



Truth and myth concerning the BAC protocol (entropy issue)

Jan Verschuren

Ministry of the Interior and Kingdom
Relations

The Netherlands



Outline

Basic Access Control (BAC)

- Motivation
- Way of operation
- Discussion
- Way forward
- Conclusions



Introduction of chip into MRTDs

- Machine Readable Travel document (MRTD) with contactless chip (eMRTD) versus traditional MRTD

- **Skimming**

Data can be read without opening the travel document;

- **Eavesdropping**

The communication to and from MRTD can be tapped.



Basic Access Control

- Measure against skimming
- Side effect: Reasonable measure against eavesdropping (Secure Messaging).
 - Reason: it is possible to find the protected information by other means.
- Data on the holder page
 - Name
 - Date of birth
 - Number of travel document
 - Expiry date
 - Sex
 - Photograph of the bearer
- Extra access control techniques for additional biometrics
- ICAO: BAC optional
- EU: BAC obligatory.



BAC operation (principle) (1)

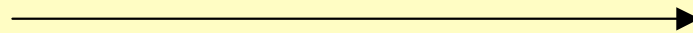
ICC Ke (encryption)

Ki (integrity checking)

Reader Ke

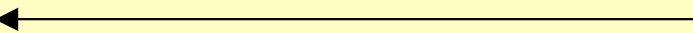
Ki

RND_{ICC}



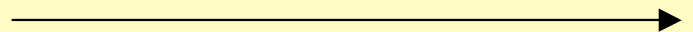
Generate RND_{reader}

RND_{ICC} , RND_{IFD} , K_{reader}



- Check integrity of message (K_i)
- Decrypt message (K_e)
- Check RND_{ICC}

RND_{ICC} , RND_{IFD} , K_{ICC}



- Check integrity of message (K_i)
- Decrypt message (K_e)
- Check RND_{IFD}

- Authentic reader
- Session keys (encryption and integrity) based on K_{reader} and K_{ICC}

- Authentic ICC
- Session keys (encryption and integrity) based on K_{reader} and K_{ICC}



Entropy of Ke and Ki

- Ke and Ki (and also session keys for encryption and integrity) are based on:
 - Documentnumber (9 alpha numeric characters)
 - $36 * 36 * \dots * 36 \approx 1.0 * 10^{14}$ possibilities
 - date of birth (YYMMDD)
 - $365 * 100 = 36,500$ possibilities
 - expiry date (YYMMDD)
 - $365 * 10 = 3,650$ possibilities for a 10 year valid document
- Maximum possible keys (ICAO) for 10 year valid document:
 - $36 * 36 * \dots * 36 * 365 * 100 * 365 * 10 \approx 1.6 * 10^{22}$ possibilities
- Using additional knowledge:
 - Guess the age of the holder:
 - $36 * 36 * \dots * 36 * \mathbf{365} * \mathbf{10} * 3,650 \approx 1.6 * 10^{21}$ possibilities
 - Guess the age of the holder and document number consists of digits only:
 - $\mathbf{10} * \mathbf{10} * \dots * \mathbf{10} * 365 * 10 * 3,650 \approx 1.3 * 10^{16}$ possibilities



Activities of ICAO

- September 2005:
 - ICAO explores activities to find a stronger mechanism than the current version of BAC as a mechanism against eavesdropping.
- February 2006:
 - Taskforce 5: two proposals
 - Increase entropy of BAC keys
 - Chip authentication



Results of exploration of ICAO

- Increase entropy of BAC keys
 - No protocol change
 - No chip OS consequences
 - Inspection system consequences
- Chip authentication
 - Protocol change
 - Chip OS consequences
 - Inspection system consequences



Increase entropy of BAC keys

- Three possibilities presented
 - Use optional data field in MRZ
 - Use entire line 2 of MRZ
 - Use complete MRZ.



ICAO's way forward with respect to BAC

- At present: no modification of BAC:
 - Modification of BAC at this moment would imply heavy organisational impact.
 - Skimming: BAC is effective against skimming (primary objective)
 - Eavesdropping:
 - Within the present BAC standard, sufficient ways exist to obtain enough protection against eavesdropping (e.g. by issuing document numbers in a randomised way, by using alphanumerical document numbers).
- Future
 - New consideration of strength of BAC:
 - Increase entropy of BAC keys;
 - Chip authentication (EAC);
 - EU: chip authentication compulsory if fingerprints are stored on the chip (DG 3);
 - ...



Conclusions of ICAO

- BAC is primarily meant to protect against skimming.
BAC is a sufficiently strong mechanism against skimming.
- ICAO explored possibilities to obtain a higher level of protection against eavesdropping.
- ICAO:
 - Present:
 - The standard for BAC is not adapted. If states aim for a higher level of protection against eavesdropping ICAO advises them to consider
 - issuance of random document numbers
 - issuing document numbers consisting of alpha numerical characters
 - ...
 - Future
 - ICAO will consider new countermeasures against eavesdropping:
 - Increase entropy of BAC keys
 - Chip authentication
 - ...