Supplemental Access Control – the next generation of ePassports

Carsten Müller, Senior Business Advisor ID Systems
Madrid, June 2014

Giesecke & Devrient
Creating Confidence.

PACE – The basis for SAC

PACE is an Access Control Mechanism for eDocs required for privacy reasons

- Protects electronic data against unauthorized access
- Establishes a secure connection between chip and terminal
- Protects against skimming and eavesdropping
- Supplemental to BAC

PACE was invented to overcome weakness of BAC

- Design based on asymmetric cryptography (Diffie-Hellman)
- Provides cryptographically strong session keys independent of the entropy / length of "password" input
- Adds flexibility and convenience for the user AND for the issuing authority using different "passwords"
  - Personal Identification Number
  - Card Access Number
  - Machine Readable Zone

PACE has been approved in ICAO NTWG as "Supplemental Access Control"

What is SAC – Supplemental Access Control?

PACE allows different ways of mapping for the domain parameters used for Elliptic Curve Cryptography:

- Generic mapping (original design from the German BSI)
- Integrated mapping

Get the nomenclature right:

☞ **PACE** is the name of an access control mechanism (like BAC or EAC)

- **PACE v1:** refers to PACE with generic mapping
- **PACE v2:** extended version for generic and integrated mapping

☞ **SAC** is the name of the Technical Report from ICAO (TR SAC)

- The TR SAC specifies a supplementary control mechanism based on **PACE v2**

☞ MRTDs implementing SAC according to the TR SAC support integrated and generic mapping of the domain parameters

SAC ePassports: Specifications, Legislation & Certification

Relevant Specifications:

- ICAO Technical Report „SAC for MRTDs“, V1.01, 11th Nov 2010
- BSI Technical Guideline TR-03110, V2.10, 20th March 2012
  - Part 1 – eMRTDs with BAC/PACEv2 and EACv1
  - Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)
  - Part 3 – Common Specifications

Legislation:

- EU regulation EC1030/2002 + 3770 (2009)
  - ePassports in the EU must support SAC starting from December 2014

Protection Profiles:

- EU binding PP is available since 22nd March 2012
  - MRTD with ICAO Appplication, EAC with PACE: **BSI-CC-PP-0056 v2**
  - Only this PP will certify EU compliant passports

Impact of SAC for the Chip OS & the Personalization System

Chip operating system:

- Chip OS of passports has to implement PACE v2 acc. to TR SAC
- Certification acc. to BSI-CC-PP-0056 v2 is required
- Chip OS has to support BAC and SAC

Electrical & optical personalization:

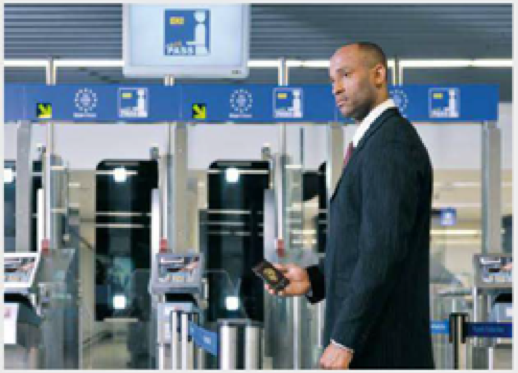
- Data preparation has to support PACE enabled passports
- Additional files / DG necessary for PACE
- No change in hardware for chip encoding
- Card Access Number can be optionally personalized on data page

- Quality control at personalization site must support PACE

☞ QA system must implement PACE algorithm, readers do not need to be updated

Impact of SAC for the Border Control Systems

- Border Control Software needs to be upgraded to support PACE enabled ePassports
- Inspection system chooses if BAC or PACE is used
- If the ePassport and the inspection system support PACE, it is **MANDATORY** to use PACE
- All ePassports with PACE must still support BAC
- Existing hardware don't need to be changed
- Keys are derived from passwords (either MRZ or CAN, CAN can be typed in manually (or scanned))



☞ No deadline yet visible to deprecate BAC

☞ Gradual change over the next 10-20 years from BAC to PACE

☞ Introduction step by step possible:

1. Introduce SAC enabled passports first
2. Upgrade the BCS afterwards

G&D's offering

Dual Sourcing & Backup Production Facilities

1 Documents:

- Complete (printed) ePassport documents
- Polycarbonate data pages with chip
- eCovers (Inlays + passport covers)
- Inlays (embedded modules + antenna)
- Modules (chip + OS)

2 Systems & Services:

- Data Capturing Systems
- Personalization Systems
- CSCA, DSCA, CVCA
- Key directories
- Border Control and Verification Systems

G&D’s Passport OS: STARCOS® 3.5PE

- G&D’s native OS developed for next generation of ePP
- Optimized write / read performance (e.g. fast border control)
- Support of two personalization methods
  - Standard ISO
  - Proprietary PDI with min. 10% time-savings compared to ISO personalization
- Security protocols / mechanims of COS could be defined at personalization time
  - ☞ Smooth transition from one (electrical) passport generation to the next
  - ☞ Beneficial for stock management

- We have been the 1st supplier worldwide with a Common Criteria certified solution for the PACE protection profile **(BSI-PP-056v2 SAC/BAC/EAC)**

  ☞ Mandatory for EU passports from Dec’ 2014 onwards

  ☞ Protection profiles of vendors carefully to be checked

Deutsches IT-Sicherheitszertifikat

[illegible]

Project References - PACE / SAC already in usage

German National eID

- ***Going Live***: Nov' 2010
- ***G&D's Role***: Main supplier of chip inlay
- ***Chip OS technology:***: Native STARCOS 3.5 ID
- ***Highlights:***
  - First PACE implementation worldwide
  - First CC certified c'less signature functionality

Macao SAR Resident eID

- ***Going Live***: Nov' 2013
- ***G&D's Role***: Main contractor overall system incl. docs
- ***Chip OS technology:***: JavaCard Sm@rtCafé Expert 7.0
- ***Highlights:***
  - First country migrating from pure contact based to pure contactless card interface

Kosovo ePassport

- ***Going Live***: Q4 / 2013
- ***G&D's Role***: Main contractor overall system incl. docs
- ***Chip OS technology:***: Native STARCOS 3.5 PE
- ***Highlights:***
  - First certfied SAC e-Passport worldwide complying to BSI-PP-056v2 SAC/BAC/EAC

Kosovo National eID

- ***Going Live***: Q1 / 2014
- ***G&D's Role***: Main contractor overall system incl. docs
- ***Chip OS technology:***: Native STARCOS 3.5 ID
- ***Highlights:***
  - First country following similar approach to German NeID

...

Many thanks for your attention!

Carsten Müller
Title: Senior Business Advisor ID Systems

Phone: +49 89 4119 2895
Fax: +49 89 4119 2778
Cell: +49 173 3513583
Email: Carsten.Mueller@gi-de.com