

# The EAC for MRTD

Rafik Chaabouni

Serge Vaudenay

26 January 2010



# Outline

- MRTD?
- Standards
  - RFID
  - ICAO and BAC
  - EAC
- Solutions?

# MRTD?

- Machine Readable Travel Document



# Standards

- RFID
- ICAO and BAC
- EAC

# RFID

- ISO Standard (14443)
- Radio-Frequency IDentification (tag)



# ICAO and BAC

- International Civil Aviation Organization
- Information divided into DGs
- Passive authentication
  - for DGI (MRZ) and DG2
  - with SOD
- Identities unforgeable
- Need Access Control to avoid Privacy threats



# ICAO and BAC

- Basic Access Control
  - Symmetric-key cryptography based
- Key printed on passport (MRZinfo)
  - Low entropy (~56 bits key)
  - Vulnerable to passive adversaries
- Optional Active Authentication (AA)
  - Protects against cloning attacks
  - Vulnerable to man-in-the-middle attacks

# ICAO and BAC

- Achievements:
  - Unforgeable identities
- Dangers:
  - Unlimited permanent access with MRZinfo
  - Passive adversary threats
  - Cloning attacks threats
  - Privacy threats (release of DG2 and SOD)



# EAC

- Extended Access Control



- EACv1 2006 - 2008
- EACv2 2008 - 2009  
(latest version in November)

# EACv1

- Secure messaging based on ECDH
- Anti-cloning protection with chip authentication
- Terminal authentication for non-mandatory Data Groups
- Time-limited privileges to readers with time approximation

# EACv1

- Mandatory Data Groups remain readable (ICAO standard compatibility)
- Privacy issues remain (DG2 and SOD)
- No reliable clock in passports
- Terminal certificates usable after expiration

# EACv2

- PKI for terminals (CVCA and DV)
  - Country Verifying Certificate Authorities
  - Document Verifiers
  - Terminals
- Privacy issues resolved by
  - Access rights
  - Mandatory terminal authentication
- BAC replaced by PACE (resists active attacks)

# EACv2

- Retro-compatibility issue  
“If compatibility to ICAO is required, the MRTD shall” behave as in the ICAO standard
- Still no reliable clock in passports  
Restriction to certificates generation date from
  - National domestic CVCA certificate
  - DV authorization certificate
  - National domestic Terminal certificate

# Solutions?

- RFID Switch
  - Avoid traceability
  - Current solution: Faraday cage
  - Potential solution:  
Sensor for open/closed passport

# Solutions?

- BAC abolishment
  - DGI, DG2 and SOD cannot be protected with BAC  
can be protected with EACv2
  - No need for heavy PKI deployment  
(initial single key shared)

# Solutions?

- Time-Based Revocation
  - How to be more accurate on date?
  - Mandatory identity checks at departure to encounter national domestic terminals
  - Clock-update booths for voluntary updates
  - Future chips with real clock?



# Solutions?

- Reputation-Based Revocation
  - Decrease terminal corruption
  - Append to terminal authentication  
 $(t, n, \tau, \eta)$ -threshold authentication
  - Whole country corrupted or untrusted  
case not resolved

# Conclusion

- Acknowledgment on progression
- EACv2 still requires improvements
- Retro-compatibility issue,  
imprecise time approximation, ...
- Terminal threshold authentication,  
RFID on/off switch, ...

# Questions?

1. R. Chaabouni, S.Vaudenay.  
The Extended Access Control for Machine Readable Travel Documents.  
In BIOSIG 2009: Biometrics and Electronic Signatures, volume 155 of Lecture Notes in Informatics, pages 93-103, Darmstadt, Germany, 17.-18. September, 2009. Gesellschaft für Informatik.
2. Machine Readable Travel Documents.  
Part 1: Machine Readable Passport, Specifications for Electronically enabled Passports with Biometric Identification Capabilities. International Civil Aviation Organization – ICAO Doc 9303, 2006.
3. Machine Readable Travel Documents.  
Part 3: Machine Readable Official Travel Documents, Specifications for Electronically enabled Official Travel Documents with Biometric Identification Capabilities. International Civil Aviation Organization – ICAO Doc 9303, 2008.
4. Technical Guidelines TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents. Extended Access Control (EAC), Version 2.02. Federal Ministry of the Interior, Bundesamt für Sicherheit in der Informationstechnik, 2009.