ePaszport: bezpieczeństwo

Seminarium z Kryptologii i Ochrony Informacji, 13.06.2012

Katarzyna Kalinowska
K.Kalinowska@stud.elka.pw.edu.pl

Plan prezentacji

- ePaszport – co, gdzie i jak, po co i dlaczego?
- zabezpieczenia kryptograficzne
- zagrożenia i ataki
- zabezpieczenia kryptograficzne: rozszerzenie

ePaszport – co, gdzie i jak, po co i dlaczego?

- Standard ICAO (International Civil Aviation Organization)
- **Doc 9303:** Machine Readable Travel Documents
- **Part 1**: Machine Readable Passports

Vol 1:

Passports

with Machine Readable Data

Stored in Optical Character Recognition Format

Vol 2:

Specifications for Electronically Enabled Passports with Biometric Identification Capability

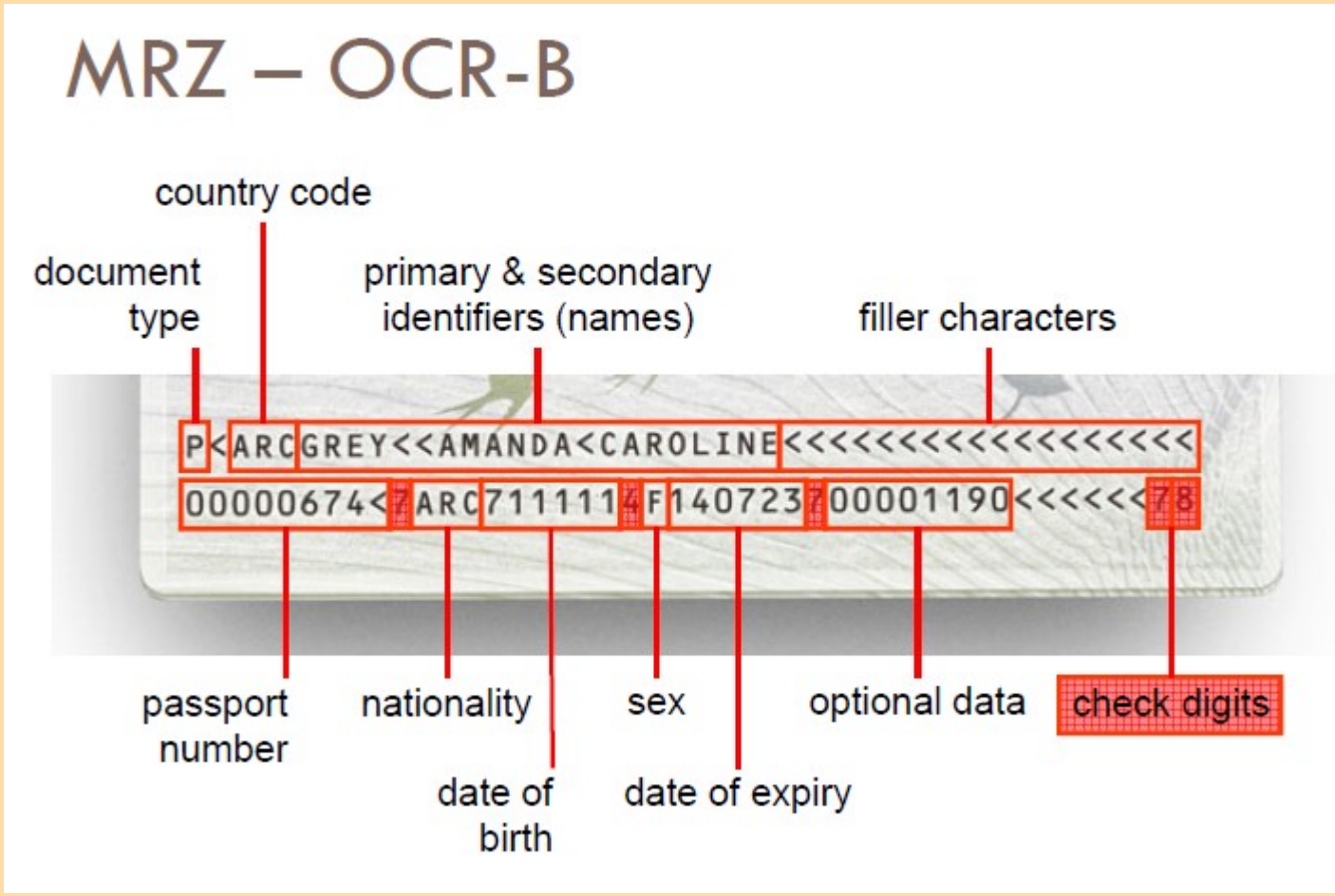
ePaszport – co, gdzie i jak, po co i dlaczego?

Machine Readable Passport

- Visual Inspection Zone
- Machine Readable Zone

ePaszport – co, gdzie i jak, po co i dlaczego?

Machine Readable Passport



ePaszport – co, gdzie i jak, po co i dlaczego?

Definicja wg ICAO:

A machine readable passport (MRP),

containing a contactless Integrated Circuit (IC) chip within which is stored:

- data from the MRP data page,
- a biometric measure of the passport holder,
- a security object to protect the data with PKI cryptographic technology,

and which conforms to the specifications of Doc 9303, Part 1

ePaszport – co, gdzie i jak, po co i dlaczego?

- Układ scalony z następującymi możliwościami:

  - komunikacja bezdotykowa, standard *proximity card* RFID (ISO/IEC 14443)

  - pojemność pamięci min. 32kB (przech. danych)

  - (wsparcie dla kryptografii symetr./asymetr.)

- zgodność z określonym modelem przechowywania danych (LDS - Logical Data Structure)

- Wymagane dane:

  - z MRP (dane osobowe, dane nt. wydawcy)

  - obraz twarzy (kol., 300dpi, JPEG / JPEG2000)

ePaszport – co, gdzie i jak, po co i dlaczego?

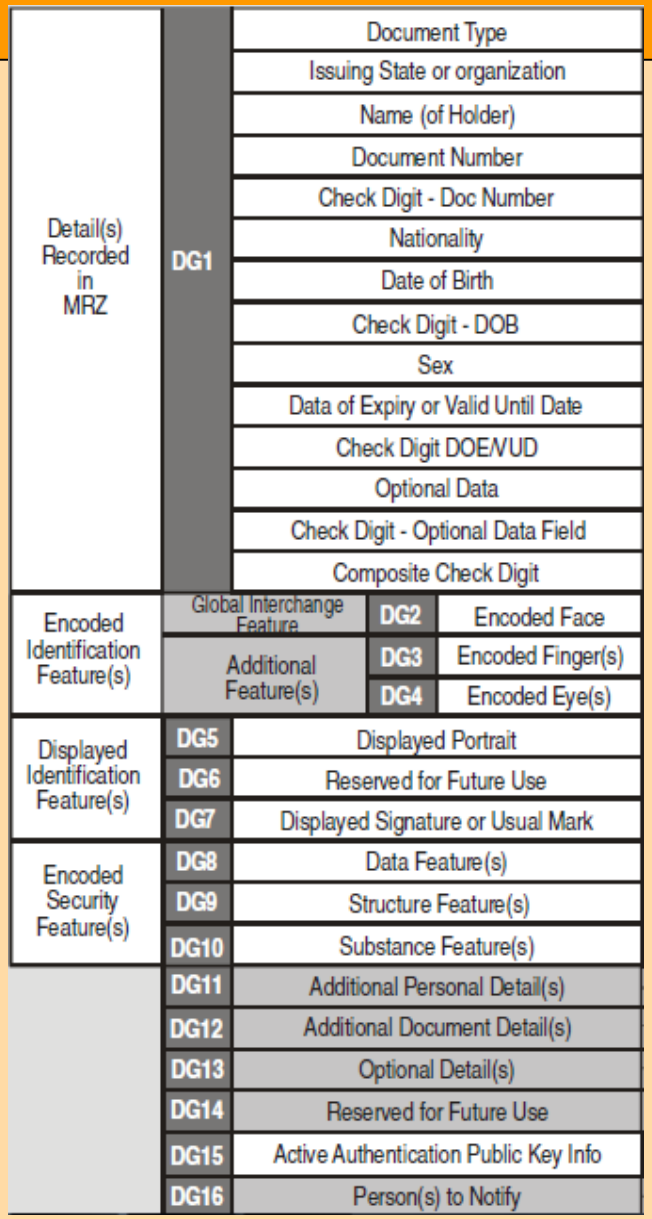
LDS - standard

- Dane podzielone na grupy (Data Groups), wymagane DG1, DG2
- Inne wymagane pliki:

  - EF.COM

  - EF.SOD

- Dane zapisywane tylko podczas wydawania dokumentu



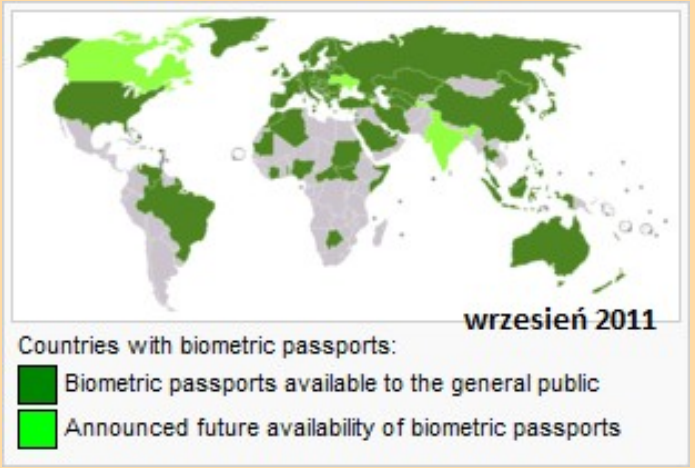
ePaszport – co, gdzie i jak, po co i dlaczego?

- Cele MRTD:

  ułatwienie kontroli granicznej

  (OCR), interoperacyjność:

  państwa, wystawcy



- Cele eMRTD:

  ulepszone uwierzytelnienie (biometria) na granicy, automatyzacja; lepsze zabezpieczenie przed atakami terrorystycznymi?

  A po co RFID?

ePaszport: zabezpieczenia kryptograficzne

- Obowiązkowe:

  - Passive Authentication (uwierzytelnienie danych)

- Opcjonalne:

  - Active Authentication (potw. autentyczności układu scalonego)

  - Basic Access Control (kontrola dostępu do mniej wrażliwych danych)

  - Extended Access Control (kontrola dostępu do wrażliwych danych biometrycznych)

ePaszport: zabezpieczenia kryptograficzne

Passive Authentication

- Potwierdza autentyczność danych
- NIE potwierdza, że dane te znajdują się na oryginalnym chipie
- Document Security Object (EF.SOD):

  - skróty DG 1-15, podpisane przez wydawcę

  - informacje nt. wydawcy (klucz publiczny)

  - ew. certyfikat wydawcy

ePaszport: zabezpieczenia kryptograficzne

Passive Authentication

- **Country Signing Certificate**
- **Document Signer Certificate** (cert. modułu odpowiedzialnego za bezpieczeństwo podczas personalizacji dokumentu)
- Terminal musi mieć dostęp do obu certyfikatów
- Terminal musi wiedzieć, czy certyfikaty są ważne (dostęp do CRLs - Certificate Revocation Lists)

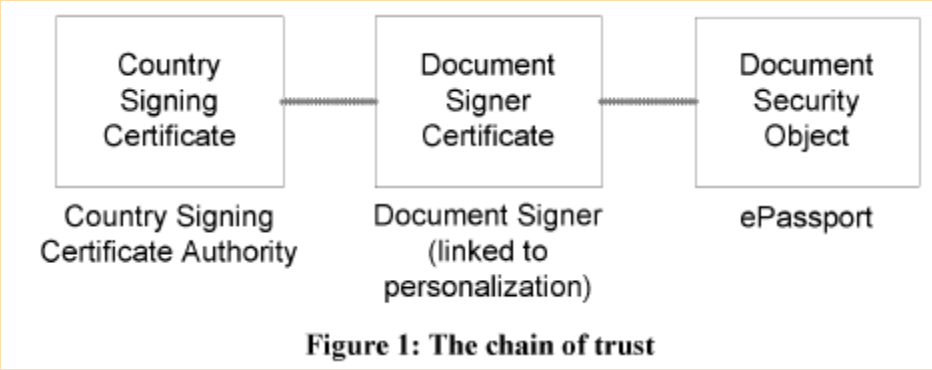
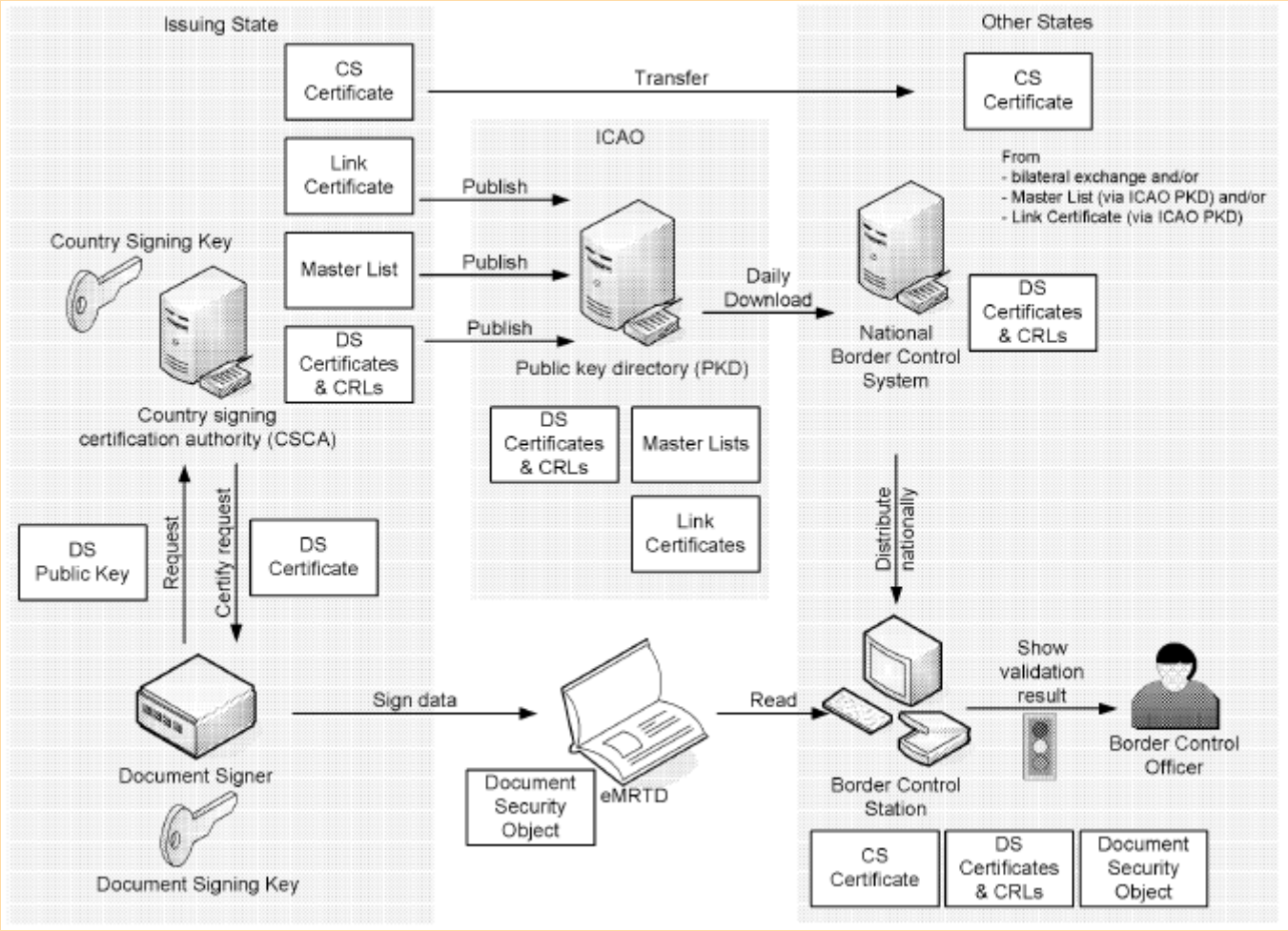


Figure 1: The chain of trust

ePaszport: zabezpieczenia kryptograficzne

Passive Authentication

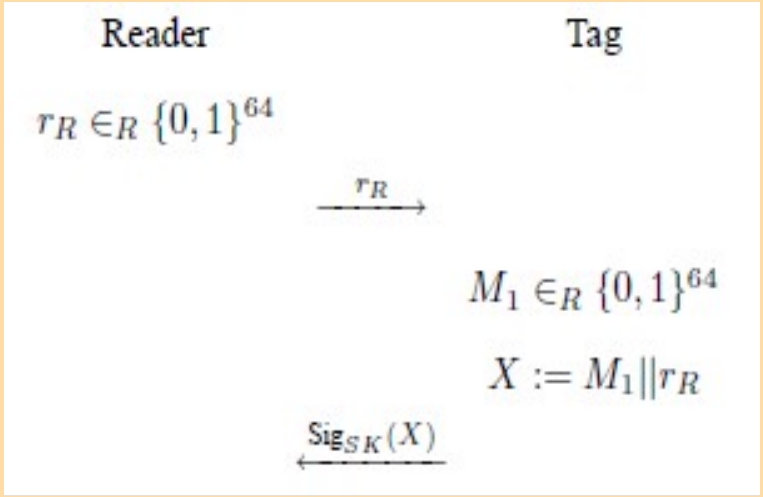


ICAO Public Key Directory

ePaszport: zabezpieczenia kryptograficzne

Active Authentication

- Potwierdza autentyczność układu scalonego (tj., że prezentowane dane nie zostały skopiowane)
- Kryptografia asymetryczna, protokół challenge-response
- Klucz publiczny w DG15 (czyli chroniony przez PA)
- Klucz prywatny w bezpiecznym obszarze pamięci
- Sig_{SK} - mechanizm podpisu z odzyskiwaniem wiadomości



ePaszport: zabezpieczenia kryptograficzne

Passive / Active Authentication

- RSA / DSA / ECDSA
- SHA-1 (!) / SHA-224 / SHA-256 /SHA-512

	RSA min. n [bit]	DSA min. p,q [bit]	ECDSA min. rozmiar rzędu punktu bazowego
CSCA Keys	3072	3072, 256	256
DS Keys	2048	2048, 224	224
AA Keys	1024	1024, 160	160

ePaszport: zabezpieczenia kryptograficzne

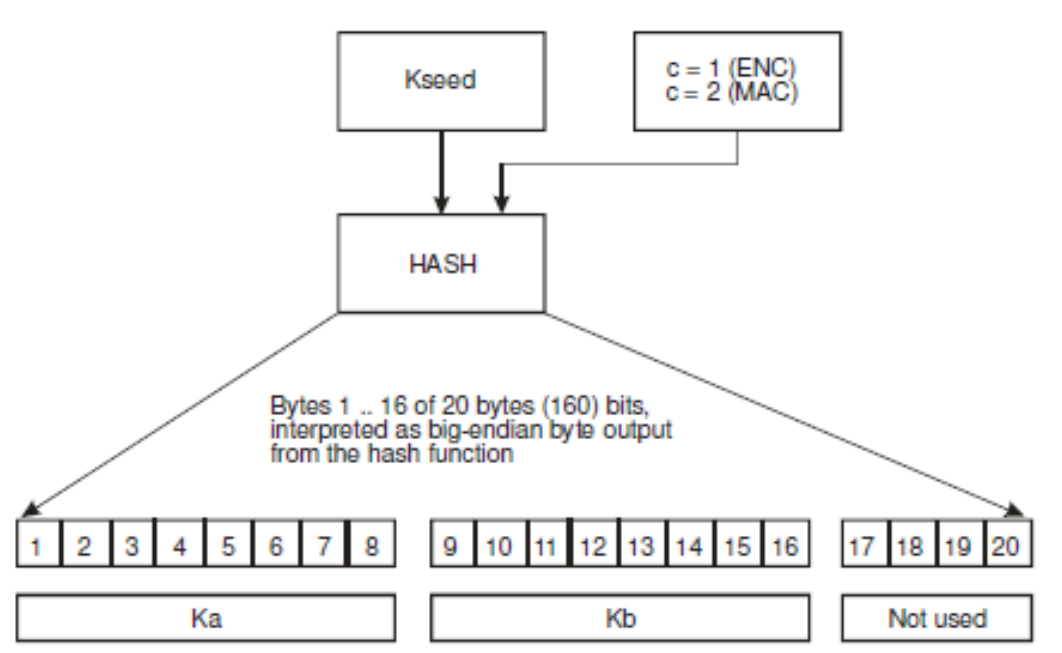
Basic Access Control / Secure Messaging

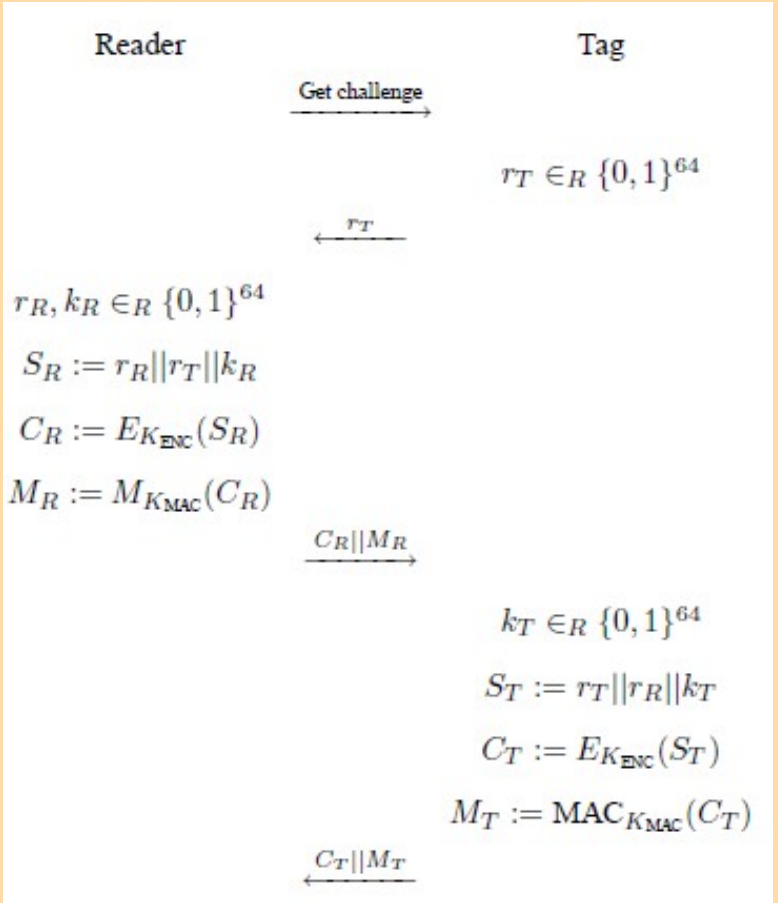
- Ochrona przed podsłuchem i nieuprawnionym odczytem
- Chip przechowuje parę kluczy Kenc, Kmac
- Terminal generuje tę samą parę używając danych z MRZ (numer dok., data urodzenia, data utraty ważności dok., +3 cyfry kontrolne)
- Terminal udowadnia, że jest w posiadaniu właściwej pary (protokół challenge-response)
- Generowane są klucze sesyjne do 3DES / MAC, komunikacja szyfrowana

ePaszport: zabezpieczenia kryptograficzne

Basic Access Control / Secure Messaging

Kseed: SHA-1 z danych MRZ, 16 najstarszych bajtów (klucze BAC) lub kr⊕kt (klucze SM)





ePaszport: zabezpieczenia kryptograficzne

Extended Access Control

- zabezpieczenie dostępu do wrażliwych danych biometrycznych (odciski palców, obrazy tęczówki)
- podobny do BAC, ale lepsze klucze
- brak szczegółowych zaleceń co do rodzaju i rozmiaru kluczy, implementacja pozostawiona zainteresowanym państwom
- proponowana też alternatywa: przechowywanie zaszyfrowanych danych

ePaszport: zabezpieczenia kryptograficzne

Extended Access Control – standard UE

- Protokół uwierzytelnienia chipa
- Szyfrowanie: 3DES, klucze z ECDH
- Protokół uwierzytelnienia terminala:

  - mechanizm oparty na PKI (dla czytników; Card Verifiable Certificates)

  - ePaszport nie ma zegara – problem dokładnego określenia ważności certyfikatów

ePaszport: zagrożenia i ataki

Passive Authentication

- Klucze publiczne nie są weryfikowane przez terminale (większość państw nie korzysta z ICAO PKD: 5/60 korzystających - stan na 2009)

Active Authentication

- Podatny na ataki *side channel* (2005, M. Witteman: analiza mocy); ale można użyć odpowiedniego sprzętu
- Może być deaktywowany poprzez manipulację pliku EF.COM (plik ten nie jest objęty PA)
- Problem *Challenge Semantics* – możliwość stworzenia systemu trackującego

2009: Jeroen van Beek, podrobienie ePaszportu

ePaszport: zagrożenia i ataki

Basic Access Control

- Niska entropia kluczy:

  - 9-cyfrowy numer dokumentu: 10^9 = 30 bitów

  - wersja alfanumeryczna: 36^9 = 46 bitów

  - data urodzenia: zał. najstarszy podróżny ma 100 lat: 365*100 = 15 bitów

  - data ważności: 365*n, n = 5/10 => 11 / 12 bitów

- Ale zazwyczaj: korelacja pomiędzy numerem dokumentu a datą ważności, możliwość określenia wieku posiadacza, sekwencyjne numery dokumentów
- Praktyczna entropia: 40-50 bitów
- Wiele demonstracji udanych ataków *brute-force*

ePaszport: zagrożenia i ataki

Basic Access Control

- klucz stały, czyli potwierdzający ma go na zawsze
- nie można zakładać, że stosunki dyplomatyczne między państwami będą uczciwe

RFID

- potajemny odczyt (standardowy zasięg: 10cm, w rzeczywistości: kilka metrów); klatka Faradaya
- śledzenie (prot. antykol. ISO 14443: chip ID udostępniany bez uwierzytelnienia)
- podsłuch (pasywny – ciężko wykryć)

ePaszport: zagrożenia i ataki

RFID

- atak na BAC - śledzenie na podstawie komunikatu o błędzie (francuski paszport – nieprawidłowy MAC/nieprawidłowy nonce)
- atak czasowy – różnica pomiędzy czasem otrzymania komunikatu o błędzie MAC a o błędzie nonce (analiza statystyczna)
- ataki wymagają jednego podsłuchu

ePaszport: zagrożenia i ataki

Biometria

Nawet założywszy silną kontrolę dostępu:

- Przechowywane pełne obrazy, a nie szablony biometryczne (interoperacyjność) – nie można zastosować np. mechanizmów prywatnej biometrii
- Po uwierzytelnieniu, udostępnienie systemowi potwierdzającemu wrażliwych danych biometrycznych (pełnych i na zawsze)
- Brak możliwości wprowadzenia innych mechanizmów ochrony prywatności np. weryfikacja typu *match-on-card*
- Kompromitacja danych biometrycznych nieodwracalna; wpływ na inne systemy ident. biom.

ePaszport: zagrożenia i ataki

...inne...

ePaszport: zabezpieczenia kryptograficzne, rozszerzenie

Supplemental Access Control

- Proponowany w związku ze słabością BAC
- Jeśli chip implementuje SAC, SAC musi być użyty przez terminal
- PACEv2 (Password Authenticated Connection Establishment) – uzgodnienie silnych kluczy sesyjnych na podstawie wspólnego sekretu o niskiej entropii (min. 6 cyfr)
- Sekret: MRZ lub CAN (Card Access Number)
- Zapewnia wzajemne uwierzytelnienie chip-terminal

ePaszport: zabezpieczenia kryptograficzne, rozszerzenie

Supplemental Access Control

1) Chip losuje liczbę, szyfruje kluczem wygenerowanym ze wspólnego sekretu, przesyła do terminala, który odszyfrowuje ją
2) Chip i terminal używają funkcji mapującej liczbę na parametry dla kryptografii asymetrycznej
3) Chip i terminal przeprowadzają protokół Diffie-Hellmana (z użyciem uzyskanych parametrów)
4) Chip i terminal generują klucze sesyjne, potwierdzają je wzajemnie

ePaszport: zabezpieczenia kryptograficzne, rozszerzenie

Supplemental Access Control

MRTD Chip (PICC)		*Inspection System (PCD)*
static domain parameters D_{PICC}		
choose random nonce $s \in_R Dom(E)$		
$z = \mathbf{E}(K_\pi, s)$	$\xrightarrow{z}$	$s = \mathbf{D}(K_\pi, z)$
additional data required for **Map**( )	$\langle - \rangle$	additional data required for **Map**( )
$\tilde{D} = \mathbf{Map}(D_{PICC}, s)$		$\tilde{D} = \mathbf{Map}(D_{PICC}, s)$
choose random ephemeral key pair $(\widetilde{SK}_{PICC}, \widetilde{PK}_{PICC}, \tilde{D})$		choose random ephemeral key pair $(\widetilde{SK}_{PCD}, \widetilde{PK}_{PCD}, \tilde{D})$
check that $\widetilde{PK}_{PCD} \neq \widetilde{PK}_{PICC}$	$\langle \frac{\widetilde{PK}_{PCD}}{\widetilde{PK}_{PICC}} \rangle$	check that $\widetilde{PK}_{PICC} \neq \widetilde{PK}_{PCD}$
$K = \mathbf{KA}(\widetilde{SK}_{PICC}, \widetilde{PK}_{PCD}, \tilde{D})$		$K = \mathbf{KA}(\widetilde{SK}_{PCD}, \widetilde{PK}_{PICC}, \tilde{D})$
$T_{PICC} = \mathbf{MAC}(KS_{MAC}, \widetilde{PK}_{PCD})$	$\langle \frac{T_{PCD}}{T_{PICC}} \rangle$	$T_{PCD} = \mathbf{MAC}(KS_{MAC}, \widetilde{PK}_{PICC})$
verify T_{PCD}		verify T_{PICC}

- Π – wspólny sekret
- Kπ =KDF(π)

- **Map / Key agreement:** DH, ECDH
- **Secure Messaging:** 3DES, AES

ePaszport: zabezpieczenia kryptograficzne, rozszerzenie

Supplemental Access Control

- wyprowadza silne klucze sesyjne
- usuwa problem *Challenge Semantics*
- nie usuwa wszystkich problemów

ePaszport: i co z tego wynika?

- ICAO ustosunkowuje się do zgłoszonych zagrożeń i ataków – suplementy do doc. 9303, raporty techniczne

- Twardy orzech do zgryzienia:
  - zapewnienie interoperacyjności
  - zmuszenie wszystkich do dostosowania się
  - poprawki w standardzie a zapewnienie wstecznej kompatybilności dokumentów/czytników

Źródła obrazków

- **s. 3**: http://en.wikipedia.org/wiki/International_Civil_Aviation_Organization
- **s. 4,5**: ICAO Regional Seminar on MRTDs, Biometrics and Border Security, 30 November - 2 December, Singapore, David Philp: ICAO MRTD STANDARDS AND SPECIFICATIONS
- **s. 6,8,17**: ICAO Doc 9303, Part 1, Vol. 2, Sixth Edition 2006
- **s. 9**: http://en.wikipedia.org/wiki/Biometric_passport
- **s. 12,13**: ICAO, A Primer on the ICAO Public Key Directory, White Paper, Version V1.5
- **s. 14, 17**: A. Juels, D. Molnar, D. Wagner: Security and Privacy Issues in E-passports
- **s. 28**: ICAO Technical Report: Supplemental Access Control for Machine Readable Travel Documents, V. 1.01, November 11, 2010

Literatura

- ICAO: Doc 9303: Machine Readable Travel Documents, Part 1: Machine Readable Passports Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability
- M. Hartmann, S. Körting, O. Käthler: A Primer on the ICAO Public Key Directory
- ICAO Technical Report: Supplemental Access Control for Machine Readable Travel Documents, V. 1.01, November 11, 2010
- Bundesamt für Sicherheit in der Informationstechnik: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTD with BAC/PACEv2 and EACv1, marzec 2012
- J. van Beek.: ePassports reloaded goes mobile, prezentacja BlackHat Europe 2009, Amsterdam, oraz http://www.dexlab.nl/epassports.html
- A. Juels, D. Molnar, D. Wagner: Security and Privacy Issues in E-passports
- S. Sheetal: Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues
- T. Chothia, V. Smirnov: A Traceability Attack Against e-Passports
- ICAO Regional Seminar on MRTDs, Biometrics and Border Security, 30 November - 2 December, Singapore, David Philp: ICAO MRTD STANDARDS AND SPECIFICATIONS
- A. Czajka: slajdy wykładu z przedmiotu Biometryczna Identyfikacja Tożsamości na Wydziale EiTI, zima 2012, w. 14: Paszport biometryczny

Dziękuję