis nebo PIN
      - typicky závisí na typu (magnetický proužek nebo čip) i na druhu (např. MasterCard nebo VISA) karty
      - v praxi ne vždy výlučně (po PINu může být žádán i podpis)
    - bezhot. platba z Internetu – CVV/CVC/CID čísla
  - je-li úspěšná, následuje ověření velikosti disponibilního zůstatku a je-li ten dostatečný, tak platba proběhne
  - je-li neúspěšná, tak ji lze v závislosti na bezpečnostní politice vydávající banky několikrát zopakovat

Struktura bankovní sítě

- Základní terminologie
  - vydávající banka – banka kde má zákazník účet a která vydala vlastníkovi účtu kartu a PIN
  - poskytující banka – banka počátečně zodpovědná za transakci uživatele (např. provozující danou síť bankomatů či zajišťující příjem bezhotovostních plateb v místě prodeje)
- Banky vzájemně propojeny pomocí přepínačů
  - využití symetrické kryptografie (typicky 3DES)
    - potřeba předem ustavených tajných šifrovacích klíčů
- Kryptografické operace a bezpečné uložení klíčů obstarávají HW bezpečnostní moduly




Online verifikace PINu I

- Probíhá vzdáleně ve vydávající bance
  - potřeba bezpečného přenosu PINu od poskytující k vydávající bance (jiný PIN než u běžné čipové karty!)
    - banky si vzájemně nedůvěřují, nedůvěřují svým pracovníkům, a nedůvěřují ani zákazníkům
    - řeší HSM a různá administrativní/procedurální opatření
  - bankomat či platební terminál v místě prodeje je typicky bezpečné zařízení (HW bezpečnostní modul)
    - po vložení je PIN formátován do PIN-bloku
      - struktura obsahující PIN a další data zvyšující celkovou entropii
    - tento PIN-blok je odpovídajícím klíčem zašifrován a odeslán
    - na přepínačích dochází k přešifrovávání a někdy také k přeformátovávání PIN-bloku (různé sítě => různé formáty)

Online verifikace PINu II

- Originální PIN není v bance uložen
  - vygenerován v HW modulu na základě čísla účtu a bezpečně uloženého tajného PIN generujícího klíče
  - bezpečně vytištěn, zalepen do obálky, zaslán držiteli karty
- Verifikace také probíhá uvnitř HW modulu
  - přijatý PIN je dešifrován a extrahován z PIN-bloku
  - originální PIN je znovu vygenerován
  - přijatý PIN je srovnán s tímto originálním PINem
- Problém: nejednotnost standardů
  - mnoho formátů PIN-bloků, různé metody generování PINů a šifrování => špatná interoperabilita + bezpečný návrh HW modulů a jejich API se stává obtížný (ne-li nemožný)

Specifikace EMV

- Standard EMV 4.1 (Europay, MasterCard, VISA) je definován ve čtyřech samostatných dokumentech
  - aplikačně nezávislé požadavky na čipové karty a platební terminály
    - elektromechanické charakteristiky (např. rozměry čipu), přenosové protokoly, struktura souborů a příkazů, ...
  - bezpečnostní požadavky
    - mechanizmy offline autentizace dat a šifrování PINů, management kryptografických klíčů, ...
  - požadavky na jednotlivé aplikace
    - definice konkrétních APDU příkazů, ...
  - povinné, doporučené, a volitelné požadavky na platební terminály

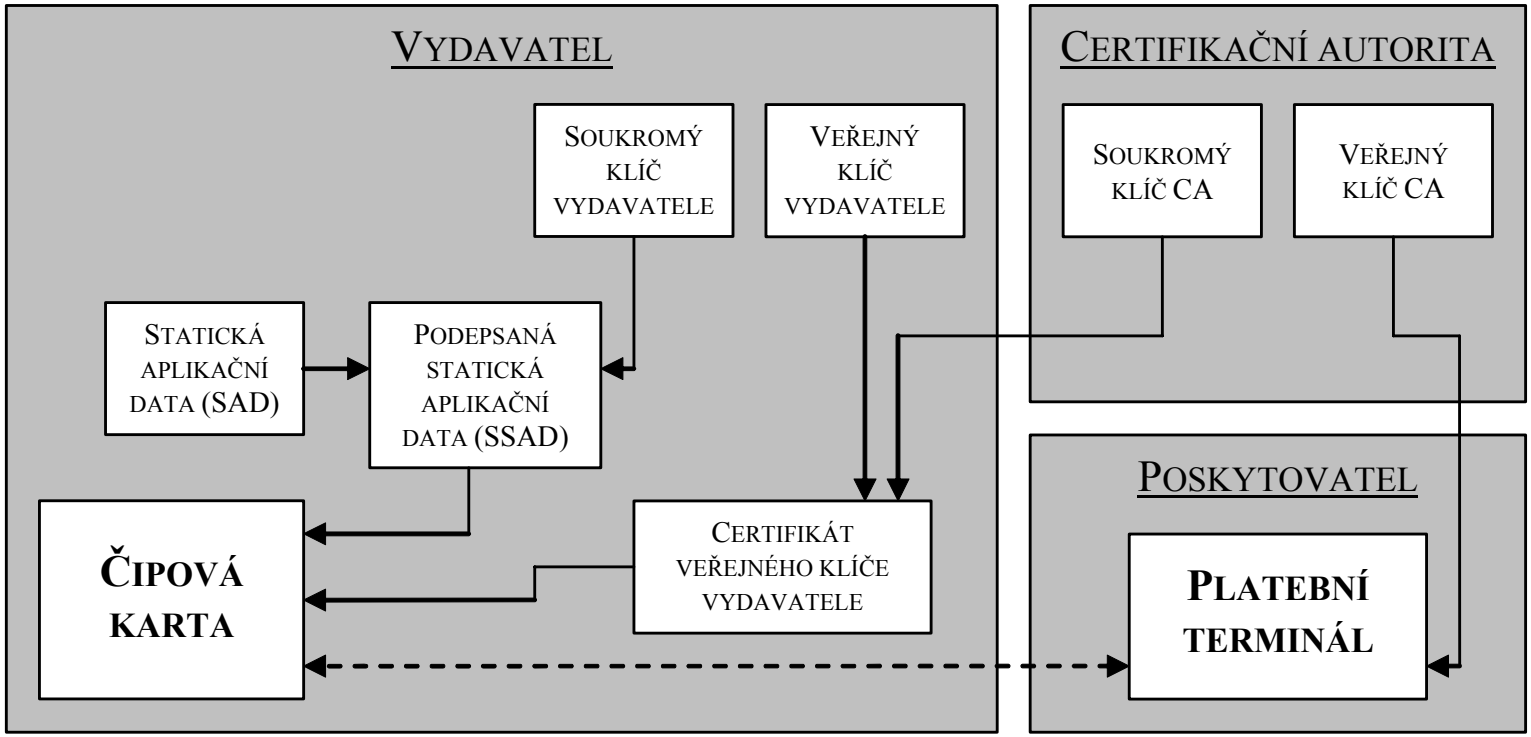
Offline autentizace dat

- Cílem je detekce falešných/padělaných karet
  - založeno na asymetrické kryptografii (RSA) a PKI
    - RSA veřejný exponent musí být vždy 3 nebo $2^{16} + 1$
  - vyžadována existence certifikační autority (CA)
    - certifikuje veřejné klíče vydávajících bank
    - každý terminál musí obsahovat veřejný klíč CA
    - musí být zajištěna integrita přenášených veřejných klíčů
- Tři základní mechanizmy
  - SDA: statická autentizace dat
  - DDA: dynamická autentizace dat
  - CDA: kombinovaná DDA a generování aplikačního kryptogramu

Statická autentizace dat I

- Základní vlastnosti SDA
  - potvrzuje pravost statických dat uložených v čipové kartě
    - detekuje neautorizovanou změnu dat po personalizaci karty
  - prováděna terminálem (čip pouze zasílá potřebná data)
- Princip a průběh SDA (obrázek na dalším slajdu)
  - veřejný klíč CA je uložen v každém terminálu
  - veřejný klíč vydávající banky je certifikován CA a uložen uvnitř čipu
  - statická aplikační data jsou podepsána soukromým klíčem vydávající banky a uložena uvnitř čipu
- Bezpečnost SDA
  - závisí na bezpečnosti soukromých RSA klíčů
  - padělání/duplikace čipových karet nevyřešena

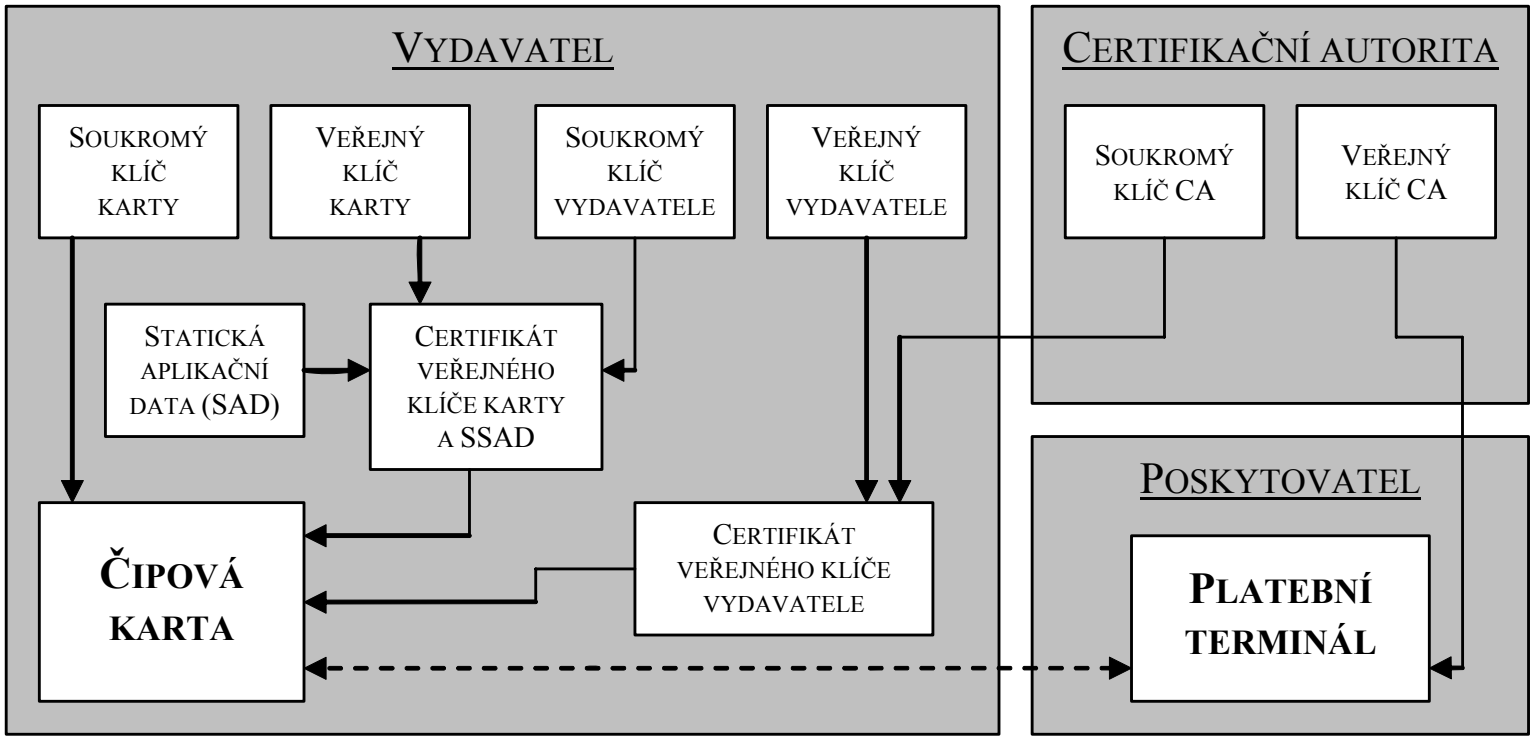
Statická autentizace dat II



Dynamická autentizace dat I

- Základní vlastnosti DDA
  - prováděna terminálem i kartou (potřeba čip s koprocesorem)
  - potvrzuje pravost statických dat uložených a generovaných v čipové kartě a dat obdržených z terminálu
    - detekuje padělané/duplikované karty
- Princip a průběh DDA (obrázek na dalším slajdu)
  - oproti SDA je v čipu uložen nový unikátní pár RSA klíčů
    - soukromý klíč je bezpečně uložen v čipu (nikdy jej neopouští)
    - veřejný klíč je podepsán a uložen společně ze stat. apl. daty
- Bezpečnost DDA
  - závisí také na bezpečnosti soukromých RSA klíčů
    - čipová karta musí být také schopna zajistit bezpečnost svého soukromého RSA klíče

Dynamická autentizace dat II



Kombinovaná DDA a ACG

- Základní vlastnosti CDA
  - prováděna terminálem i kartou společně s analýzou akcí karty (která se normálně provádí později)
- Princip a průběh CDA
  - náhodná výzva je oproti DDA součástí požadavku na získání aplikačního kryptogramu
  - je tedy i součástí podepsaného aplikačního kryptogramu
- Bezpečnost CDA
  - stejné požadavky jako v případě DDA
  - CDA navíc zabezpečuje zasílaný aplikační kryptogram
    - výhoda zejména pokud nelze garantovat bezpečnou komunikaci mezi terminálem a čipovou kartou

Dohoda autentizační metody

- Vzájemná komunikace mezi terminálem a kartou
  - Přichází na řadu ihned po offline autentizaci
  - Základní podporované metody
    - použití podpisu (ručně psaného)
    - použití PINu (online/offline, plaintext/encrypted)
    - některé kombinace (např. online => encrypted)
- Prioritně uspořádaný seznam podporovaných metod (CVM) je uložen v každé čipové kartě
  - terminál zvolí první podporovanou metodu ze seznamu
    - zvolená metoda je závislá na typu terminálu
    - jedna z metod může být „autentizace nevyžadována“
  - úspěšná verifikace PINu
    - alespoň jedna z metod úspěšně proběhla

Autorizace platby

- Autentizace založená na podpise či na online verifikaci PINu
  - stejný proces jako u karet s magnetickým proužkem
    - PIN je formátován do PIN-bloku, zašifrován, ...
  - čipové karty => ochrana proti skimmingu (zkopírování karty)
    - na kartě navíc uloženy 3 symetrické klíče (3DES, MAC)
- Autentizace založená na offline verifikaci se šifrováním PINu
  - vyžaduje nový RSA pár klíčů pro šifrování PINů
  - uložen/certifikován jako pár klíčů pro DDA (či CDA)
  - originální PIN (nutný pro verifikaci) bezpečně uložen v čipu
  - PINpad/terminál musí být fyzicky/logicky dobře zabezpečen

Automatická správa rizik

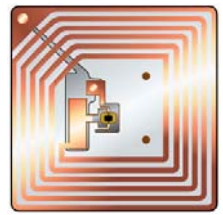
- Přichází na řadu po úspěšné autentizaci uživatele
- Ochrana proti hrozbám nedetekovatelným v offline prostředí
  - rozhoduje zda by transakce měla být: přijata offline, zamítnuta offline, autorizována online
- Správa rizik terminálu
  - kontrola horního limitu stanoveného obchodníkem
    - typicky při provádění několika malých oddělených transakcí
  - kontrola rychlosti oběhu peněz
    - omezení počtu po sobě jdoucích offline transakcí
  - náhodný výběr transakce pro online autorizaci
- Analýza akcí terminálu a karty
  - terminál má při zamítnutí transakce rozhodující slovo

Důsledky specifikace EMV

- Zajištění interoperability platebních systémů založených na použití kontaktních čipových karet
  - jeden standard (ideálně akceptovaný všemi stranami)
- Zavedením autorizace PINem je zodpovědnost za transakce převedena na zákazníka
  - výhodné pro banky i obchodníky – ne pro zákazníka
- Častá tvrzení o EMV a technologii Chip&PIN
  - čipové karty poskytují bezpečnější úložiště pro citlivá data
    - pokud se nepoužívá SDA
  - autentizace uživatelů pomocí PINu je bezpečnější
    - pokud je vyjednána bezp. autentizační metoda (jen pokud je dobře zajištěna integrita CVM)
  - protokol lze snadno přesměrovat (relay attack)
    - žádná ze zavedených techn. tomu nezabrání

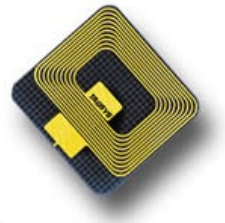
Bližší informace na http://www.cl.cam.ac.uk/research/security/projects/banking/

Bezdrátová technologie RFID



- RFID – Radio Frequency Identification
  - určeno k automatické identifikaci objektů
  - umožňuje přenos dat pomocí elektromagnetického pole
- Základní rozdělení RFID tagů (kromě R/O a R/W)
  - pasivní – bez vlastního zdroje energie
    - velmi malé (bez antény 0,15 mm × 0,15 mm) a tenké (7,5 μm)
    - levné a téměř neomezená životnost (není limitována baterií)
    - dosah max. několik metrů (v závislosti na frekvenci a anténě)
  - aktivní – vlastní zdroj energie a větší paměť/výkon
    - mohou šířit svůj vlastní signál – tzv. majáky (beacons)
    - dražší, dosah desítky metrů, životnost baterie až 5 let
  - semi-aktivní (či semi-pasivní) – vlastní zdroj energie pouze pro napájení čipu => rychlejší odezva než pasivní tagy

Bezpečnost RFID



- Bezkontaktní komunikace s RFID tagem většinou nevyžaduje přímou viditelnost
  - komunikační vlastnosti závisí na použitém frekv. pásmu
    - většina tagů pracuje na 13,56 MHz => nelze přečíst na vzdálenost větší než 1 m
    - tagy pracující na 868/915MHz => vyžadují přímou viditelnost
  - v blízkosti čtečky vysílá jedinečný identifikátor (číselný kód)
    - EPC kód obsahuje další inf. (výrobce, typ produktu apod.)
- Bezpečnostní problémy RFID (předmětem výzkumu)
  - soukromí – problém sledování a inventarizace
    - ochrana tagů proti neautorizovanému čtení
  - autentizace – problém snadného falšování/padělání tagů
    - ochrana čteček proti padělaným tagům

Techniky zajištění soukromí I

- Deaktivace tagu (absolutní jistota)
  - typicky čtečkou a na místě, kde zákazník přebírá zboží
  - ne vždy lze použít (knihovny, obchody nevyužívající RFID)
- Pasivní či aktivní rušení
  - pasivní – princip Faradayovy klece (kovová síť či hliníková fólie bránící průchodu rádiových signálů)
  - aktivní – použití speciálního rušícího zařízení (dlouhé rušení může být nelegální a pro okolní RFID nežádoucí)
- Měření vzdálenosti (pomocí poměru signál/šum)
  - pokus o vzdálené čtení => odvysílání nesprávných dat
- Využití prostředníka (nutná autentizace vůči tagu)

Techniky zajištění soukromí II

- Změna jedinečného identifikátoru
  - nepravidelná: jednorázové přeznačení (neeliminuje problém sledování) či smazání (ostatní data zůstanou)
  - pravidelná: malá množina pseudonymů (rozpozná je pouze autorizovaná čtečka) či přešifrovávání
- Selektivní blokování
  - identifikátory rozděleny dle 1. bitu na soukromé a veřejné
  - blokující RFID tag „ruší“ čtení soukromých identifikátorů
    - využívá antikolizního protokolu používaného čtečkou
    - ne vždy funguje spolehlivě (závisí na umístění)
    - po úpravě lze zneužít k úplnému blokování identifikátorů

Podrobnější informace lze nalézt na http://www.rsasecurity.com/rsalabs/node.asp?id=2115 konkrétně v http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf

Cestovní pasy

- Pas je identifikační průkaz nutný k přechodu státních hranic (až na výjimky) =>
- Kontroluje se
  - zda je pas originál (vydaný patřičnou autoritou), a ne padělek
    - tiskové technologie, vodoznak, prvky viditelné v UV světle …
    - *digitální podpis dat, aktivní autentizace*
  - zda osoba, které jej předkládá, je osoba, jíž byl pas vydán (a ne někdo kdo pas našel, ukradl …)
    - fotka oprávněného držitele
    - *biometrické údaje*
  - zda pas je stále platný (doba platnosti případně další omezení (lidé, po nichž je vyhlášeno pátrání, jimž bylo omezeno právo cestovat apod.))
    - policejní databáze (např. Interpol)
    - *automatizované čtení dat z pasu*

Automatizovaná kontrola

- Dnes jen za pomoci strojově čitelné zóny (MRZ), max. 88 znaků:

Ptzzzjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj
ccccccccccKnnnRRMMDDKprrmmddKooooooooooooooKX

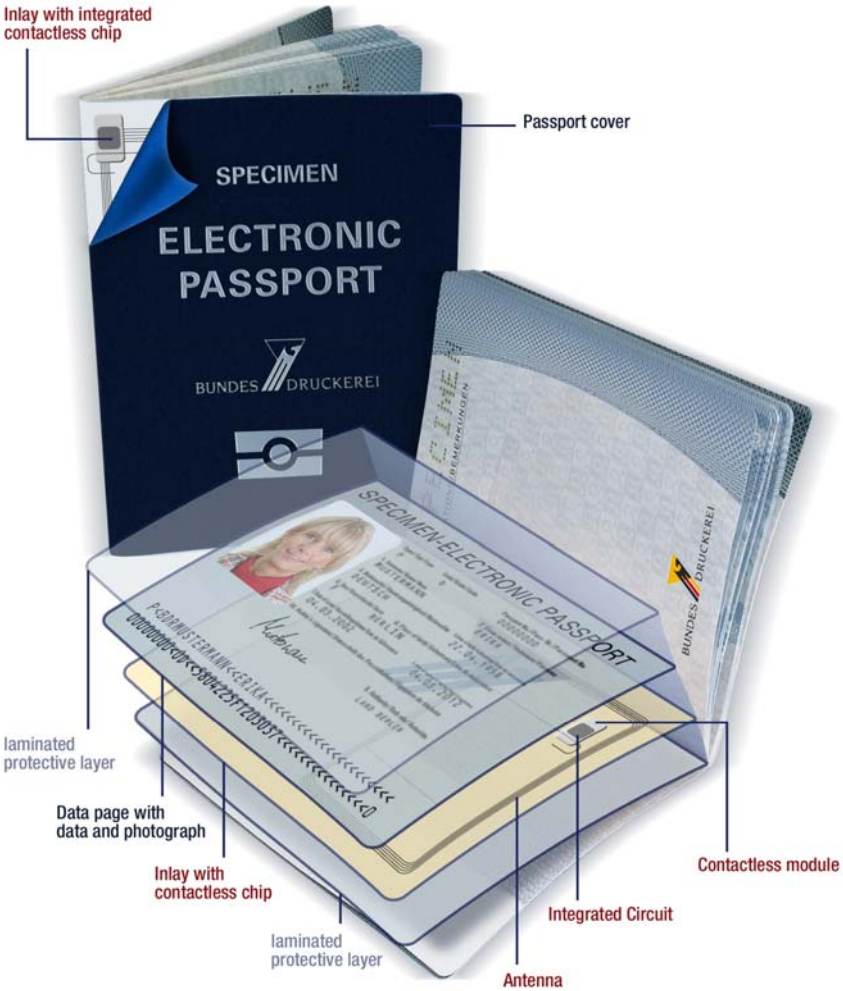
- t (typ pasu), z (země vydání), j (jména a příjmení),
  c (číslo pasu),
  RRMMDD (datum narození),
  p (pohlaví),
  rrmmdd (datum platnosti),
  o (osobní číslo – RČ),
  X & K (kontrolní číslice)
  < (položka nevyužita)

ePasy – elektronické pasy

- Pasy s vloženým RFID čipem
  - bezdrátová čipová karta podle ISO 14443
  - komunikace na 13,56 MHz
  - obvykle čtecí rozsah 0–10 cm
  - data uložena v 16 souborech (DG1 až DG16)
  - metadata v souboru EF.COM (verze + indikace, který z 16 DG je přítomen)
  - bezpečnostní soubor $EF.SO_D$
- Na přední straně typicky označeny logem 

Obrázky ePasů převzaty z http://www.bundesdruckerei.de/

ePasy – další obrázky



▶ The contactless chip can be integrated into either the cover page or the data page.

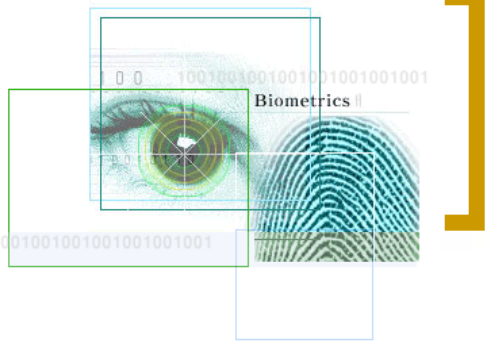
Pasivní autentizace

- *Pasivní i aktivní autentizace do jisté míry podobná metodám SDA a DDA ve specifikaci EMV*
- Všechna data (každá datová skupina DG) jsou digitálně podepsána vydávající autoritou
  - soubor EF.SO_D obsahuje podepsané haše všech uložených DG
- Pro ověření podpisu je třeba mít k dispozici certifikát vydavatele
  - certifikační řetěz je obvykle uložen v pase
  - kořenové certifikáty nutné získat bezpečnou cestou (diplomatickou poštou, vznikající infrastrukturou ICAO)

Aktivní autentizace

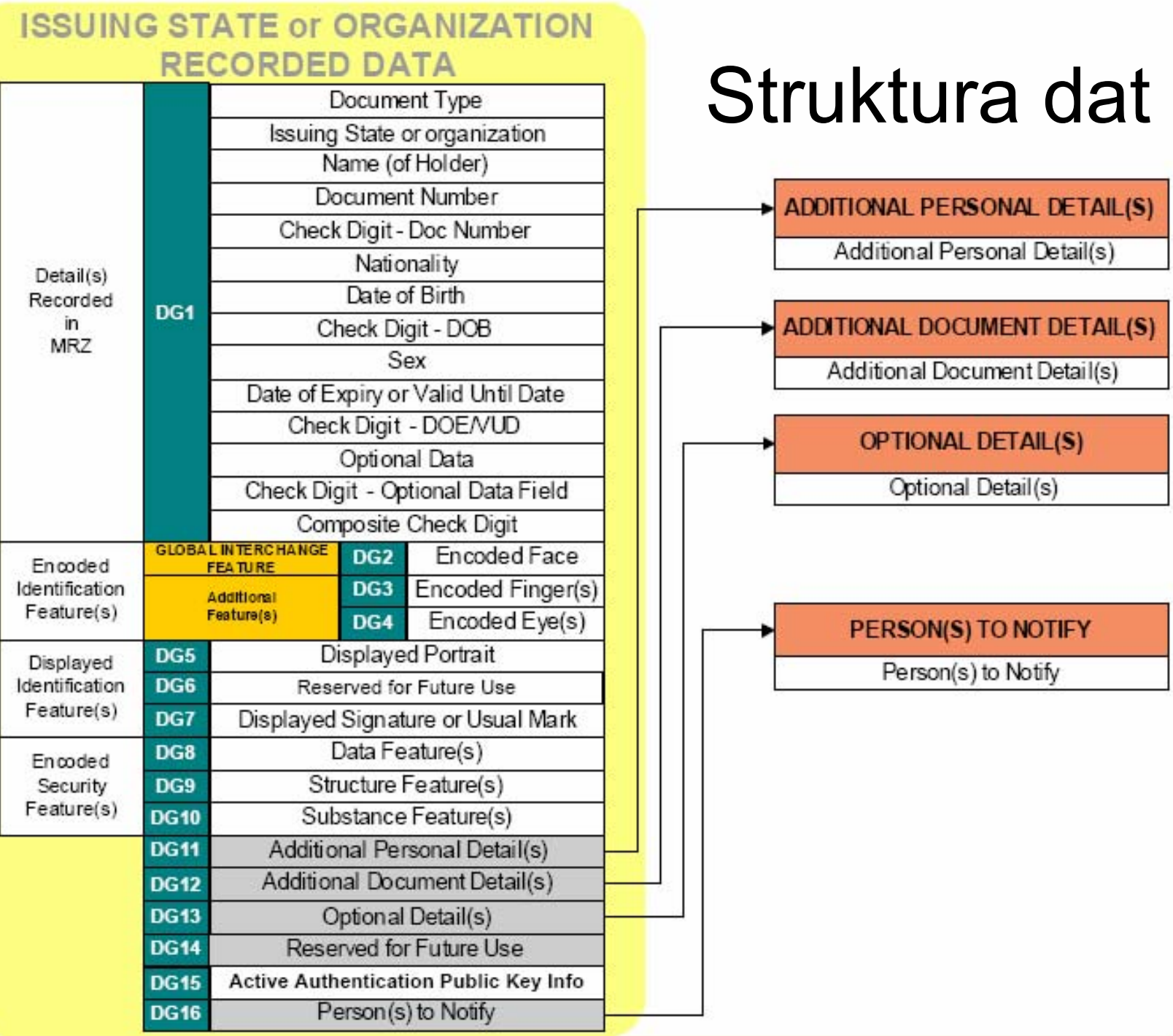
- Digitálně podepsaná data lze kopírovat (zkopírují se data včetně jejich podpisu)
- Snadnému kopírovaní se pasy mohou bránit aktivní autentizací
  - asymetrický pár klíče
    - soukromý klíč uložen v čipu, bez možnosti jeho přímého získání (čip je fyzicky bezpečný)
    - veřejný klíč je uložen v DG15 (tj., je digitálně podepsán)
  - protokol výzva-odpověď pro ověření, zda má pas k dispozici soukromý klíč
    - přečtu veřejný klíč pasu (DG15) a ověřím jeho podpis pomocí veřejného klíče vydávající autority
    - pošlu pasu náhodné číslo
    - pas náhodné číslo doplní svou náhodnou částí a podepíše
    - ověřím digitální podpis na základě veřejného klíče pasu

Biometriky



- Pro automatizovanou verifikaci identity předkladatele pasu (DG 2-4)
  - obličej (ve formátu JPEG/JPG2000 s případnými dalšími významnými biometrickými body, viz ISO 19794-5)
  - otisk prstu (obrázek WSQ nebo zpracovaná data ve formě markantů, vzorů apod., viz ISO 19794-2, 19794-3, 19794-4, 19794-8)
  - duhovka (obrázek viz ISO 19794-6)
- Dále jako digitální verze vytištěných dat (DG5-7)
  - fotografie držitele (viz ISO 10918)
  - podpis držitele (viz ISO 10918)

Struktura dat



Ochrana dat

- RFID umožňuje zjištění existence čipu i čtení dat z čipu na dálku
  - viz techniky zajišťující soukromí
    - u ePasů zatím pouze pasivní rušení/stínění
      - efektivní pouze pokud je pas uzavřen
  - navíc také logické omezení přístupu k datům
- Řízení přístupu k datům
  - základní řízení přístupu (BAC)
    - tajný klíč lze získat z dat v MRZ
  - rozšíření řízení přístupu (EAC)
    - stejné jako BAC, ale tajný klíč se získá jiným způsobem (není řečeno jak)

Základní řízení přístupu

- Z MRZ je třeba získat
  - číslo pasu
  - datum narození
  - datum vypršení platnosti
- Hašujeme SHA-1 a generujeme dva 3DES-2 klíče
- Podle ISO 11770-2 autentizujeme a ustavíme sdílený šifrovací klíč
  - následná komunikace je šifrovaná, což brání odposlechu přenášených dat
- Data používaná k odvození klíče mají teoretickou entropii ±56 bitů (v praxi však klesá ke 35 bitům)
  - odposlechneme-li úspěšnou komunikaci, lze hrubou silou zjistit klíče a přenášená data dešifrovat

Více informací o strojově čitelných cestovních dokumentech lze nalézt na http://www.icao.int/mrtd/Home/

Rozšířené řízení přístupu

- Bezpečnější varianta kontroly přístupu
  - založeno na opravdu tajných klíčích (ne jako BAC)
  - důležité pro ochranu citlivých biometrik
    - otisk prstu (v EU nejpozději od 28.6.2009), DG3
    - duhovka, DG4
  - pro ochranu dat, které není nutné zpřístupnit všem zemím
    - lze určit, které země budou mít přístup (práva v certifikátu)
- Principiálně možné varianty založené na symetrické i asymetrické kryptografii
  - u symetrické problém s velkým množstvím (dlouho platných) klíčů ve zranitelných inspekčních zařízeních
  - on-line/off-line varianty (vzdálené ostrovy, problém DoS)
  - návrh německého BSI s využitím PKI
    - bude s největší pravděpodobností použit v rámci EU

BSI rozšířené řízení přístupu

- Každá země zřídí CV (Country Verifying) CA
  - určuje vydávání certifikátů, které další země budou mít přístup k citlivým biometrikám
  - certifikát CV CA uložen v pase (kořenový certifikát)
- Další země zřizují DV (Document Verifier) CA
  - certifikována od CV dalších zemí
    - země které chtějí povolit přístup k biom. datům
  - vydává koncové certifikáty inspekčním zařízením
- Pas pak od CV CA ověřuje inspekční zařízení
  - řádně certifikovaný veřejný klíč => ověření ex. soukromého klíče (výzva-odpověď) => přístup k datům
- Autentizace čipu i terminálu
  - Diffie-Hellman (PKCS#3 nebo eliptické křivky ISO 15946)

Autentizace čipu

1. Terminál získá z pasu jeho veřejný DH_P
   - uložen digitálně podepsán v DG14
2. Terminál vygeneruje čerstvý dočasný DH_S pár
   - stejné doménové parametry jako klíčový pár čipu
   - zašle jej pasu zašifrován pomocí DH_P
3. Odvození sdíleného klíče z DH_S
4. Ustavení nového šifrovaného kanálu namísto BAC
   - oproti BAC nyní již opravdu bezpečný (šifrování i MAC)
   - funkčně nahrazuje aktivní autentizaci
     - pas musí znát privátní část DH pro odvození klíče => test
     - aktivní autentizace stále podporována (systémy bez EAC)

Autentizace terminálu

- Cílem je přesvědčit pas, že čtečka může přistupovat k citlivým datům (DG3,DG4)
- Terminál předkládá certifikační řetěz až k cert. CV (ten je uložen v pase)
  - po úspěšném ověření pas získá z certifikátů přístupová práva terminálu (jako AND práv celého cert. řetězce)
  - pas také testuje, zda terminál zná privátní klíč pomocí protokolu typu výzva-odpověď
    - obdoba aktivní autentizace, ale „opačně“
- Použití zjednodušených certifikátu (ne X.509)
- Problém ověření vypršení platnosti certifikátů
  - čip nemá žádné vlastní hodiny
  - nejčerstvější datum vydání korektně ověřeného certifikátu
    - toto datum už určitě nastalo

Otázky???

Děkujeme za pozornost a přejeme úspěšné nastudování a složení zkoušky! ☺