Use Case: Migrating to the 3rd Generation ePassports

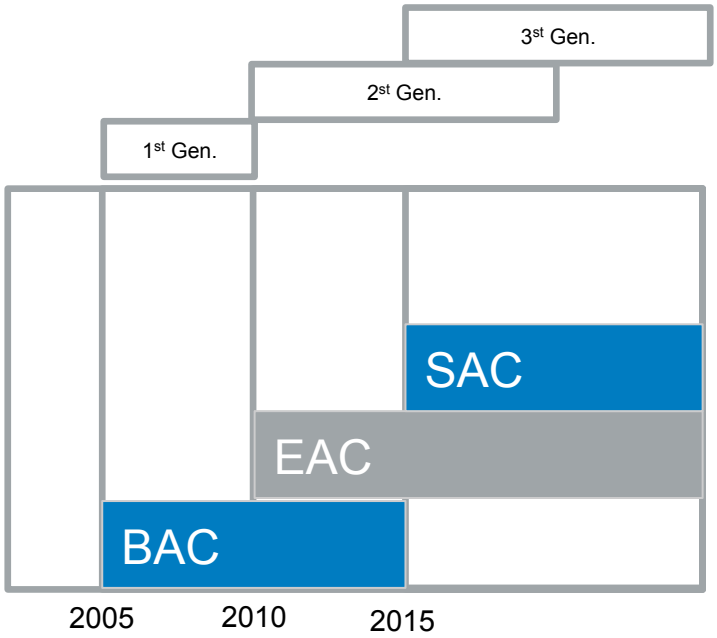
From a security Infrastructure vendor point of view

utimaco®

Jose G Rivera, CISSP,

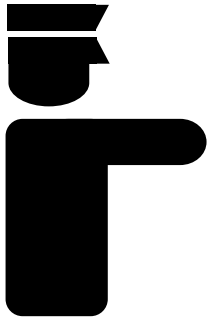
The Landscape today

- Three generation of security mechanisms are in used today
- **BAC: Basic Access Control**
  - by ICAO DOC 9303
- **EAC: Extended Access Control**
  - by BSI in Version 2
- **SAC: Supplemental Access Control**
  - by ICAO in 2010



The evolution of the ePassport security mechanism

1st Generation - BAC



- mechanism specified to ensure only authorized parties] can wirelessly read personal information from passports with an RFID chip
- It uses data such as the passport number, DOB, and expiration date to negotiate a session key
- The data used to encrypt the BAC communication can be read electronically from the bottom of the passport called the Machine Readable Zone (MRZ)

2nd Generation – EACv1 (2009 – 2014)

Chip authentication (For strong session encryption)

- Authenticate the chip and prove that the chip is genuine. Only genuine chip can implicit communication securely;
- Establish strong secured communication channel whereby it uses ship-individual key pair with strong encryption and integrity protection.
- Have an add on Basic Access Control (BAC) with protection against skimming and eavesdropping.

2nd Generation – EACv1 (2009 – 2014

utimaco®

Terminal authentication (Access restricted to authorized terminals)

- ***Terminal authentication*** **(TA)**: Is this terminal allowed to read the sensitive data from the ePassport?
  - **Card Verifiable Certificate (CVC)** from a **document verifier (DV)**. The inspection system's certificate is valid only for a short time period, typically between 1 day to 1 month.
  - An inspection system may have several CVCs installed at any time, one for each country that allows it to read sensitive data.
  - The CVC allows the inspection system to request one or more items of sensitive data, e.g. fingerprints.
- Document verifier certificate is granted from the country verification certificate authority (CVCA).

3rd Generation – SAC (from Dec. 2014 on)

- **Combination of measures for data transaction:**
- PACE - generates keys for secure messaging using **asymmetric encryption**
- Secure Messaging – using key generated by PACE
- Terminal Authentication
- Passive Authentication – checks if passport data has been manipulated
- Chip Authentication – proves authenticity of security IC (same mechanism as active authentication as defined in ICAO)
- Secure Messaging - uses session key generated during chip authentication

What do we need to keep in mind?

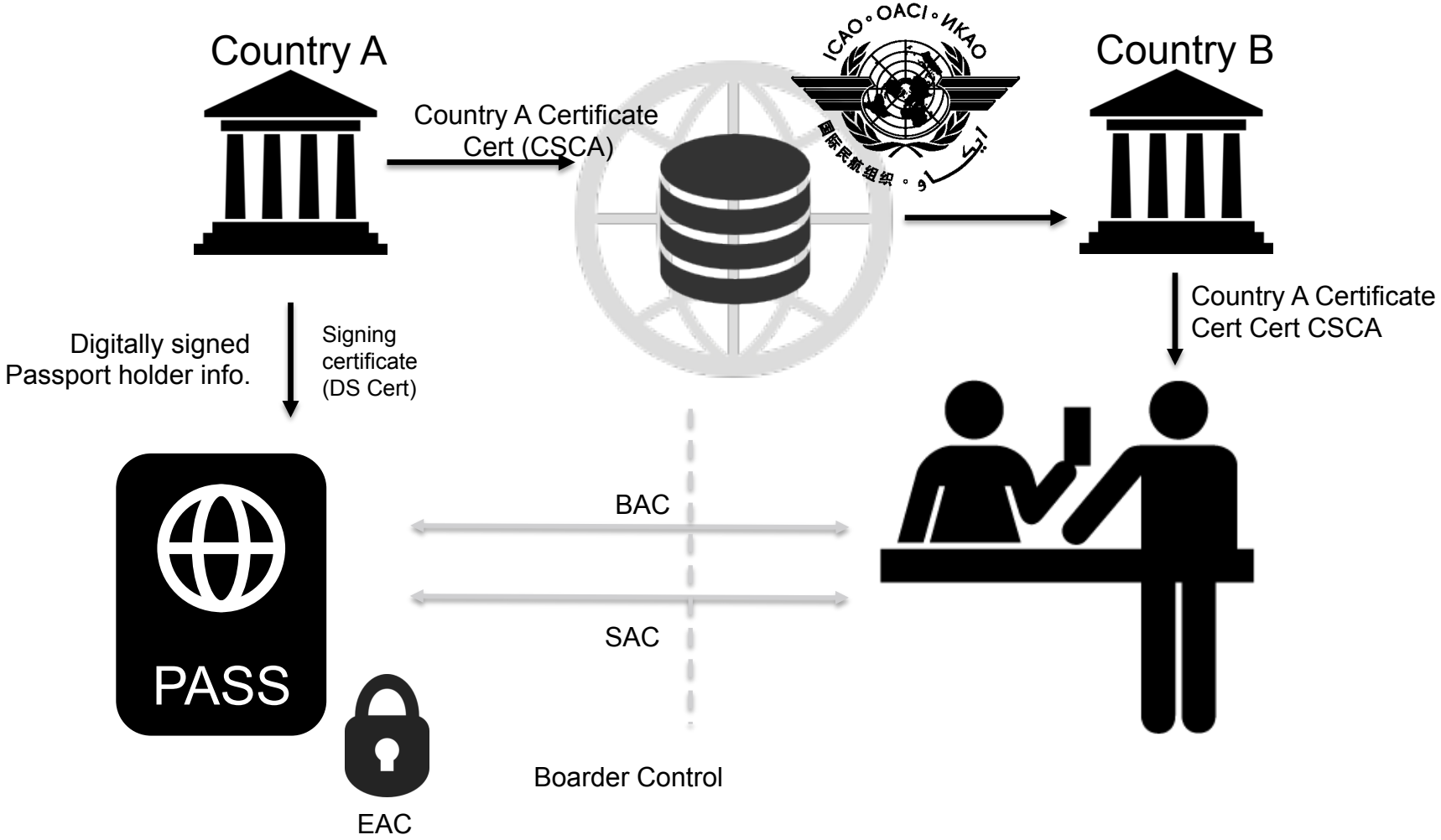
- Our entire solution must be “capable” to support legacy protocols, (e.g. BAC has been around since 2005, and it will be around for you years).

- When planning, designing, and implementing a solution you must always keep in mind the basic three Information System Requirement Principles (CIA: Confidentiality, Integrity, and Authentication)

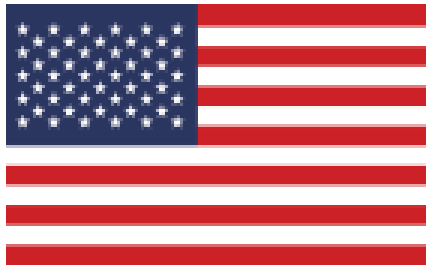
- Encryption: It is just not about simply implementing encryption anymore: Who, and how are those Encryption Keys being Managed? Where exactly are these keys being generated, stored, protected? How are they managed?

-

ePassport system operation



Who is Utimaco?



- German Based company
- U.S headquarters in Palo Alto, CA

- **Hardware Security Modules** (HSMs)
  - Key Management (Shared Custody, Split Knowledge)
  - Off loading cryptographic operations to a FIPS level 3 / FiPS Level 4 compliant device
  - - They are used with your “Hardware Infrastructure and/or Applications” (Keys generate in software are simply insecure)
  - They should always be used when implementing PKI

Conclusion

- The Infrastructure for ePassports
  - Security equipment should support evolving standards
  - At the same time support for previous standards
    - ePassports that were issued many years ago may still be in use
  - Clear understanding of security mechanism
  - Product requirements:
    - Maximum Flexibility in upgrading
    - Open and security execution environment
    - High product quality
    - to meet short- and long-term needs

Thanks for your attention!

Jose Rivera

Jose.Rivera@utimaco.com

Utimaco Inc.

3790 El Camino Real
Palo Alto, CA 94306
United States of America
Tel +1 650 485 4920
Fax +1 650 485 4921