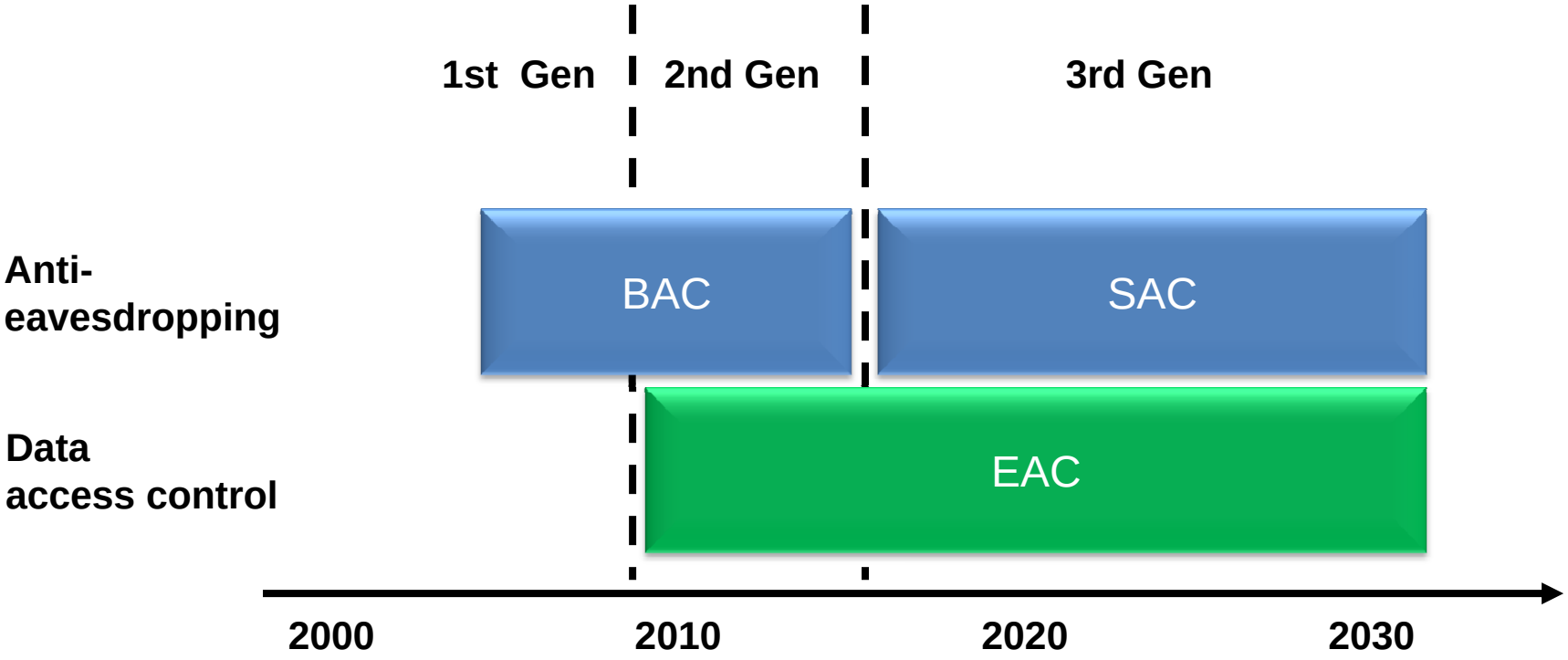
Moving Towards 3rd Generation ePassports

Joe Soh
Marketing Manager

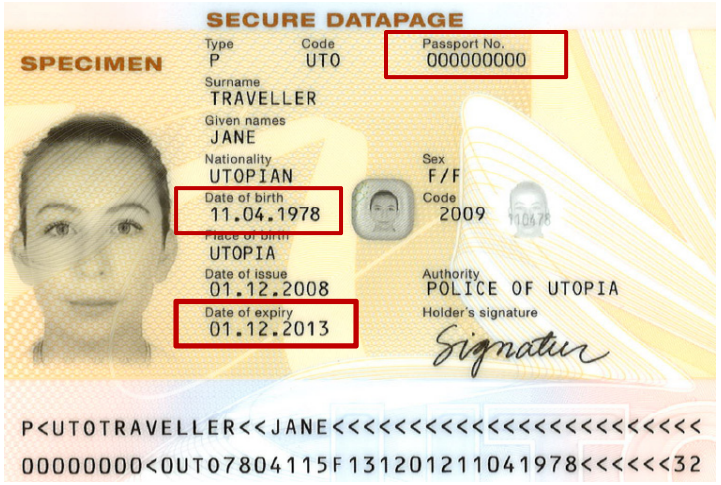
29 Nov 2011

Natural evolution of the ePassport...



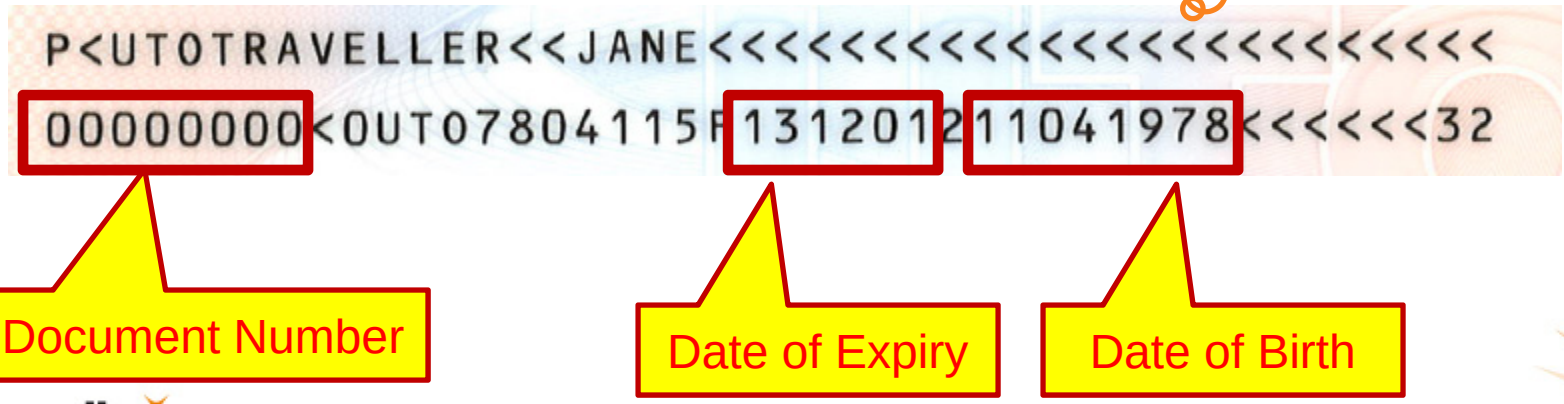
- Europe mandates SAC in 2014 (Passport and Residence Permit)
- ICAO recommends SAC for ePassports worldwide in 2014

Basic Access Control limitations



- Document number
  - Numeric : 109 possibilities - > 30 bits
  - Alpha Numeric : 369 possibilities -> 46 bit
- Date of birth
  - Date of Birth
  - Oldest Traveler 100 years : 365 * 100 possibilities ->15 bit
- Date of Expiry
  - 5 years validity : 365 * 5 possibilities -> 11 bits
  - 10 years validity : 365 * 10 possibilities -> 12 bits

One Million Billion Combinations
Is this secure enough?



Moore’s Law

- Every 18 months
  - Double speed or
  - Half the price

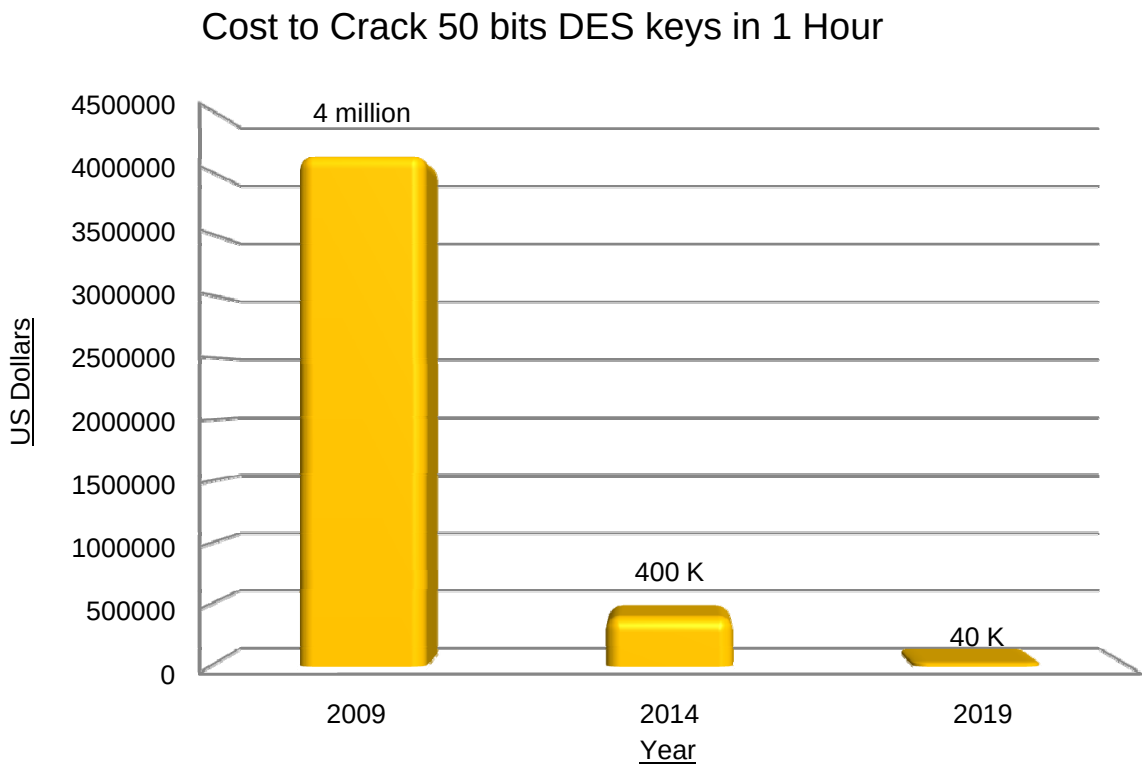
1982 Osborne Executive Portable Computer vs Modern Day Smart Phone

Source : http://en.wikipedia.org/wiki/Moore's_law

Moore's Law

- 1998: Deep Crack
  $250K → 88,000,000,000 DES keys/s

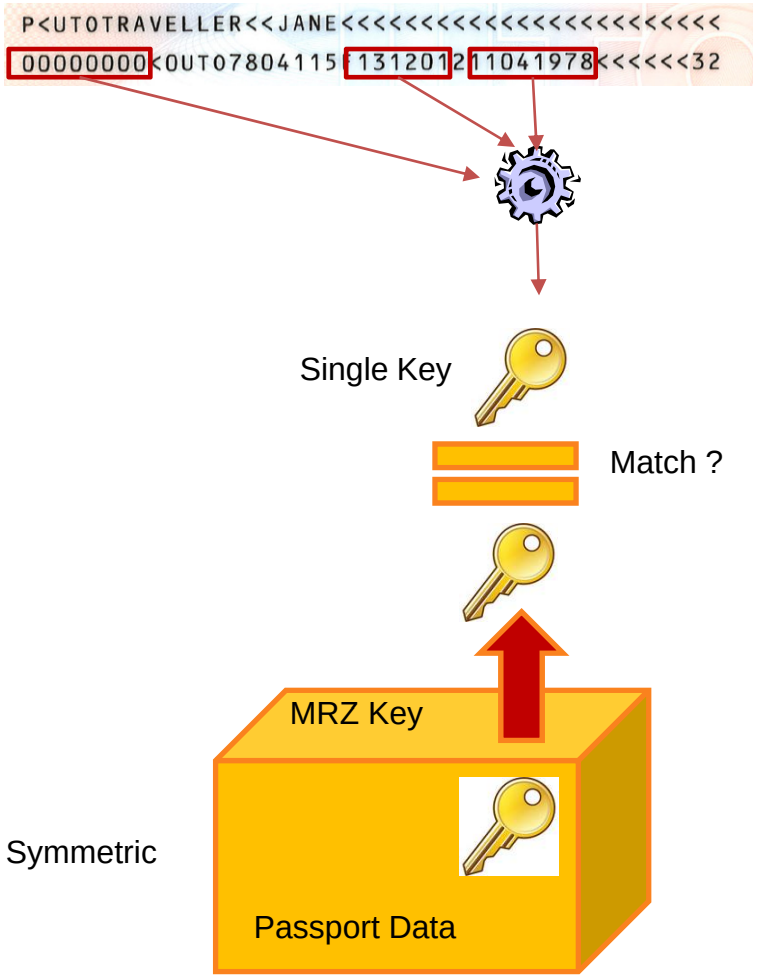
- 2006: Copacobana
  $10K → 65,000,000,000 DES keys/s



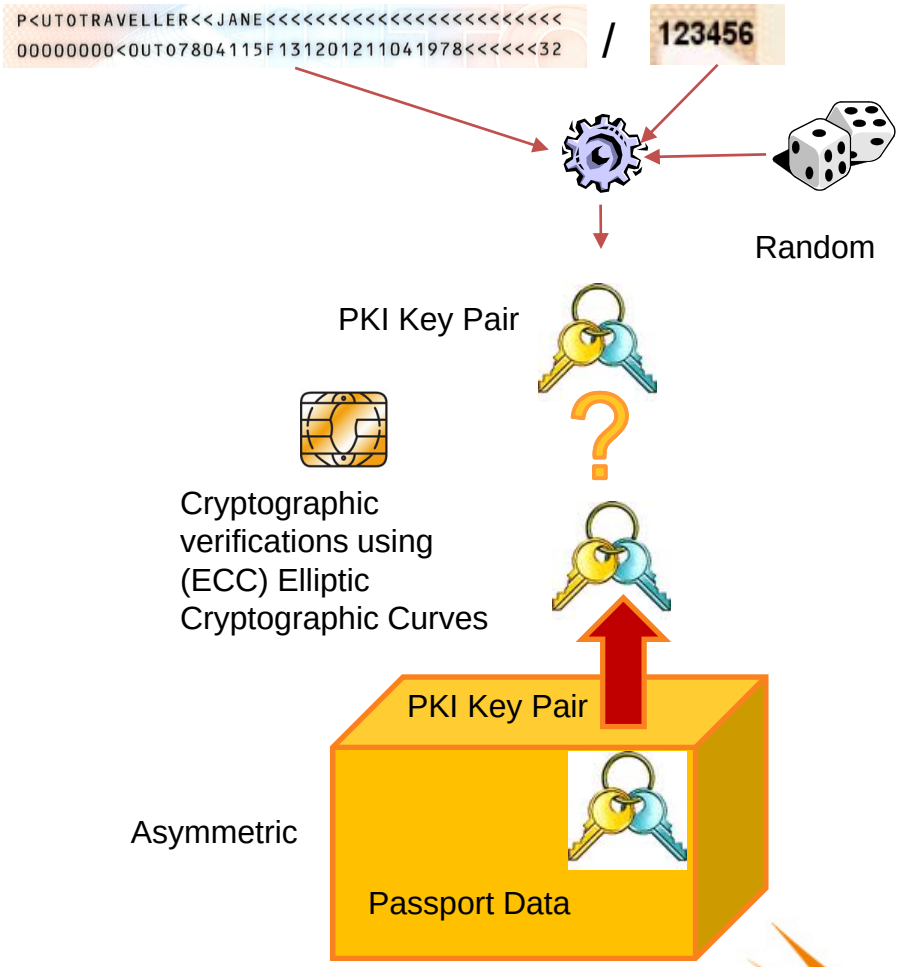
Source : Adapted from ISO/IEC JTC1SC17 WG3 /TF5
Tom Kinneging's Presentation on SAC

BAC vs SAC

BAC



SAC



Supplemental Access Control

Static Domain Parameter

PACE Key

Random

Z

PACE Key

Static Domain Parameter

Random

Map

Dynamic Domain Parameter

Map

Random

Static Domain Parameter

Private Key

Public Key

Dynamic Domain Parameter

KA

Shared Secret Key

KA

Public Key

Private Key

Dynamic Domain Parameter

K_{MAC}

K_{ENC}

K_{MAC}

K_{ENC}

K_{MAC}

Public Key

MAC

TOKEN

TOKEN

MAC

Public Key

K_{MAC}

K_{MAC}

Public Key

MAC

TOKEN

TOKEN

MAC

Public Key

K_{MAC}

TOKEN

Compare

TOKEN

TOKEN

Compare

TOKEN

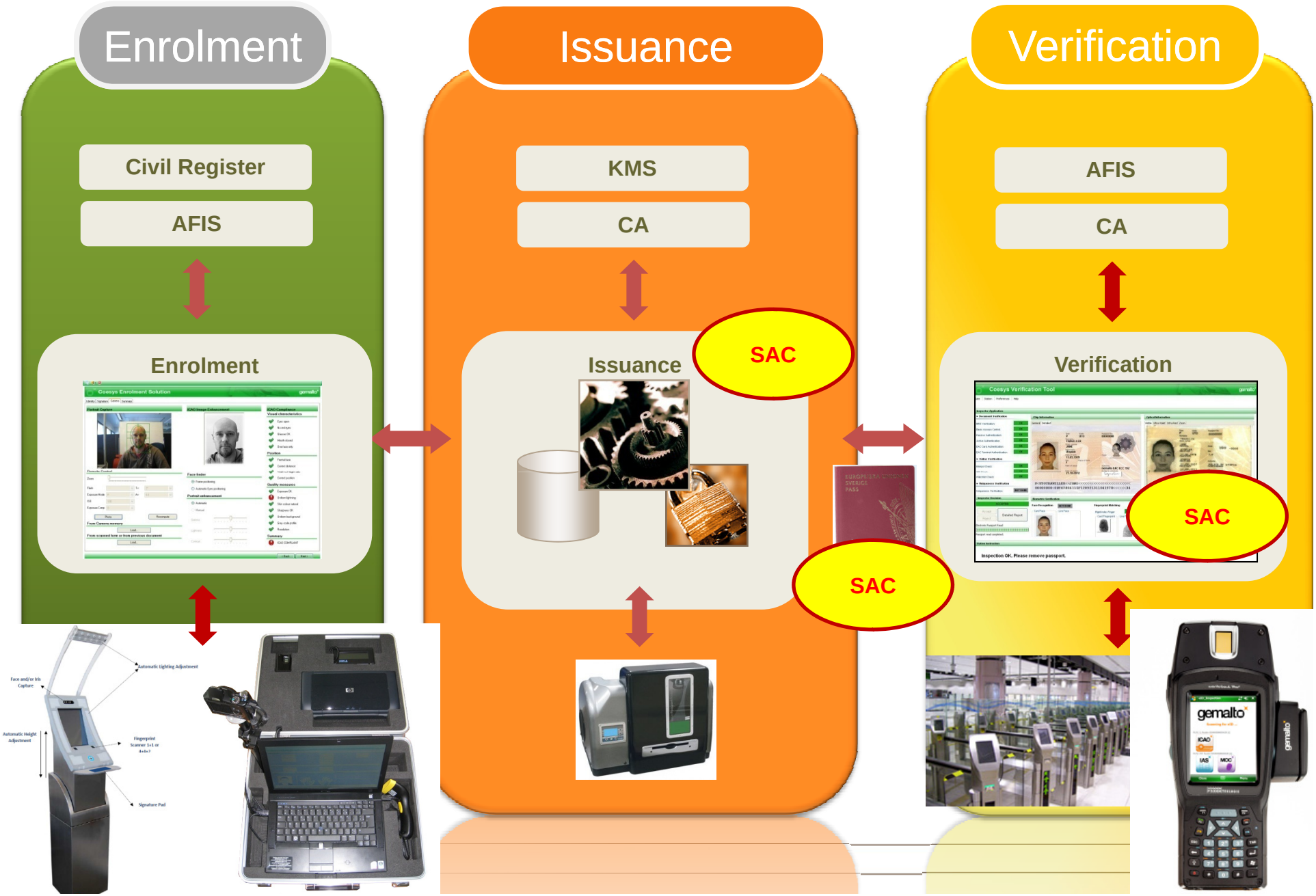
Secure Messaging Established

In Summary

- SAC similar to BAC, main target is to prevent skimming but solves the issue of low entropy

- Thanks to PKI and Elliptic Cryptographic Curves (ECC) implementation, SAC provides more security than using BAC MRZ alone

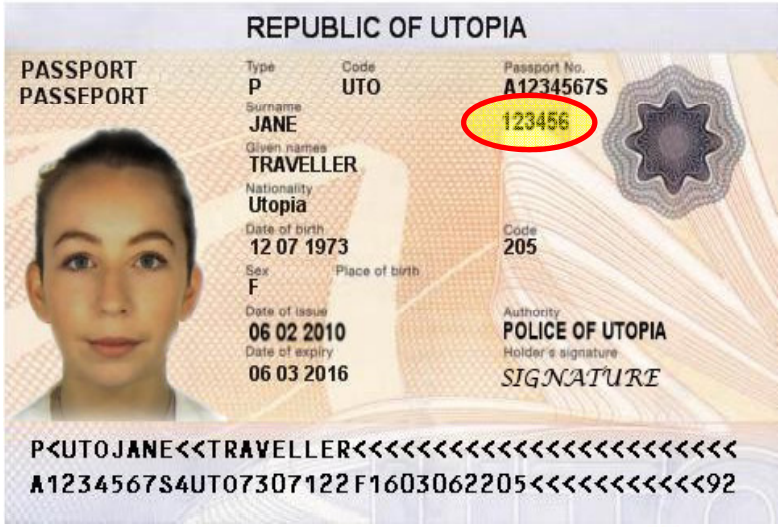
Minimum impact to existing infrastructure



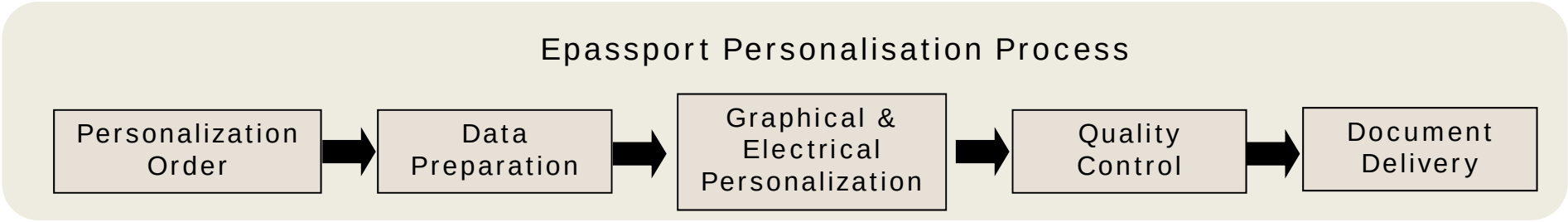
SAC impact on ePassport

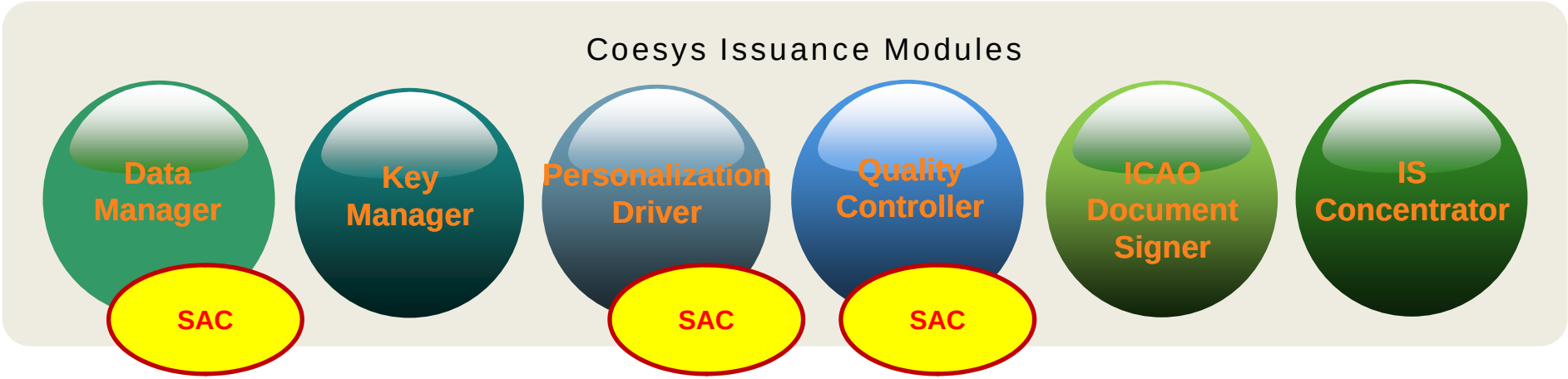
- ePassport OS must now support
  - Both SAC and BAC
    - SAC mode using MRZ / CAN
  - Operating System inside the chip needs to be upgrade to support SAC Mechanism
  - Existing Passports needs to be replaced

- Planned Migration in Phases
  - New Passports application
  - Expiring Passports for Replacement

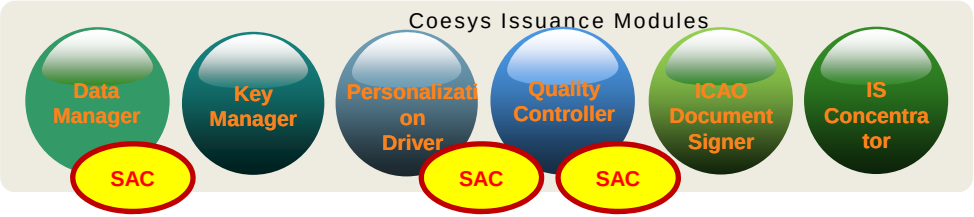


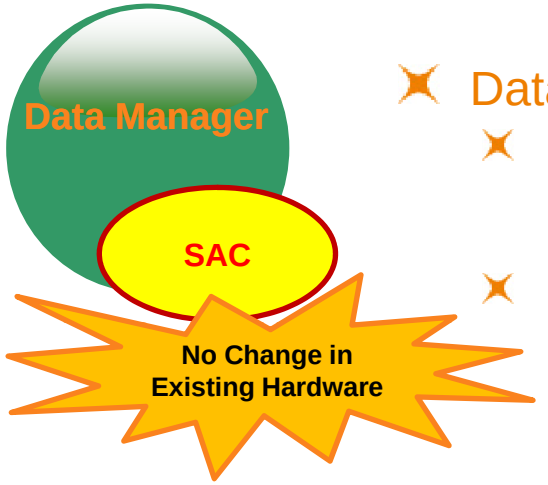
Issuance Impact for SAC





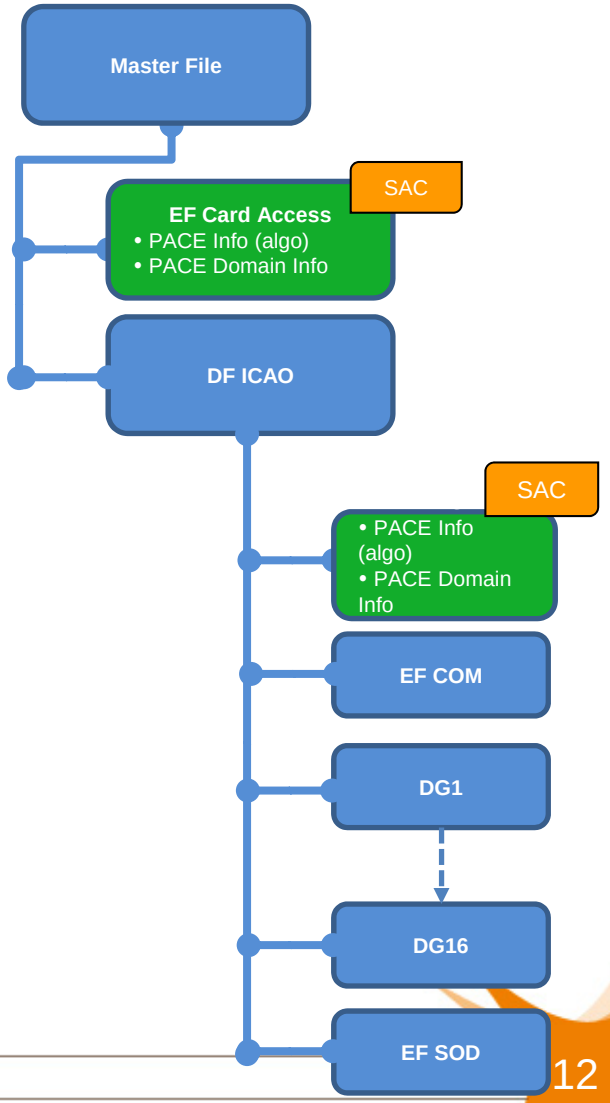
Issuance Impact

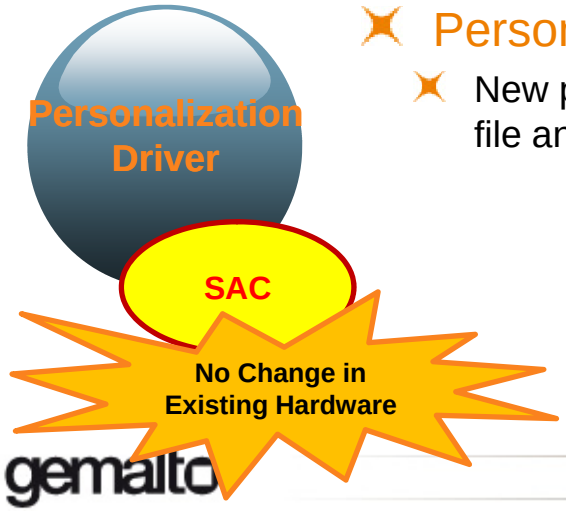




Data Preparation

- Data preparation and personalization of SAC data: PACE Info, PACE Domain parameters, Password
- Changes in ICAO LDS: PACE security parameters shall be stored in DG 14 in addition to the Card Access file.

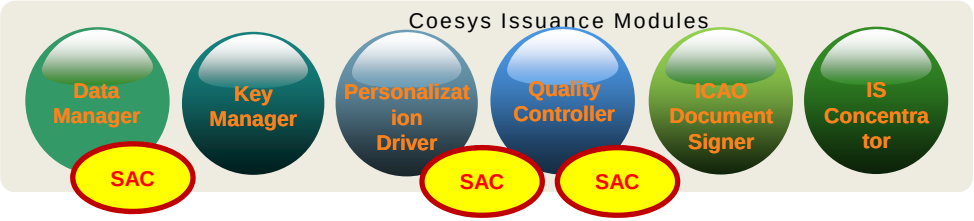




Personalization Scripting

- New personalization script for Card access file and DG14 file personalization

Issuance Impact



Quality Control

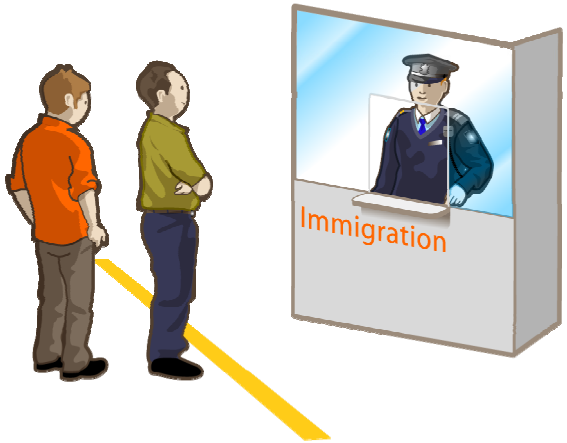
- Support for advanced cryptography mechanisms to protect citizens data during reading
- Various Access control mechanisms to be validated: BAC, SAC – MRZ, SAC - CAN

Graphical Printing

- New graphical layout for Card Access Number printing.
  - Most existing laser /inkjet / thermal epassport printers in market should be able to support the printing of additional CAN number

Border Control Inspection System Impact for SAC

- Readers
  - MRZ readers need to be upgraded to full page OCR readers if CAN number is used to generate PACE Keys



No Changes in Existing Hardware

- Terminals
  - Software Support for new Inspection Procedure
  - Choice to perform
    - BAC or
    - SAC
  - Support all combinations of algorithm
  - Support the exchange of ephermal public keys
  - Generation of random numbers
  - Support all ECC domain parameters
  - Support Secure messaging based on AES

No Changes to Operational Flow

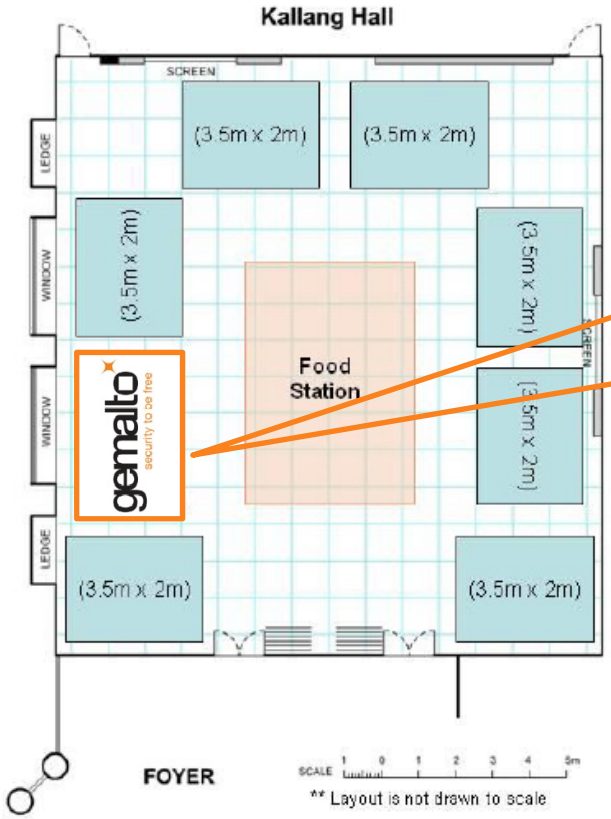
Citizen and Border Control Personnel will not notice or realise whether BAC or SAC is being performed

- Compatible with automated border control

Benefits of SAC

- Travellers: Holding on to a secure document! Ease of mind that data is not easily skimmed
- Border Control: same hardware equipment
- Passport issuers: enhanced security with minimal effort
- In line with ICAO Worldwide 2014 recommendation

Thank you
Please visit us at our booth.



gemalto
security to be free

gemalto