ePassport
Contents

- Introduction
- Technologies
- Generations – 1\textsuperscript{st}, 2\textsuperscript{nd}, 3\textsuperscript{rd}
- Conclusion
Malaysia > US (VWP) > ICAO > EU (NTWG) > Germany (BSI)
Technologies

Biometrics

RFID (Radio Frequency Identification)

PKI (Public Key Infrastructure)
Major threads
- Scanning
- Tracking
- Eavesdropping
- Cloning

Standards
- ISO 14443 (specifies the use of 13.56MHz radio frequencies)
- ISO 7810 ID-3 (physical features)

32-144KB EEPROM

Data Groups
DG1  Document Details
DG2  Encoded Headshot
DG3  Encoded Fingerprint
DG4  Encoded Iris
DG5  Displayed Portrait
DG6  Reserved for Future Use
DG7  Signature
DG8-10 Data Feature
DG11 Additional Personal Details
DG12 Additional Document Details
DG13 Other Details
DG14 CA Public Key
DG15 AA Public Key
DG16 Persons to Notify
--- SOD (Security Data Element)
PKI

- Country Verifying Certificate Authorities (Country Signing CA)
  - CVCA- Signs DV certificates
  - CVCA+
- Document Verifier
  - DV- Signs IS certs and SOD fields
  - DV+
- Inspection System

- PKD (Public Key Directory) by ICAO
  - Stores registered DV’s certificates
  - CRL (Certification Revocation Lists)
ePassport – 1\textsuperscript{st} Generation

Crypto Protocols
\begin{itemize}
\item Passive Authentication (PA)
  \begin{itemize}
  \item Mandatory
  \item Goal: to allow a Reader to verify that the data in the ePassport is authentic (prevents modification based on the SOD file)
  \item PA does not tie the Tag to a passport (data correctness; cloning problems)
  \item Reader checks certificate, computes hash, match: go
  \end{itemize}
\item Active Authentication (AA)
  \begin{itemize}
  \item Optional
  \item Goal: to detect substitution and cloning
  \item Keys: AA+ (DG15); AA- (secure Tag memory)
  \item Tag must prove to the Reader that it possesses AA-
  \item Challenge-Response mechanism
    \begin{itemize}
    \item 1. R->T : 64bit rnd
    \item 2. T->R : E_{AA-}(rnd) Tag signs the rnd
    \item 3. Reader verifies the signature using its knowledge of E_{AA+}
    \end{itemize}
  \end{itemize}
\item Basic Access Control (BAC)
  \begin{itemize}
  \item Optional
  \item ...
  \end{itemize}
\end{itemize}
Basic Access Control (BAC)

- **Goal:** *tries* to ensure that only Readers with physical access to the passport can read Tag data (confidentiality, integrity)
- requires the Reader to prove knowledge of a pair of secret keys (a.k.a. access keys: $K_{\text{ENC}}$, $K_{\text{MAC}}$) that are derived from data on the Machine Readable Zone (MRZ) of the passport
- sym keys for 3DES encryption
- C-R mech to prove possession of access keys

![Diagram of Basic Access Control](image-url)

- Compute session key seed $K_s = K_R \oplus K_T$
- Generate new session encryption keys: $K'_{\text{ENC}}$, $K'_{\text{MAC}}$
ePassport – 1st Generation – Flaws

- **PA**
  - It is trivial to copy passport data using standard equipments
  - Cryptographic signature remains valid

- **AA**
  - Optional
  - Secret AA- key can be retrieved using power analysis
  - Optional security mechanisms can be disabled by removing their presence from the passport index file

- **BAC**
  - Optional
  - Low key seed entropy (can be reduced to ~25 bits)
    - Predictable passport numbers (offline dictionary attack)
    - Date of birth can be easily known
    - Expiration date (ATR codes: country, version, how to read)
  - Different error messages (passport trace: get real MAC msg with eavesdropping and use it: ”rnd number error” message means match)
  - Lack of access rules
    - for secondary biometrics (fingerprints, iris scan)
ePassport – 2nd Generation

Crypto Protocols
- Extended Access Control (EAC)
  - Goal: to provide more comprehensive authentication protocols; to promote the implementation of secondary biometrics for additional security
  - Proposes 2 new protocols (to supplement PA, AA, BAC):
    - Chip Authentication (CA)
      - Mandatory
      - Aims to replace AA (as a mechanism to detect cloned ePassports)
      - Replaces BAC session keys with new encryption and MAC keys (uses DH) (in DG14: CA_T+; in secure memory: CA_T-)
    - Terminal Authentication (TA)
      - Executed only if access to more sensitive data (secondary biometrics) is required
      - Allows the Tag to validate the Reader used in CA
      - Reader proves using digital certificates that it is authorized by both the home and visiting nations

![Diagram of ePassport protocols]

- GO/noGO
- IS cert | DV cert
- check certs get TA_R+ (IS cert)
- R
- Sig_{TA_R-}[R | SHA(CA_R+)]
- verify correctness of R, CA_R+
- Sig_{TA_R+}[R | SHA(CA_R+)]
- R
- CA_T+ , DH
- verify CA_T+ (PA)
generate own key pair (DH):
CA_R+, CA_R-
compute session key seed k_s (using DH params)
generate new session encryption keys: k_{ENC}, k_{MAC}
ePassport – 2\textsuperscript{nd} Generation – Flaws

- Dependence on BAC
  - EAC > BAC > MRZ > entropy less than 56bit

- Attacks by once valid readers
  - Tags have no clocks, they can get date info from readers
  - it is possible for Readers with expired certificates to read the contents of an ePassport Tag if the date on the ePassport Tag was not updated for a long period of time

- Compromised EAC key
  - with a stolen key, an attacker can upload false certificate with an issue date far in the future
  - chip blocks read access until the future date is reached

- DoS attacks
  - TA protocol is executed only after CA
  - malicious reader can flood the tag with invalid certificates (memory leak)
ePassport – 3rd Generation

Crypto Protocols

- Password Authenticated Connection Establishment (PACE)
  - replaces the BAC protocol
  - enables the Tag to verify that the Reader has authorized access
  - Tag and Reader share a common password which is used in conjunction with the DH protocol to provide a strong session key
    - CAN (Card Access Number) – static/dynamic
    - MRZ password – derived from the MRZ
  - Shared pwd: Y, key $K_Y = \text{SHA}(Y|3)$
ePassport – 3rd Generation

- Terminal Authentication Version 2 (TAv2)
  - must be performed before CA

- Chip Authentication Version 2 (CAv2)
  - executed only after TA
  - requires the ephemeral DH key pair
ePassport – 3rd Generation – Flaws

- Attacks by once valid readers
  - Tags have no clocks, they can get date info from readers
  - it is possible for Readers with expired certificates to read the contents of an ePassport Tag if the date on the ePassport Tag was not updated for a long period of time