Security Mechanism of Electronic Passports

Petr ŠTURC
Coesys Research and Development

gemalto
security to be free


gemalto
security to be free


000 0012 3456
PURCHASING
EXPIRES END
00/00 V
4000
VALID FROM
00/00
gemalto
security to be free


opencard
opencard
opencard
opencard
gemalto
security to be free

gemalto
security to be free

Smartcard

CPU 16/32 bit

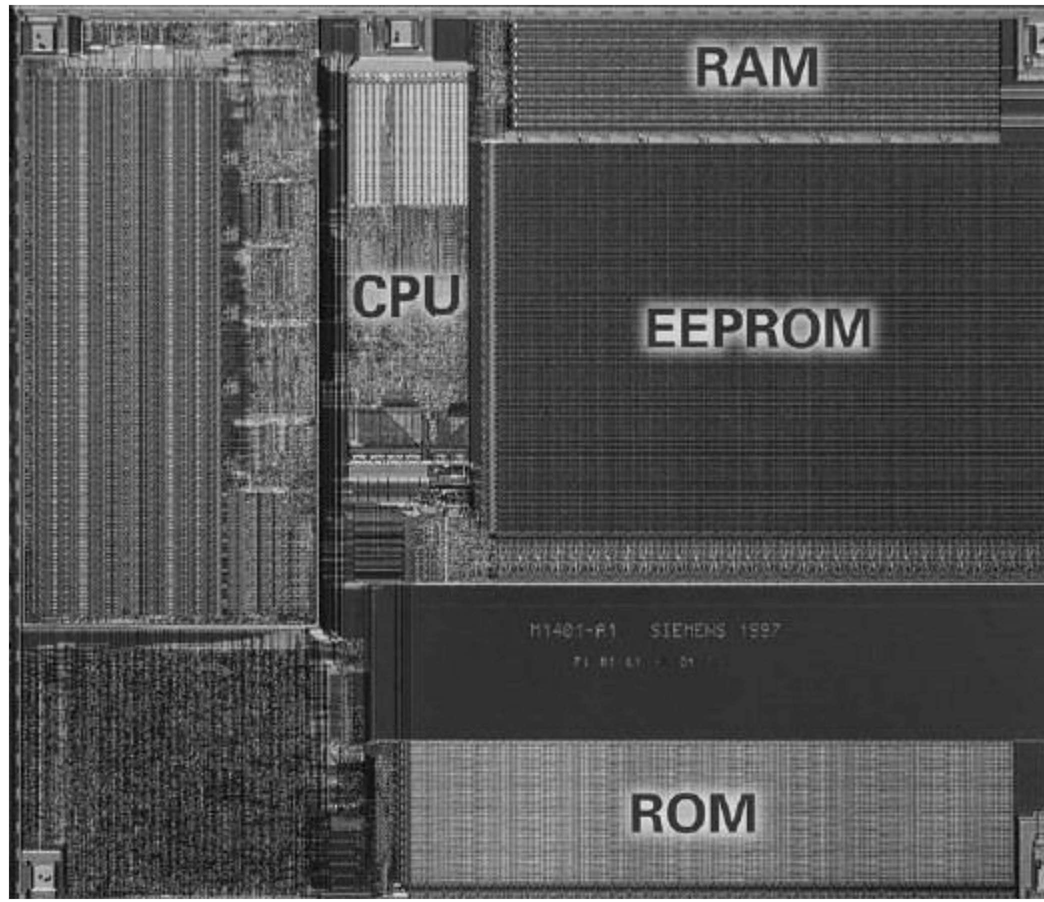
3.57MHz (20MHz)

1.8 / 3/ 5 V

ROM 16-300 kB

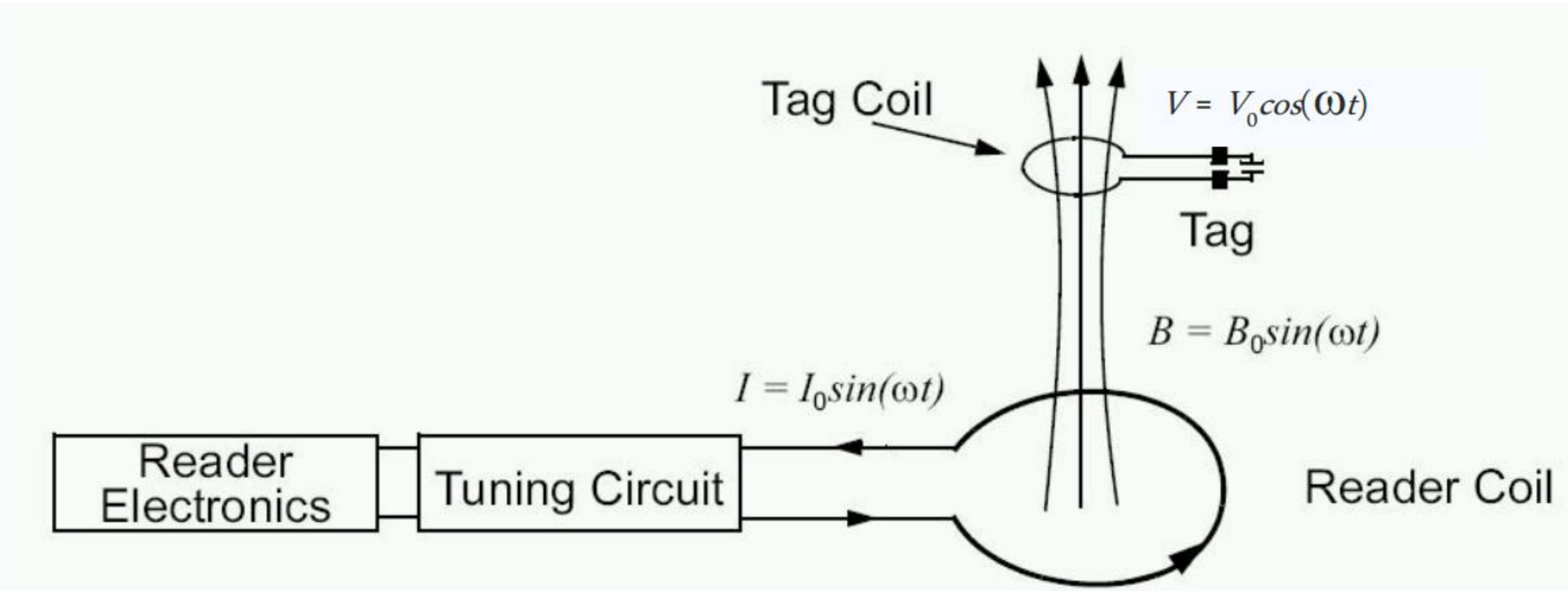
RAM 1-8 kB

EEPROM 8-128kB



gemalto
security to be free

Contactless communication



[Lee: AN710, Microchip 2003]

Not RFID!

f = 13.56 MHz

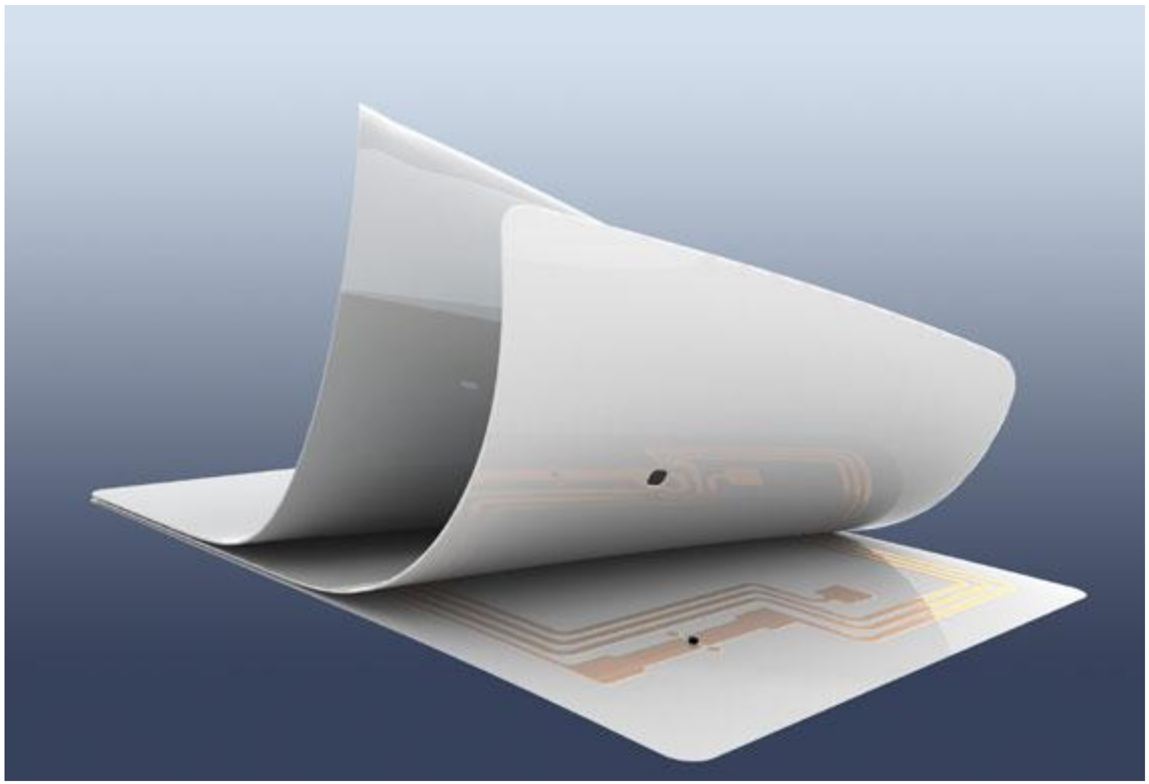
Near-field →range <10cm (300/2πf)

Power via induction

Signal via modulation

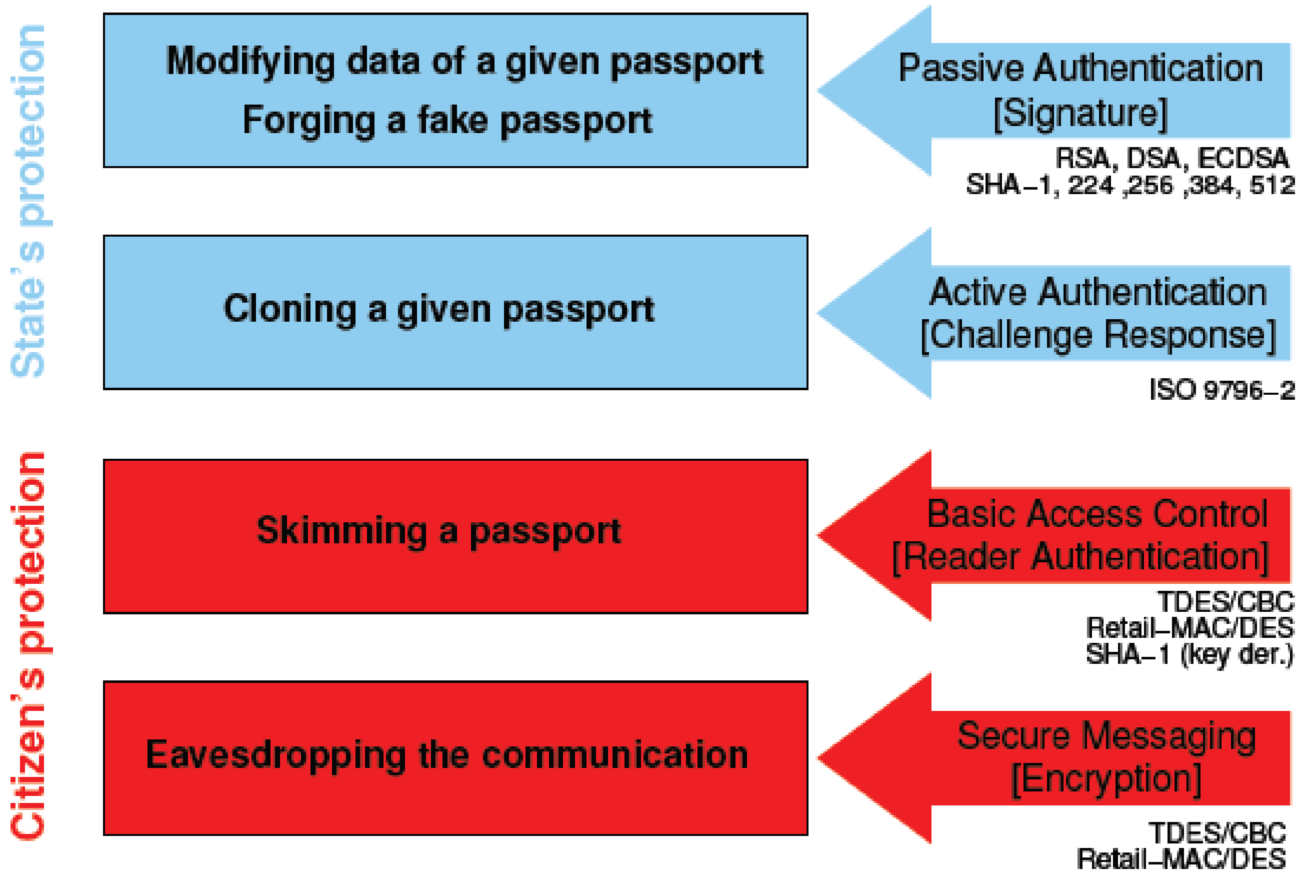
ISO 14443

Contactless communication



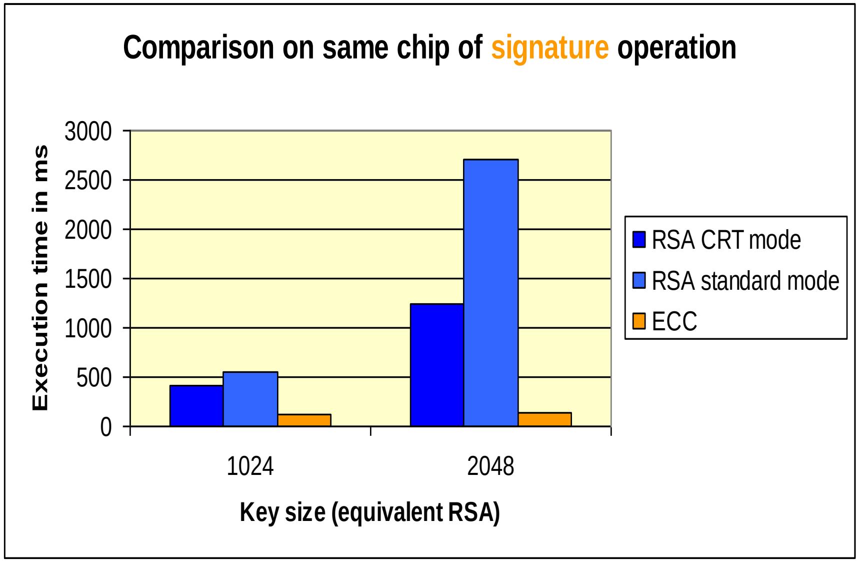
gemalto
security to be free

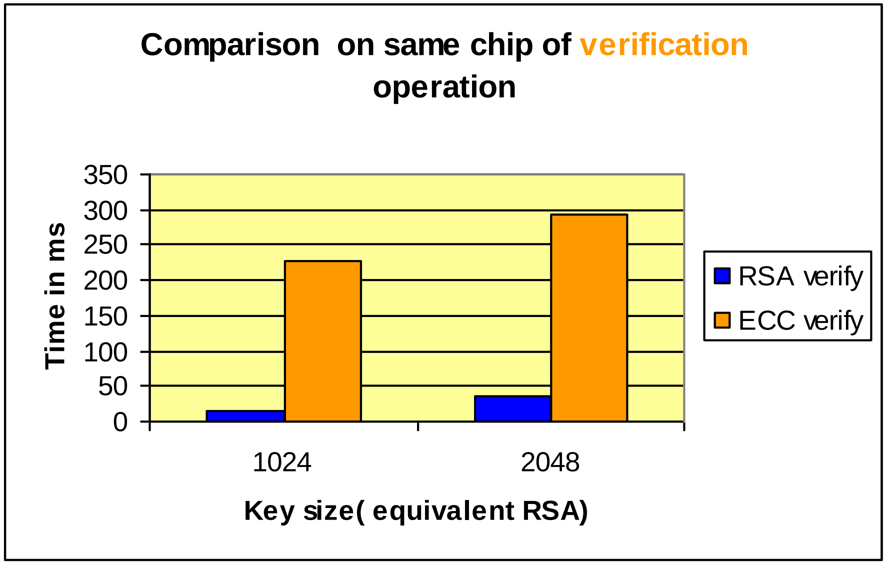
Threats vs. security mechanisms

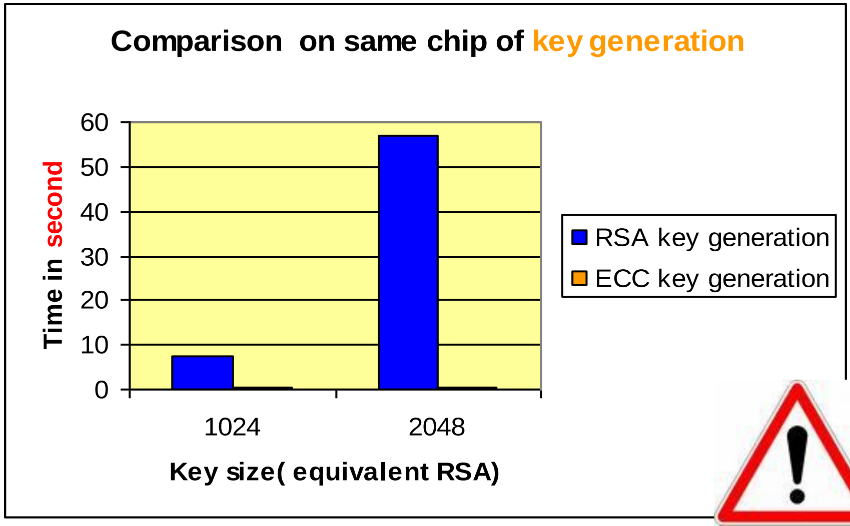


ICAO Security Mechanisms

RSA vs. ECC





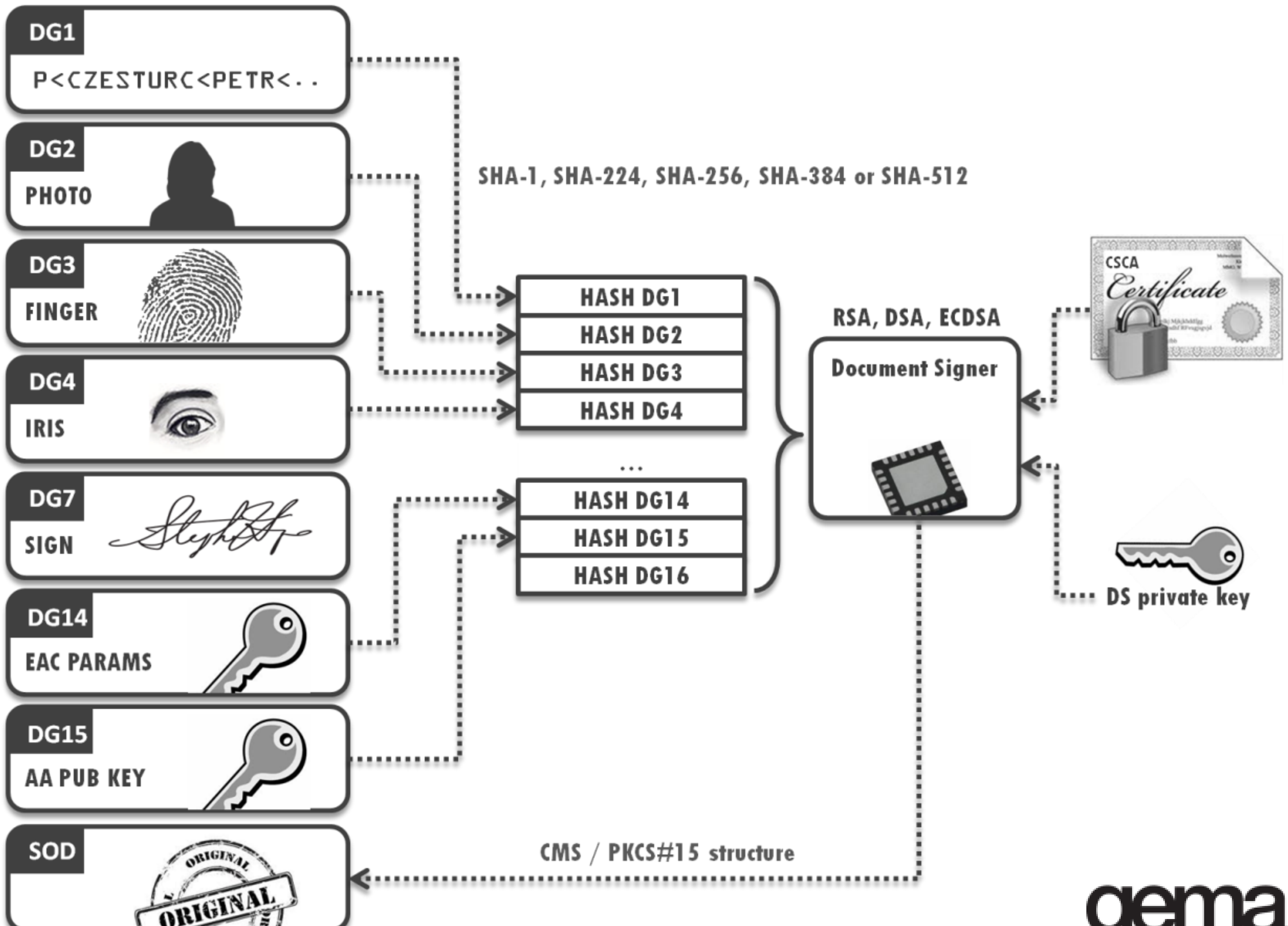


ECC : 113ms and 147 ms

- ECC wins the signature and Key generation match.
- RSA wins the verification match but ECC stays reasonable

- WARNING: Results are chip dependant

Passive Authentication (PA)



gemalto
security to be free

Document Signer

Features:

- Keypair generation, CSR generation (ASN.1 templates, cross-signatures), Certificate storage
- SOD generation (from ASN.1 templates)
- Key selection strategies (explicit selection, round-robin, “optimal”, …)
- Multiple domains
- Connector for Coesys Prod Manager
- Management GUI
- modularity

Supported crypto:

- SW (RSA, RSA-PSS, ECC)
- Luna 3000 HSM (RSA, RSA-PSS, ECC)
- KMS (RSA, RSA-PSS)

UK e-passport "attack"

THE TIMES
THE SUNDAY TIMES

Archive Article Please enjoy this article from The Times & The Sunday Times archives. F…

From The Times

August 6, 2008

'Fakeproof' e-passport is cloned in minutes

Steve Boggan

New microchipped passports designed to be foolproof against identity theft can be cloned and manipulated in minutes and accepted as genuine by the computer software recommended for use at international airports.

Tests for *The Times* exposed security flaws in the microchips introduced to protect against terrorism and organised crime. The flaws also undermine claims that 3,000 blank passports stolen last week were worthless because they could not be forged.

In the tests, a computer researcher cloned the chips on two British passports and implanted digital images of Osama bin Laden and a suicide bomber. The altered chips were then passed as genuine by passport reader software used by the UN agency that sets standards for e-passports.

CSCA Certificates - Ministry of

www.mvcr.cz/mvcren/article/csca-certificates-108056.aspx

MINISTRY OF THE INTERIOR OF THE CZECH REPUBLIC

Modern Administration

EGOVERNMENT

CSCA Certificates

The Czech Country Signing Certificate Authority (CSCA) CSCA Root Certificate issued at 24/07/2006

The Czech Country Signing Certificate Authority (CSCA)
This website contains the information on the Czech CSCA operated by the Ministry of the Interior (MI).

The distinguish name of the CSCA is
C=CZ, O=Czech Republic, OU=Ministry of Interior, CN=CSCA_CZ

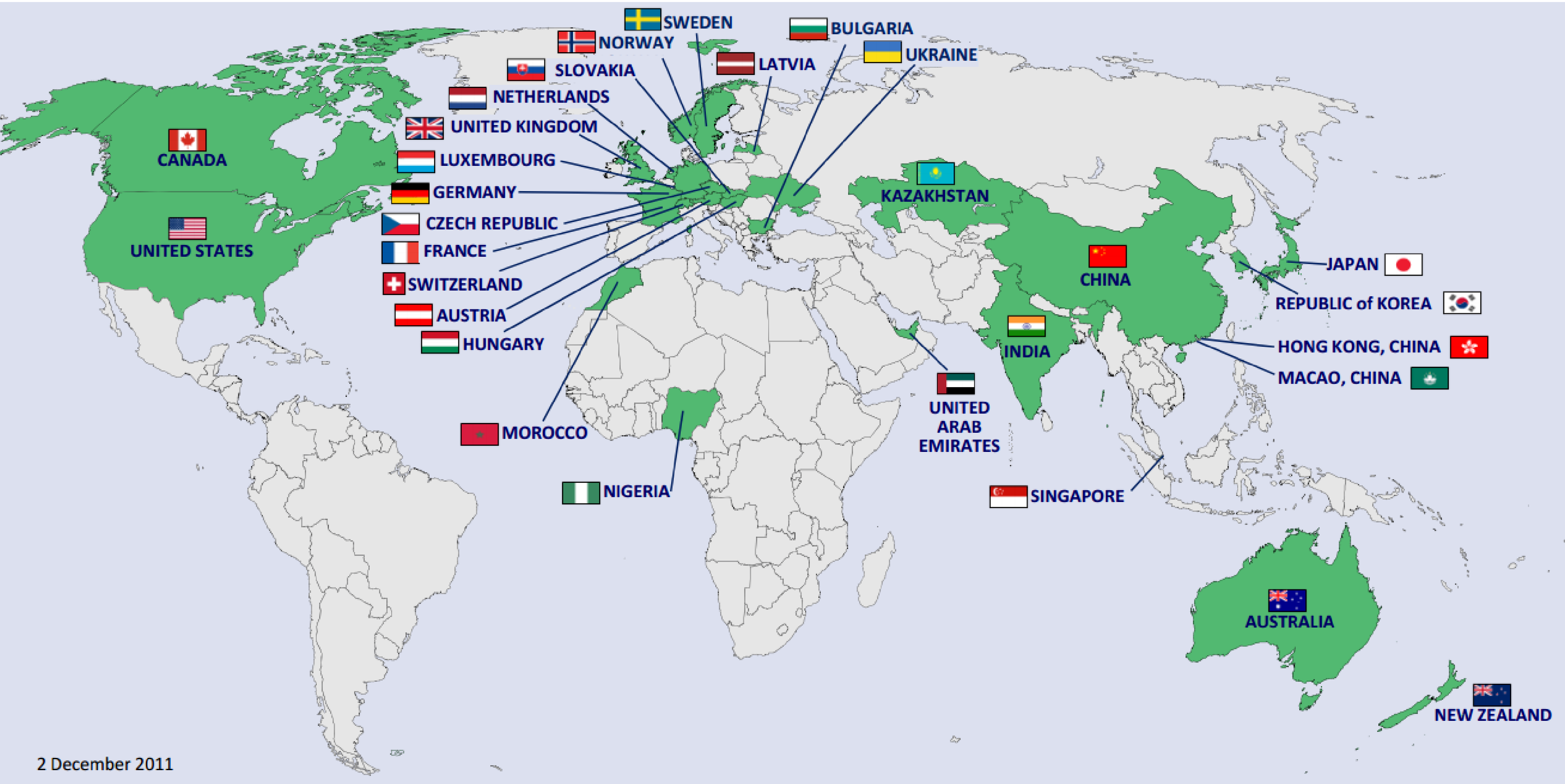
CSCA Public Key Certificate
(Serial Number SN=01)

CZE_CSCA_20060724.der

Police

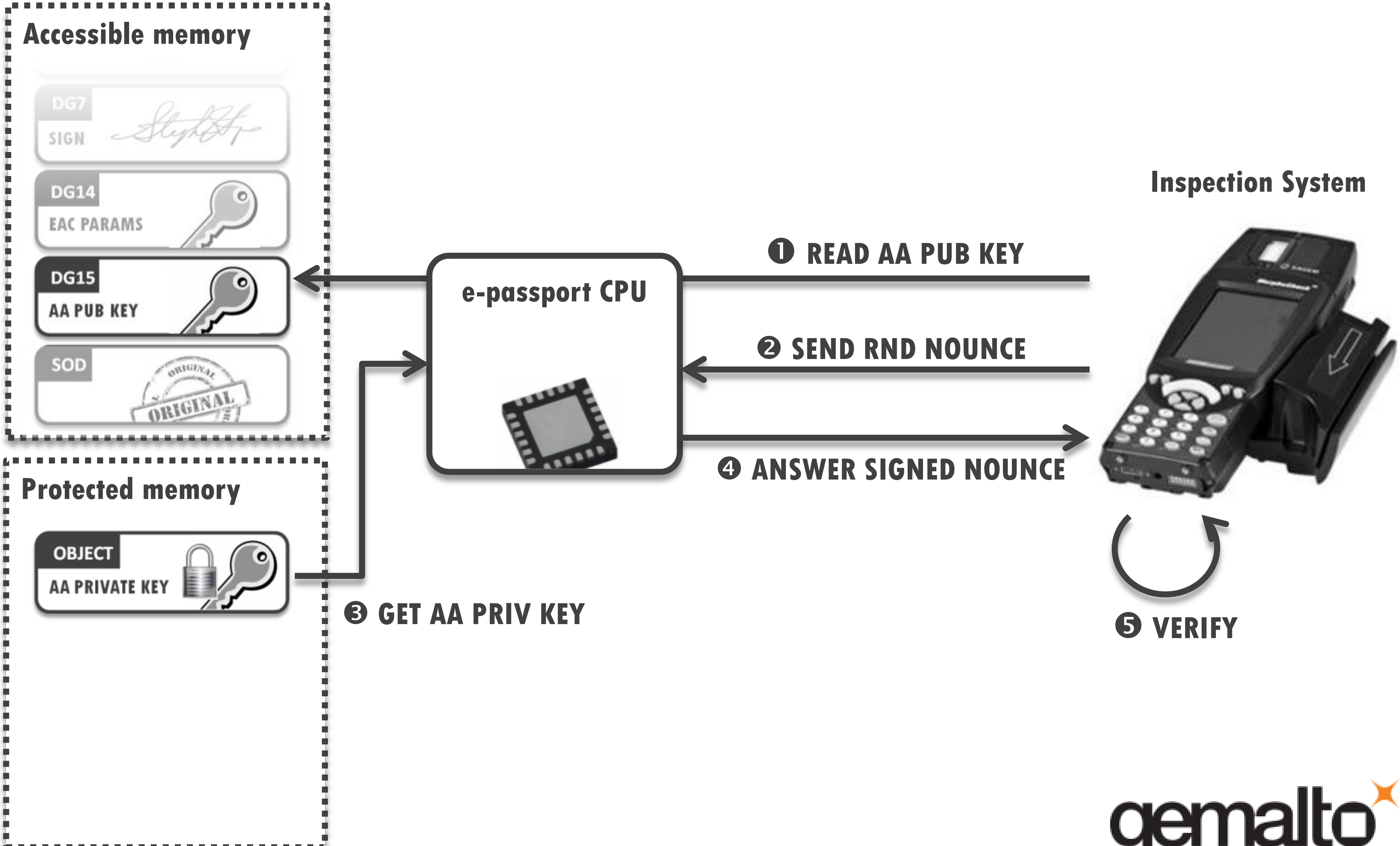
Fire Service

ICAO PKD



gemalto
security to be free

Active Authentication (AA)



gemalto
security to be free

Active Authentication - issues

EF.COM not in SOD

Challenge semantic – Active authentication gives **non-repudiation** (possibility to track the passport holder and have a proof)

- Passport receives "random" string *r* from a terminal and respond with signature *S(Kpr, r)* where *Kpr* is passport's private key. Terminal can hide a meaning into the random *r* (e.g. *r = date||time||location*)
- Can be solved by Chip Authentication (part of EAC)

gemalto
security to be free

Basic Access Control (BAC)

MACHINE READABLE ZONE (MRZ)

Inspection System

PASSPORT NR. | DATE OF BIRTH | DATE OF EXPIRY

↓

SHA-1

↓

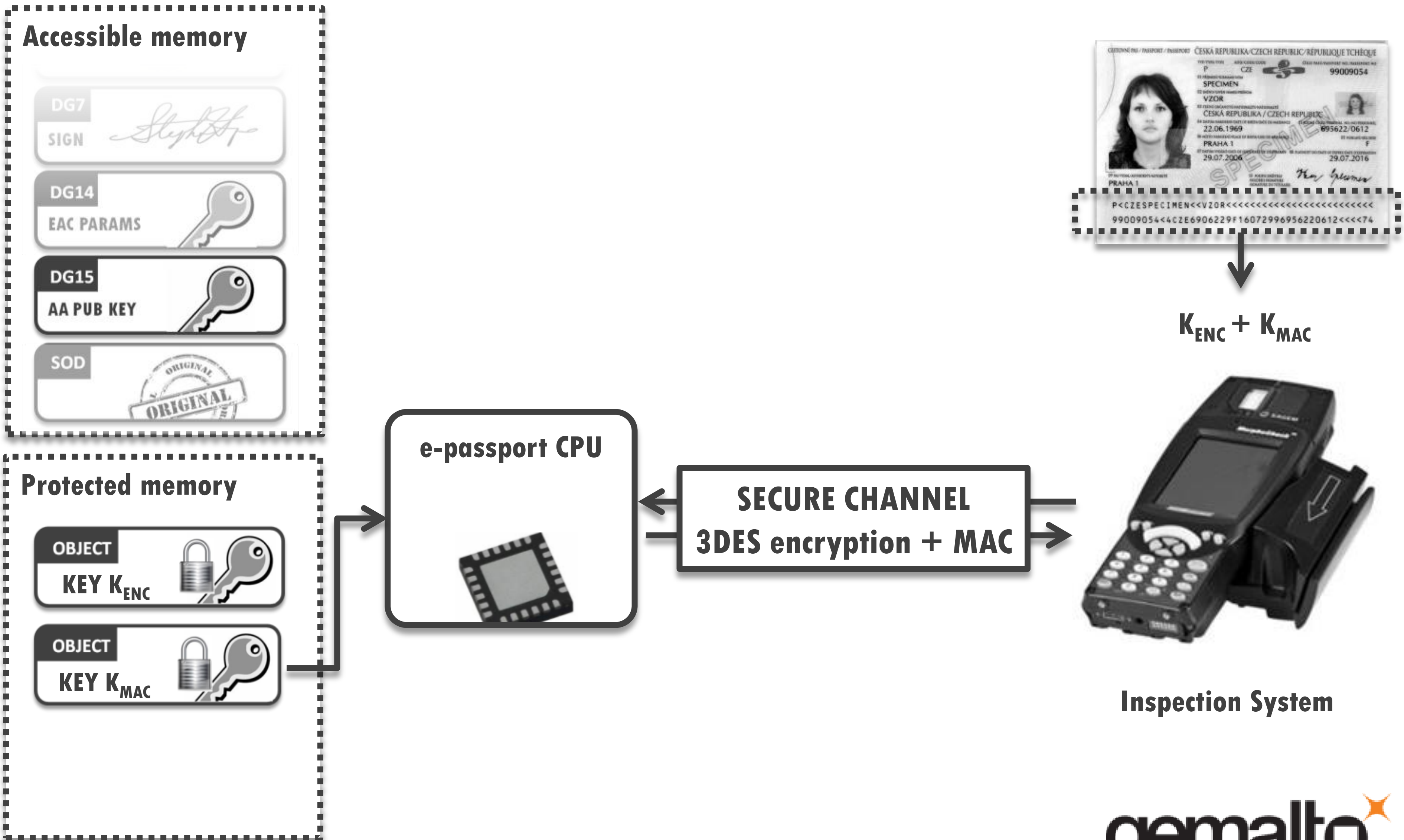
K_{SEED} | 00000001 (for K_{ENC})
00000002 (for K_{MAC})

↓

SHA-1

$K_{ENC/MAC}$ = 3DES KEY (16 BYTES)	NOT USED (4 BYTES)

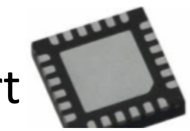
Basic Access Control (BAC)



Basic Access Control - Detailed

Inspection System

E-Passport



GET_CHALLENGE() →

Generate random number for challenge RND.ICC

← RND.ICC

Generate random number RND.IFD and keying material K.IFD

S=RND.IFD||RND.ICC||K.IFD

E_IFD=E[K_{ENC}](S)

M_IFD=MAC[K_{MAC}](E_IFD)

MUTUAL_AUTHENTICATE(E_IFD||M_IFD) →

Check M_IFD

Decrypt E_IFD

Check that RND.ICC from S is the correct value

Generate keying material K.ICC

R=RND.ICC||RND.IFD||K.ICC

E_ICC=E[K_{ENC}](R)

M_ICC=MAC[K_{MAC}](E_ICC)

← E_ICC||M_ICC

Check M_ICC

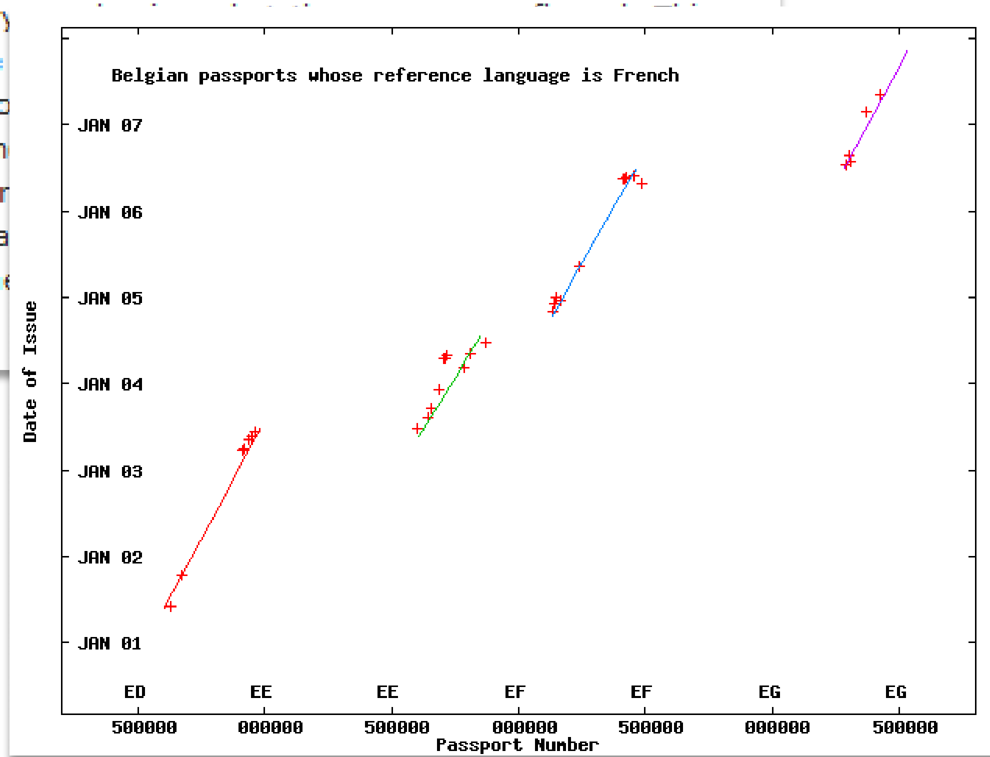
Decrypt E_ICC

Check that RND.IFD from R is the correct value

Belgian passport "attack"

Belgian Biometrics passport proven insecure

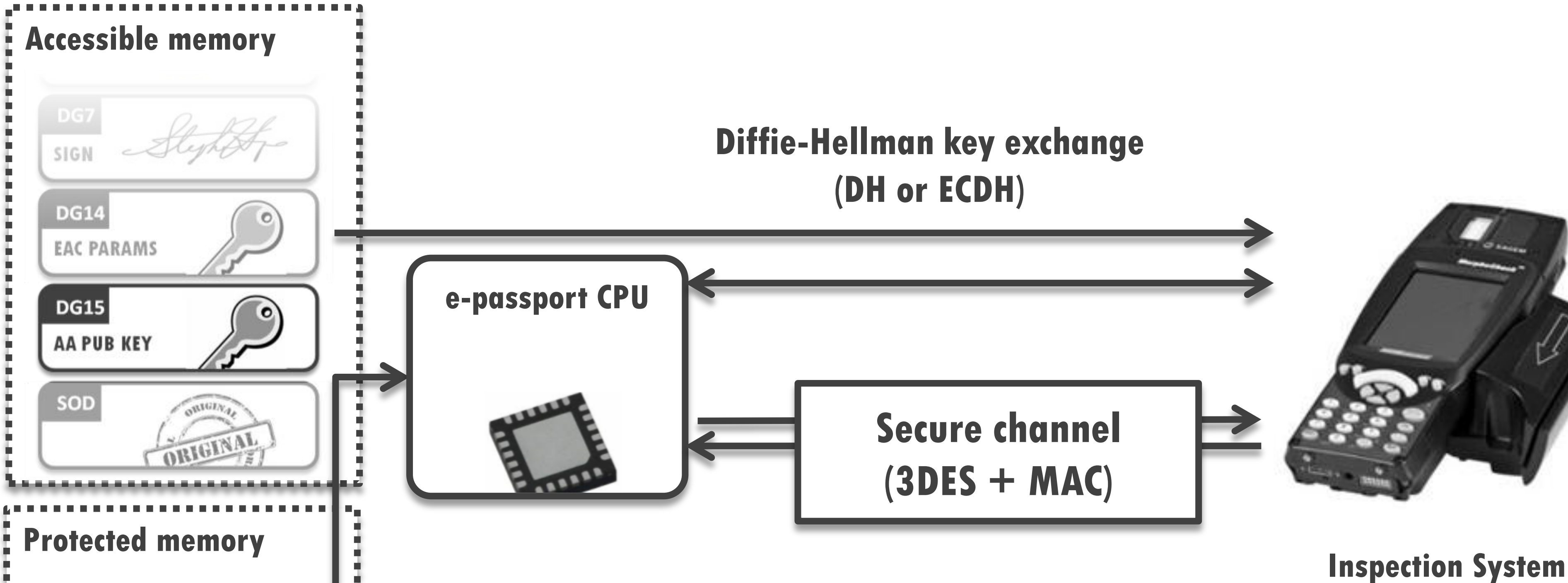
A research team in cryptography from the Catholic University of Louvain (Louvain-la-Neuve) disclosed serious weaknesses in the Belgian biometric passport, the only type of passport distributed in Belgium since the end of 2004. The work carried out in Louvain-la-Neuve during the course of May 2007 show that **Belgian passports issued between end 2004 and July 2006 do not include any security mechanism to protect the personal data** embedded in the passport's microchip. Passports issued after July 2006 do benefit from security
means that anyone possessing a little
cheap to acquire, can steal the passpo
victim owners and thus without their kn
at risk. This news is all the more surpr
Foreign Affairs, declared in the Parlia
passport benefited from the security me
Aviation Organization.

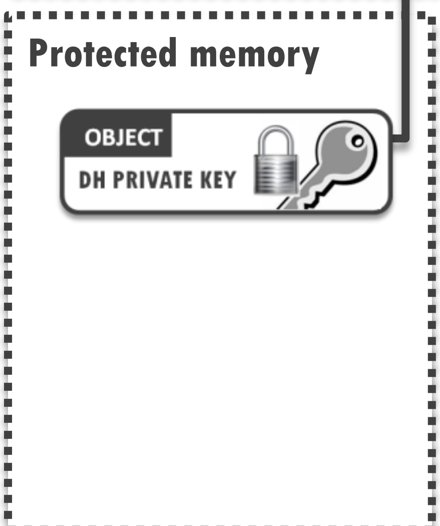


European Commission

Extended Access Control (EAC)

Chip Authentication (CA)



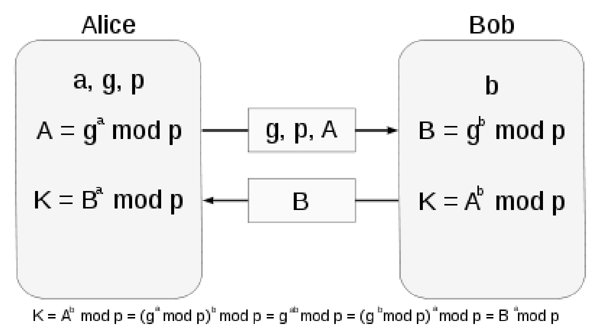


Ephemeral–Static (EC)-Diffie-Hellman

- Chip:
  - Chip individual static key pair
  - Public Key stored in the DG14(signed)
  - Private Key stored in secure memory
- Terminal:
  - Ephemeral key pair dynamically chosen by the terminal

ECDH (224Bit) asymmetric key agreement

3DES (112Bit) symmetric encryption / integrity protection

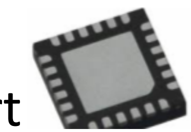


gemalto
security to be free

Chip Authentication - Detailed

Inspection System

E-Passport



READ_BINARY() →

Read Chip Authentication public key of the ICC (PK_{ICC}) and domain parameters D_{ICC} from the EF.DG14

← PK_{ICC}, D_{ICC}

Generate ephemeral key pair PK_{IFD}, SK_{IFD}

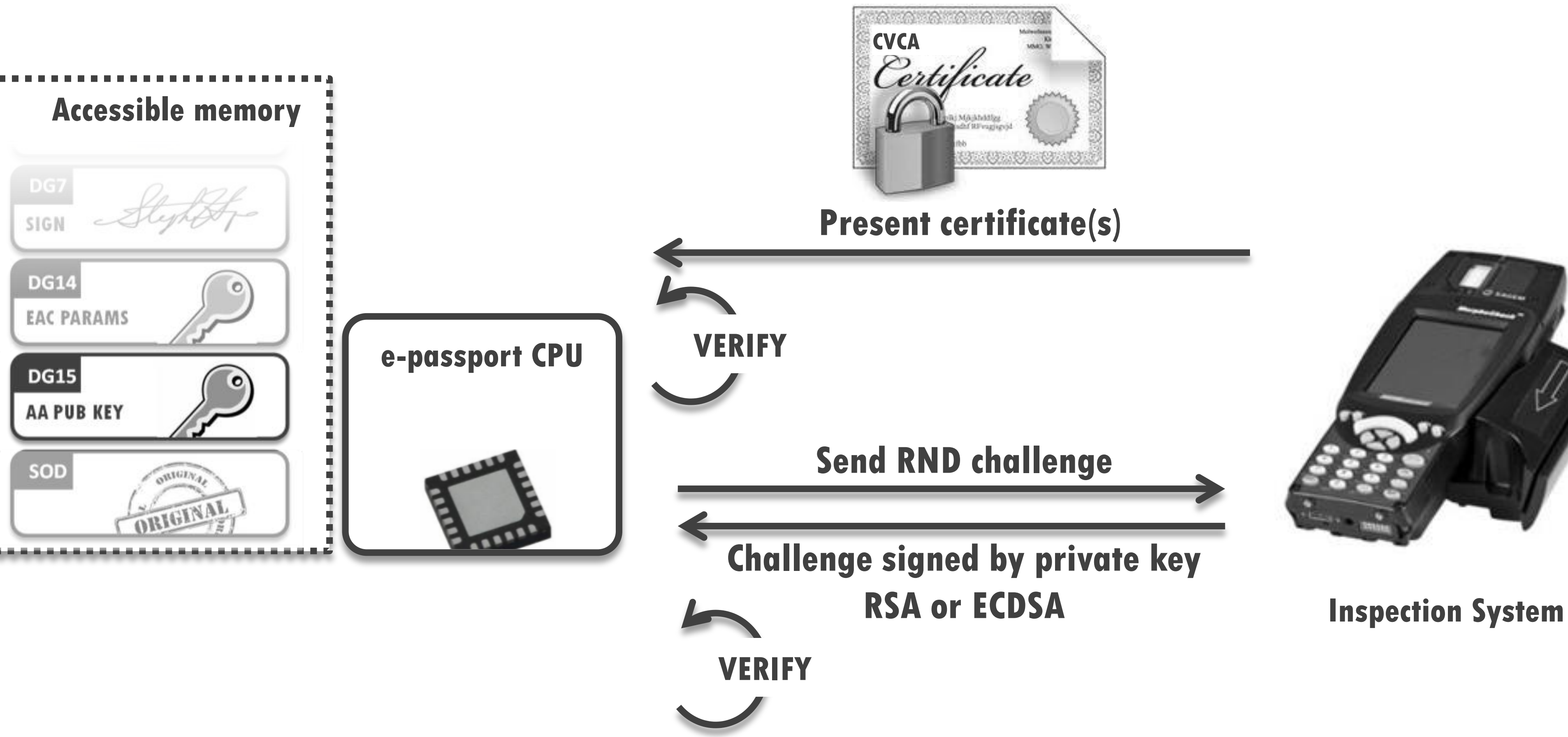
MSE_SET_KAT(PK_{IFD}) →

$K=KA(SK_{IFD}, PK_{ICC}, D_{ICC})$

$K=KA(SK_{ICC}, PK_{IFD}, D_{ICC})$

gemalto security to be free

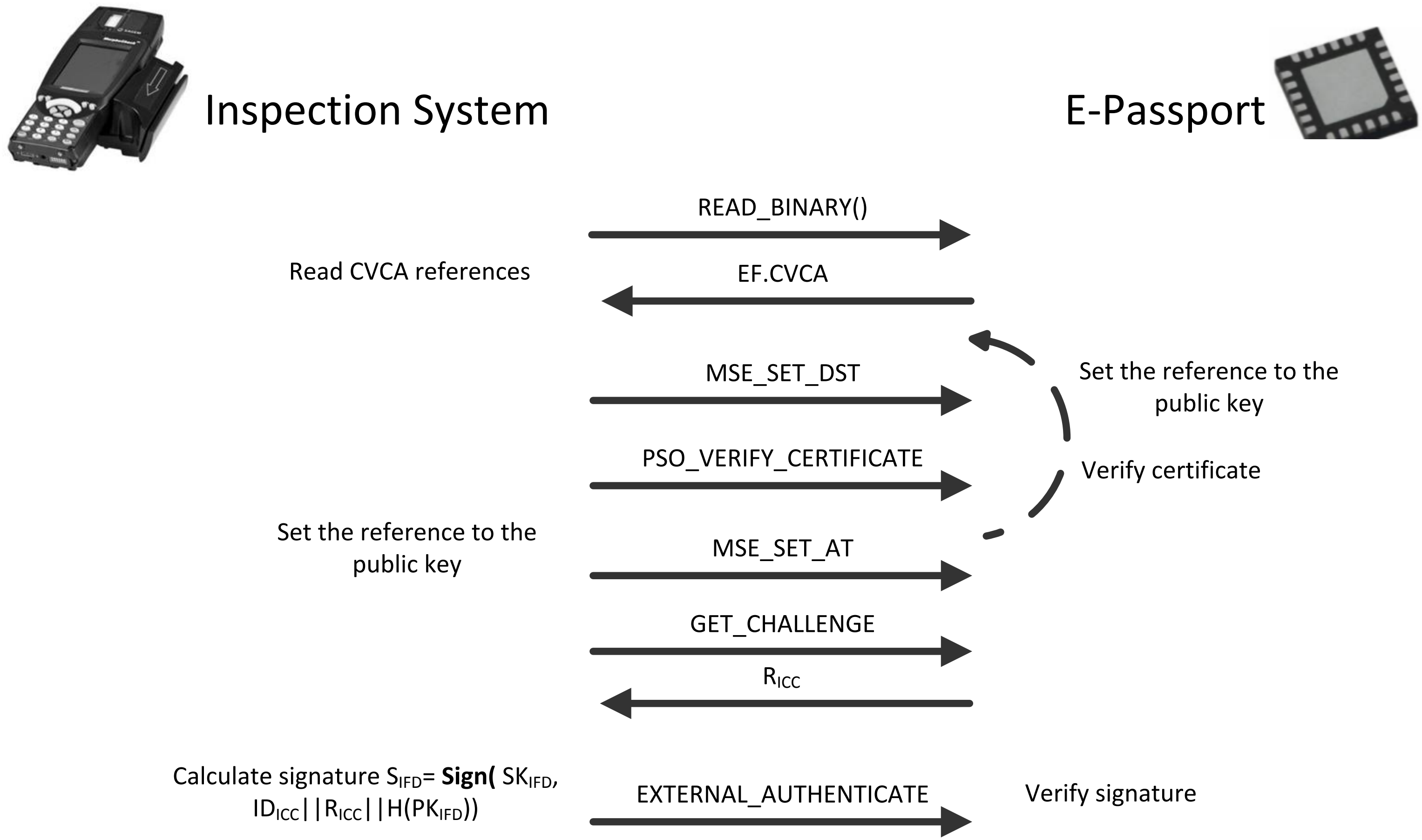
Terminal Authentication (TA)



Problem!

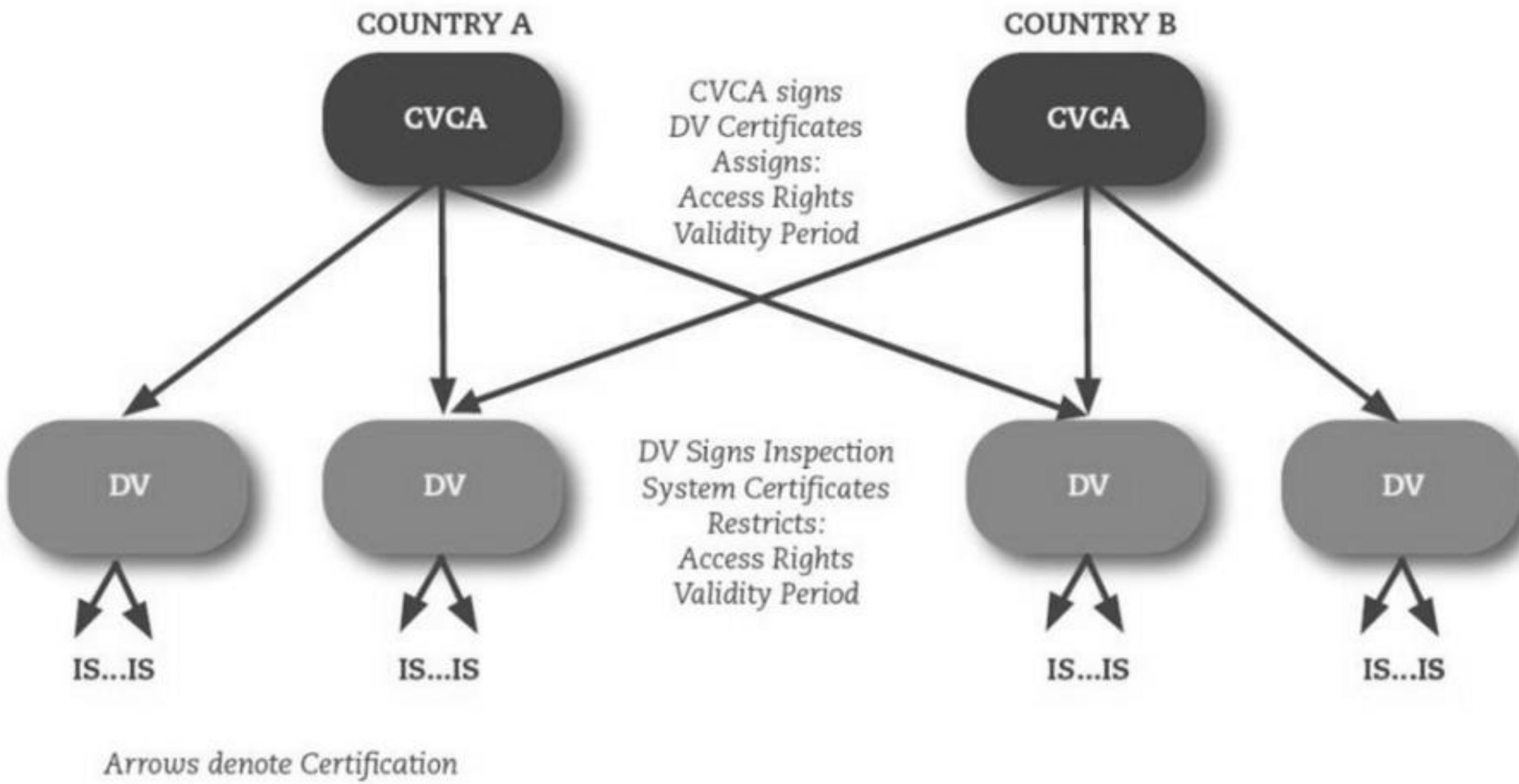
Verify cert = signature + expiration + revocation

Terminal Authentication – Detailed

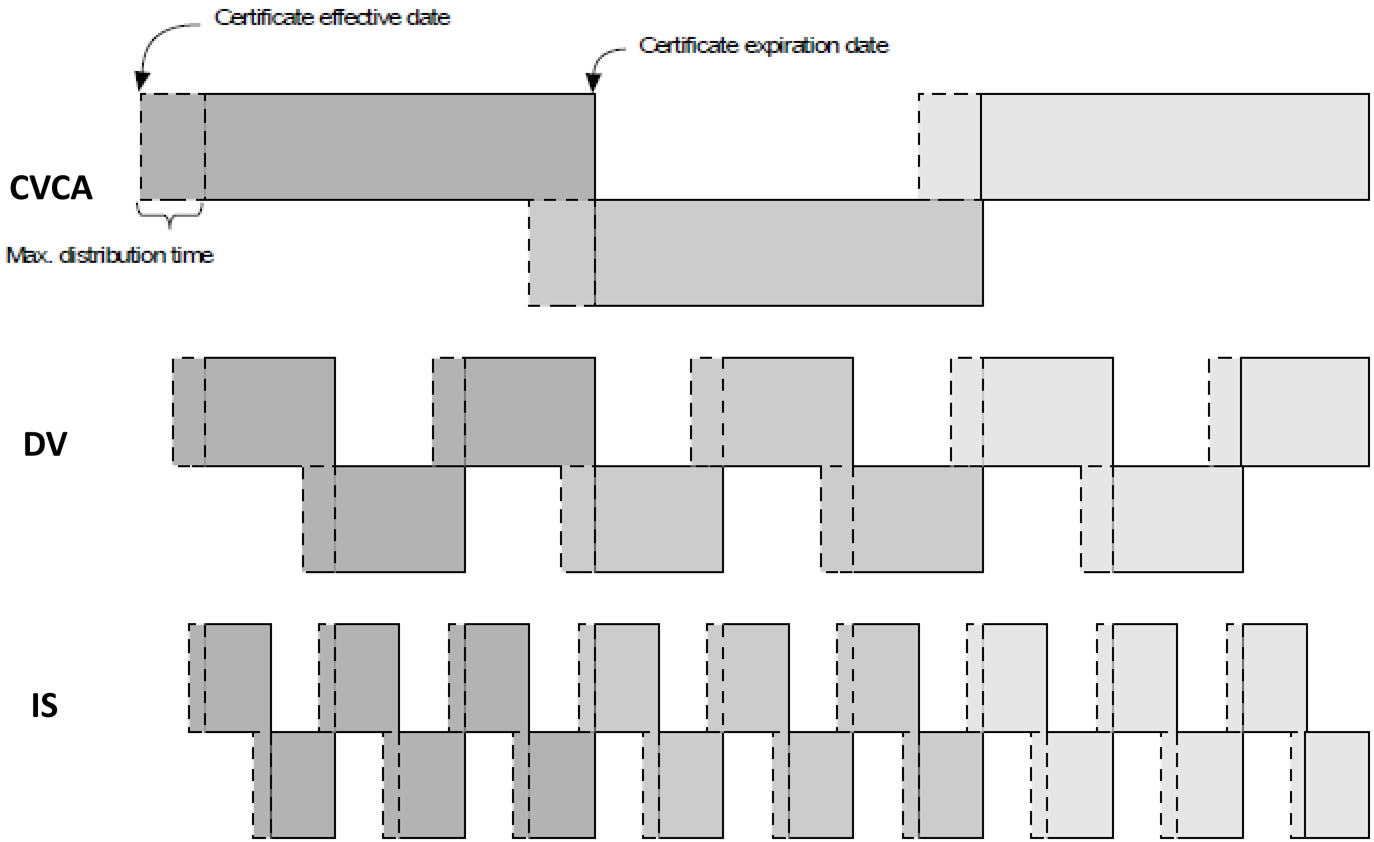


gemalto
security to be free

EAC Cross-certification



Certificate renewal



Examples of validity periods:

- CVCA certificate : 2 years
- DV Certificate : 3 months
- IS Certificate : 1 month

European Commission

Extended Access Control v2
a.k.a "3rd generation e-passport"

PACE v2

Password Authenticated Connection Establishment

MRTD Chip (PICC)		Terminal (PCD)
static domain parameters D_{PICC}		
choose random nonce $s \in_R Dom(E)$		
$z = \mathbf{E}(K_\pi, s)$	$\xrightarrow[z]{D_{PICC}}$	$s = \mathbf{D}(K_\pi, z)$
additional data required for $\mathbf{Map}()$	$\longleftrightarrow$	additional data required for $\mathbf{Map}()$
$\tilde{D} = \mathbf{Map}(D_{PICC}, s)$		$\tilde{D} = \mathbf{Map}(D_{PICC}, s)$
choose random ephemeral key pair $(\widetilde{SK_{PICC}}, \widetilde{PK_{PICC}}, \tilde{D})$		choose random ephemeral key pair $(\widetilde{SK_{PCD}}, \widetilde{PK_{PCD}}, \tilde{D})$
	$\xleftarrow{\widetilde{PK_{PCD}}}$ $\xrightarrow{\widetilde{PK_{PICC}}}$	
$K = \mathbf{KA}(\widetilde{SK_{PICC}}, \widetilde{PK_{PCD}}, \tilde{D})$		$K = \mathbf{KA}(\widetilde{SK_{PCD}}, \widetilde{PK_{PICC}}, \tilde{D})$
	$\xleftarrow{T_{PCD}}$	$T_{PCD} = \mathbf{MAC}(K_{MAC}, (\widetilde{PK_{PICC}}, \tilde{D}))$
$T_{PICC} = \mathbf{MAC}(K_{MAC}, (\widetilde{PK_{PCD}}, \tilde{D}))$	$\xrightarrow{T_{PICC}}$	

gemalto
security to be free


That's all Folks!