Rozšířené řízení přístupu EACv2 a jeho ověření v projektu BioP@ss

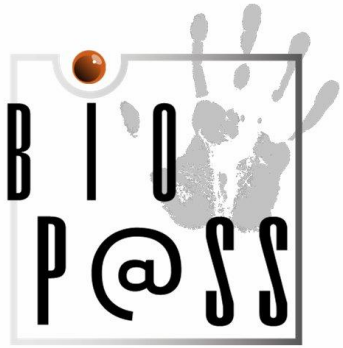
Vítězslav Vacek
Vedoucí vývojového oddělení pro čipové karty

20.5.2010

OKsystem *Spojujeme software, technologie a služby*

Osnova

- Vývoj elektronických pasů
  - První generace pasů (1G)
  - Druhá generace pasů (2G)
  - Třetí generace pasů (3G)
- Výzkumný projekt BioP@ss
  - Představení projektu
  - Příklad použití „elektronická občanka“ s využitím EACv2



OKsystem

První generace pasů (1G)

- Vznikla na základě specifikace ICAO (Doc 9303) v roce 2004
- Osobní textové údaje o držiteli pasu (DG1)
- Biometrické údaje
  - Fotografie (DG2, povinný údaj dle ICAO Doc 9303)
  - Rozšířené biometrické údaje
    - Otisk prstu – DG3
    - Obraz duhovky – DG4
    - Tyto údaje jsou dle ICAO Doc 9303 nepovinné a v pasech první generace nebyly využity
- Kryptografické mechanismy
  - Pasivní autentizace (povinná dle ICAO Doc 9303)
  - Aktivní autentizace (nepovinná dle ICAO Doc 9303)
  - Basic Access Control (nepovinný v ICAO Doc 9303, vyžadován v pasech Evropské unie)

Pasivní a aktivní autentizace (1G)

- Pasivní autentizace
  - Zajišťuje pouze autenticitu uložených dat
  - Nechrání data proti kopírování
  - Technicky řešeno podpisem uložených dat
    - Datové skupiny (DG1-DG16) mají uloženy hash v SOD, který obsahuje jejich digitální podpis
- Aktivní autentizace
  - Zabraňuje možnosti klonovat elektronický pas
  - Technicky řešeno challenge-response protokolem
    - Veřejný klíč pro aktivní autentizaci je umístěn v datové skupině DG15 a jeho hash je umístěn v SOD
    - Odpovídající soukromý klíč je uložen v bezpečné paměti čipu
    - Elektronický pas prokazuje vlastnictví soukromého klíče podpisem náhodné výzvy
  - Implementace tohoto mechanismu není příliš rozšířena, příkladem použití je Česká republika

BAC Basic Access Control (1G)

- Zajišťuje možnost čtení pouze pokud má inspekční systém fyzický přístup k pasu
- Technicky řešeno odvozením přístupových klíčů ze strojově čitelné zóny
  - Přístupové klíče jsou odvozeny z čísla pasu, data narození držitele, data platnosti pasu a kontrolních číslic
  - Z přístupových klíčů jsou odvozeny šifrovací a MAC klíče, které šifrují komunikaci s pasem na úrovni APDU a bez jejich znalosti nelze s pasem komunikovat

Inspekční procedura (1G)

- 1) Výběr aplikace (ePassport)
  - Po výběru pasové aplikace jsou k dispozici data (DG1, DG2, DG14, DG15, SOD) pouze pokud není implementován BAC
- 2) Basic Access Control
  - Optické přečtení strojově čitelné zóny
  - Výpočet šifrovacích a MAC klíčů pro další komunikaci s pasem
- 3) Pasivní autentizace
  - Ověření digitálního podpisu dat uložených v dokladu
- 4) Volitelně aktivní autentizace
  - Získání veřejného klíče z DG15, ověření jeho podpisu v SOD a provedení důkazu o vlastnictví odpovídajícího soukromého klíče

Bezpečnostní problémy (1G)

- BAC a aktivní autentizace nejsou povinné
- BAC – nízká entropie použitých klíčů
  - 9 místné číslo pasu, povoleny písmena a číslice, $\log_2(10+26)^9 = 46{,}5$ bit
  - Datum narození, předpokládejme 100 let života, $\log_2(365*100)^9 = 15{,}1$ bit
  - Datum konce platnosti,předpokládejme 10 let platnosti, $\log_2(365*10)^9 = 11{,}8$ bit
  - Maximální entropie 73,4 bit ale často se používají sekvenční čísla, věk držitele lze odhadnout... různé zdroje uvádějí reálnou entropii mezi 34-52 bit
  - Basic Access Control Knocker, http://rfid.dia.unisa.it/epass/UserGuide.pdf, po zadání min/max čísla pasu, min/max data narození a min/max platnosti pasu program hrubou silou spočítá přístupové klíče
- Aktivní autentizace – problém sémantiky výzvy
  - Pas podepisuje náhodnou výzvu terminálu, která ovšem nemusí být bezvýznamová
  - Výzva může být např. terminálem podepsaná informace o místě a času použití pasu
- Nejsou zavedeny silnější přístupové mechanismy pro citlivá biometrická data (otisky prstů, obraz duhovky)

Druhá generace pasů (2G)

- Hlavní motivací bylo zlepšení řízení přístupu k biometrickým údajům (otiskům prstů)
- Vznikla na základě následujících směrnic a specifikací specifikací
  - Evropská směrnice 2252/2004 přikazuje členským zemím použití otisků prstů nejpozději do 06/2009
  - Rozhodnutí Evropské komise č. 2909 z 28/06/2006 přikazuje použití protokolu EACv1 pro přístup k otiskům prstů
  - ICAO v současné době nemá formální standard pro EACv1
  - Evropská komise i ICAO se odkazují na technickou specifikací BSI TR-03110 verze 1.11 02/2008 (Advanced Security Mechanisms for Machine Readable Travel Documents)
- Kryptografické mechanismy
  - BAC se ustanovil jako povinný pro přístup k údaji o držiteli (DG1) a fotografii (DG2)
  - Nově zaveden protokol EACv1, který je povinný pro přístup k otiskům prstu. Skládá se z autentizace čipu verze 1 a terminálu verze 1.

Autentizace čipu verze 1 (2G)

- Nahrazuje aktivní autentizaci
- Je založena na Diffie-Hellman dohodě na klíči, čímž odstraňuje problém sémantiky výzvy
- Veřejný klíč pro autentizaci čipu umístěn v DG14, soukromý klíč v bezpečné paměti čipu
- Po úspěšné autentizaci čipu dojde k vygenerování nových šifrovacích a MAC klíčů, které nahradí klíče BAC pro šifrování následné komunikace
- Další výhodou jsou silné šifrovací/MAC klíče, které nebyly odvozeny z klíče s nízkou entropií jak je tomu v případ BAC

Autentizace terminálu verze 1 (2G)

- Ověřuje autenticitu terminálu
- Autentizace je založena na protokolu challenge-response
- K provedení autentizace musí terminál předložit patřičné certifikáty
  - Terminál musí čipu zaslat řetěz CVC certifikátů
    - CVCA následné certifikáty (CVCA Link Certificate), DV (Document Verifier) certifikát a terminálový certifikát
- Přístup ke čtení otisků prstu či obrazu duhovky je přidělen pouze pokud k tomu má terminálový certifikát uvedena patřičná práva

Inspekční procedura (2G)

- 1) Výběr aplikace (ePassport)
  - Po výběru pasové aplikace není inspekční systém oprávněn číst ani méně citlivá data
- 2) Basic Access Control
  - Výpočet šifrovacích a MAC klíčů
  - Nyní má inspekční systém přístup údaji o držiteli a fotografii (DG1, DG2, DG14, DG15, SOD)
- 2) Autentizace čipu v1
  - Získání veřejného klíče z DG14, provedení Diffie-Hellman, výpočet šifrovacích a MAC klíčů nahrazující klíče z kroku 1)
- 3) Pasivní autentizace
  - Ověření digitálního podpisu dat s SOD
  - Ověření autenticity veřejného klíče z DG14
- 4) Autentizace terminálu v1
  - Nyní je terminál oprávněn číst citlivá biometrická data (pokud má v certifikátu oprávnění)

Bezpečnostní problémy (2G)

- BAC protokol stále využíván pro přístup k údajům o držiteli (DG1) a fotografii (DG2)
- Možnost číst otisky prstů certifikáty s vypršelou platností
  - Čip nemá reálný čas, je aproximován při hraniční kontrole po přijetí platných certifikátů (CVCA link, DV, Accurate Terminal Certificate). U osob, které necestují často, lze číst otisk poměrně dlouho s vypršelými certifikáty
- Čip prokazuje svoji pravost neautentizovanému terminálu (nevhodné pořadí autentizace)
- Částečný únik informace o otisku prstu před provedením EAC
  - Hash otisku prstu je možné číst ze souboru SOD po provedení BAC

Třetí generace pasů (3G)

- V současné době teprve vzniká koncepce
- Technickou specifikací pasů třetí generace je opět dokument BSI TR-03110 verze 2 (Advanced Security Mechanisms for Machine Readable Travel Documents)
  - První verze dokumentu vznikla v roce 2008, ve verzi 1.11 dala základ druhé generace pasů. Dokument se dále vyvíjí, aktuální verze je 2.03, 03/2010.
- Specifikace nově zavádí multifunkční doklad a definuje 3 aplikace
  - Klasický elektronický pas (ePassport)
  - Aplikaci elektronické identity, „občanka“ (eID)
  - Aplikaci pro vytváření elektronického podpisu (eSign)
- Nové kryptografické mechanismy
  - PACE (Password Authenticated Connection Establishment)
  - EACv2 (Autentizace čipu verze 2, Autentizace terminálu verze 2)

PACE (3G)

- Navržen v německém BSI v roce 2007 jako náhrada za protokol BAC
- Zabezpečuje přístup do zvolené aplikace (ePassport, eID, eSign) pomocí „hesla“
- „Heslo“ tedy nahrazuje MRZ z pasů 2G a může být různého typu
  - **CAN** (Card Access Number) může být použit pro přístup k aplikaci ePassport, neblokující obvykle 6-místný číselný kód, může být statický (vytištěn na dokladu) nebo dynamický (zobrazen na displeji dokladu).
  - **PIN** blokující PIN jak jej známe z platebních karet, není uveden na dokladu, používá se ve spojení s delším neblokujícím PUKem, zabezpečuje přístup do aplikací eID a eSign
  - **MRZ** (Machine Readable Zone) klasická MRZ zóna tak, jak ji známe z protokolu BAC, může být použit pouze pro aplikaci ePassport

Porovnání BAC x PACE (3G)

- BAC
  - Navržen s důrazem na jednoduchost implementace
  - Založen na symetrické kryptografii,která byla v době návrhu běžně dostupná na bezkontaktních čipech s požadovanou rychlostí
  - Hlavním bezpečnostním problémem je jeho nevhodné použití – přístupové klíče z MRZ mají nízkou entropii
  - Není odolný proti online (skimming) ani offline (eavesdropping) útokům
- PACE
  - Založen na Diffie-Hellman dohodě na klíči autentizované heslem
  - Je odolný proti offline útokům (eavesdropping), kvalita vygenerovaných session klíčů nezávisí na složitosti hesla a proto může být pro PACE použita MRZ s nízkou entropií
  - Není odolný proti online útokům (skimming)

PACE protokol (3G)

- 1) Pas náhodně vygeneruje s, spočítá $z=E(K_{\pi},s)$, kde $K_{\pi}=KDF(\pi)$, π je heslo, z pošle terminálu společně se statickými doménovými parametry D_{PAS}
- 2) Terminál spočítá $s=D(K_{\pi},z)$ se znalostí hesla π
- 3) Terminál i pas vypočtou nové doménové parametry, dojde k jejich randomizaci na základě s

  $D_{Map}=Map(D_{PAS}, s)$, kde Map je mapovací funkce
- 4) Terminál i pas provedou anonymní DH dohodu o klíči s doménovými parametry z kroku 3)

  $K=KA(SK_{PAS}, PK_{TER}, D_{Map})=KA(SK_{TER}, PK_{PAS}, D_{Map})$
- 5) Terminál i pas spčítají session klíče $K_{MAC}=KDF_{MAC}(K)$, $K_{ENC}=KDF_{ENC}(K)$
- 6) Pas a terminál si navzájem zašlou a ověří následující tokeny

  terminál pošle: $T_{TER}=MAC(K_{MAC}, PK_{PAS})$, pas pošle: $T_{PAS}=MAC(K_{MAC}, PK_{TER})$

OKsystem

Změny v autentizaci čipu a terminálu, inspekční procedura (3G)

- Změny v EACv2
  - Protokol nyní vynucuje autentizaci terminálu před autentizací čipu
- Inspekční procedura (General Inspection Procedure)
  - 1) Výběr aplikace (ePassport)
  - 2) PACE
    - Přečtení CAN případně MRZ, navázání secure messaging na základě klíčů generovaných z PACE
  - 3) Autentizace terminálu verze 2
    - Terminál vygeneruje dočasný DH klíč, který bude použit v kroku 4) a podepsaný hash veřejné části klíče zašle pasu
  - 4) Pasivní autentizace
  - 5) Autentizace čipu verze 2
    - Pas ověří že použitý veřejný DH klíč odpovídá klíči zaslanému v kroku 3)
    - Restart secure messaging s novými klíči

Přístupová práva pro datové skupiny

DG	Obsah	PACE	Autentizace term. v2
DG1	MRZ	P	D
DG2	Foto	P	D
DG3	Otisk	P	P
DG4	Duhovka	P	P
DG14	Veř. kl. aut. čipu	P	D
SOD	Doc. sec. Object	P	D

P =povinné
D=doporučeno

OKsystem

Bezpečnostní problémy (3G)

- Odstraněn protokol BAC
- Odstraněno nevhodné pořadí autentizace čipu a terminálu protokolem EACv2 (autentizace terminálu je nyní vynucena před autentizací čipu)
- Odstraněn únik informace o otisku prstů prostřednictvím jeho hashe v souboru SOD v případě použití doporučeného nastavení přístupových práv
- Přetrvává možnost zneužití terminálových klíčů v případě jejich kompromitace i po vypršení terminálových certifikátů v důsledku toho že čip nemá hodiny reálného času

BioP@ss

- Výzkumný a vývojový projekt, kterého se v rámci infrastruktury EUREKA/MEDEA+ účastní 11 evropských firem
- Navazuje na předchozí projekt Onom@Topic+, kde byl kladen důraz na použití biometrických prvků v identifikačních dokladech. BioP@ss se zaměřuje na využití bezkontaktních technologií, vývoj multiaplikačních dokladů a pokročilých technik zabraňujících jejich zneužití.
- Projekt je naplánován Q2/2008-Q1/2011, celková kapacita 105 člověkoroků
- Účastníci projektu
  - **Česká republika**: OKsystem
  - **Francie**: Gemalto, CEA-Leti, Id3 semiconductors, NXP Semiconductors F, STMicroelectronics
  - **Maďarsko**: Compuworx
  - **Německo**: Giesecke&Devrient, Infineon technologies, NXP Semiconductors G
  - **Švédsko**: Precise Biometrics

Cíle a organizace projektu BioP@ss

- Cíle projektu
  - Vývoj bezkontaktní, bezpečné a multiaplikační mikroelektronické platformy se zabudovaným programovým vybavením, která umožní státům v Evropské unii využít potenciál elektronických čipových dokladů s biometrickými prvky a elektronických služeb založených na použití těchto dokladů.

- Organizace projektu
  - **WP1 - Řízení projektu**
  - **WP2 – Požadavky a specifikace cílové platformy**
  - WP3 – Vývoj čipové platformy
  - **WP4 – Vývoj programového vybavení**
  - WP5 – Biometrie a zabudované aplikace
  - WP6 – Bezpečnost
  - **WP7 – Demonstrace a prokázání koncepce pomocí příkladů užití**
  - WP8 – Publikace výsledků projektu a standardizace

Úloha OKsystem v pracovních úkolech

- WP1 – Řízení projektu
  - Pravidelná setkání při kterých se diskutují technické problémy, konroluje plnění úkolů a zadávají úkoly do dalšího období
- WP2 – Požadavky a specifikace cílové platformy
  - Cílem je spolupráce s ostatními partnery při stanovování požadavků na čipové karty, čtečky, hardwarová komunikační rozhraní, softwarová rozhraní a komunikační infrastrukturu
- WP4 Vývoj programového vybavení
  - Vývoj middleware dle standardu ISO 24727
  - Implementace síťové infrastruktury (Proxy, Web Service Dispatcher, Web services) dle alternativního návrhu v specifikovaného v European Citizen Card
  - Implementace driveru bezkontaktní biometrické čtečky (Interface Device Handler)
- WP7 – Demonstrace a prokázání koncepce pomocí příkladů užití
  - OKsystem má v pracovním úkolu WP7 roli koordinátora
  - OKsystem je autorem příkladu použití „elektronická občanka“ s využitím EACv2

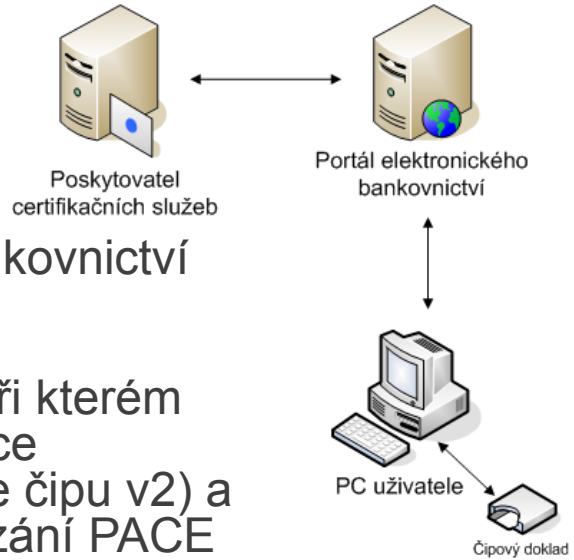
Příklad použití „elektronická občanka“ s využitím EACv2

- Příklad modeluje využití čipového dokladu v komerční oblasti, pro demonstrátor jsme si vybrali použití pro elektronické bankovnictví
- Hlavním cílem příkladu použití je zabránění útokům typu phishing. Toho je dosaženo oboustrannou autentizací internetové aplikace (služby) a čipového dokladu pomocí protokolu EACv2.
- Použití protokolu EACv2 dává veřejné správě možnost přidělovat oprávnění pro využívání čipového dokladu pouze prověřeným organizacím, podobně jako v případě elektronických pasů jedna země opravňuje druhou k možnosti čtení otisků prstů

Příklad použití „elektronická občanka“ s využitím EACv2

- Na dokladu je umístěn kvalifikovaný podpisový certifikát pro podpis transakcí
- Protokol EACv2 z třetí generace pasů nevyužíváme pro ochranu dat ale pro ochranu použití podpisového certifikátu
- Veřejná správa vystaví organizaci, která chce využívat čipový doklad certifikát, který je obdobou DV certifikátu a organizaci umožní vydávat certifikáty pro jednotlivé aplikace (obdoba terminálového certifikátu)
- Uživatelova vůle použít doklad je autentizována při přihlášení k účtu zadáním PIN pro PACE protokol, použití podpisového certifikátu je navíc podmíněno biometrickým ověřením otisku prstu

Scénář demonstrátoru



- 1) Uživatel pomocí webového portálu elektronického bankovnictví požádá o přihlášení k účtu
- 2) Přihlášení k účtu je podmíněno provedením EACv2, při kterém dojde k vzájemnému ověření autenticity bankovní aplikace (autentizace terminálu v2), pravosti občanky (autentizace čipu v2) a přítomnosti uživatele - uživatel musí zadat PIN pro navázání PACE protokolu
- 3) Uživatel si vyžádá provedení bankovní transakce, která bude podepsána kvalifikovaným podpisovým certifikátem
- 4) Vytvoření podpisu je podmíněno opětovným ověřením autenticity bankovní aplikace (auntentizace terminálu v2) a uživatel je autentizován ověřením otisku prstu.

OKsystem

OKsystem s.r.o.
Na Pankráci 125
140 21 Praha 4
tel: +420 244 021 111
info@oksystem.cz
www.oksystem.cz

Otázky?