STELAU

Cabinet de conseil et d'audit
Sécurité des systèmes d'information

Sécurités du passeport électronique

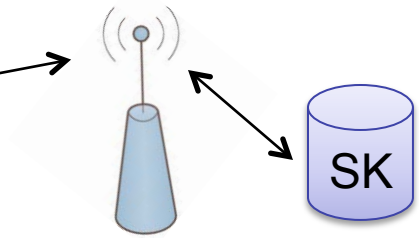
Nicolas CHALANSET
CISSP – ISO 27001-LD - GWAPT

Ce qui marche encore pas mal …

... attention, les finalités sont différentes

1 : la téléphonie mobile

SK



full on-line

2 : la carte bancaire

SK

DDA

on-line & off-line

3 : le passeport biométrique

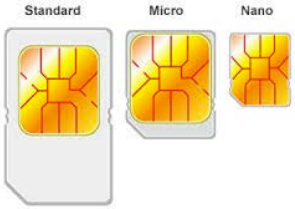
BAC EAC
PA & AA

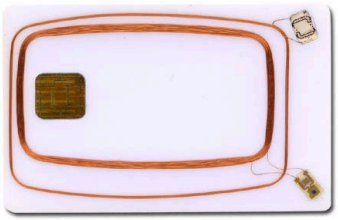
full off-line

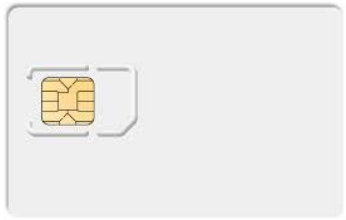
le dernier sanctuaire des petits secrets et autres clés privées ?

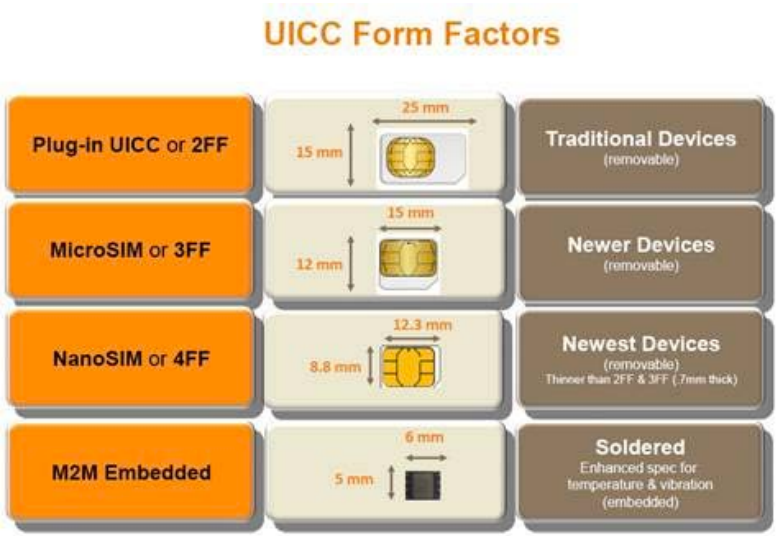
MultiApp ID IAS ECC Combi complies with the following international and European standards:
Java Card 2.2.1
Global Platform 2.1.1
ISO 7816 parts 1, 2, 3, 4, 5, 6, 8 & 9
ISO14443 type-A and type B
CEN TS 15480 part 1 and 2
E-SingK EN 14890 part 1 and 2
ICAO EAC V1.11
ICAO Doc 9303 Sixth Edition
ICAO Machine Readable Travel Document ? RF Protocol and Application Test Standard for e-Passport.
Pre-loaded applets in ROM
IAS ECC applet
ICAO applet
One time password applet
Mifare emulation upon request.
Security
MultiApp ID IAS ECC Combi includes multiple hardware and software countermeasure against various public & non-public attacks as:
Side channel attacks (SPA, DPA, Timing attacks etc)
Invasive attacks
Advanced fault attacks.

carte à puce = smart card = ISO 7816-4 [APDU]

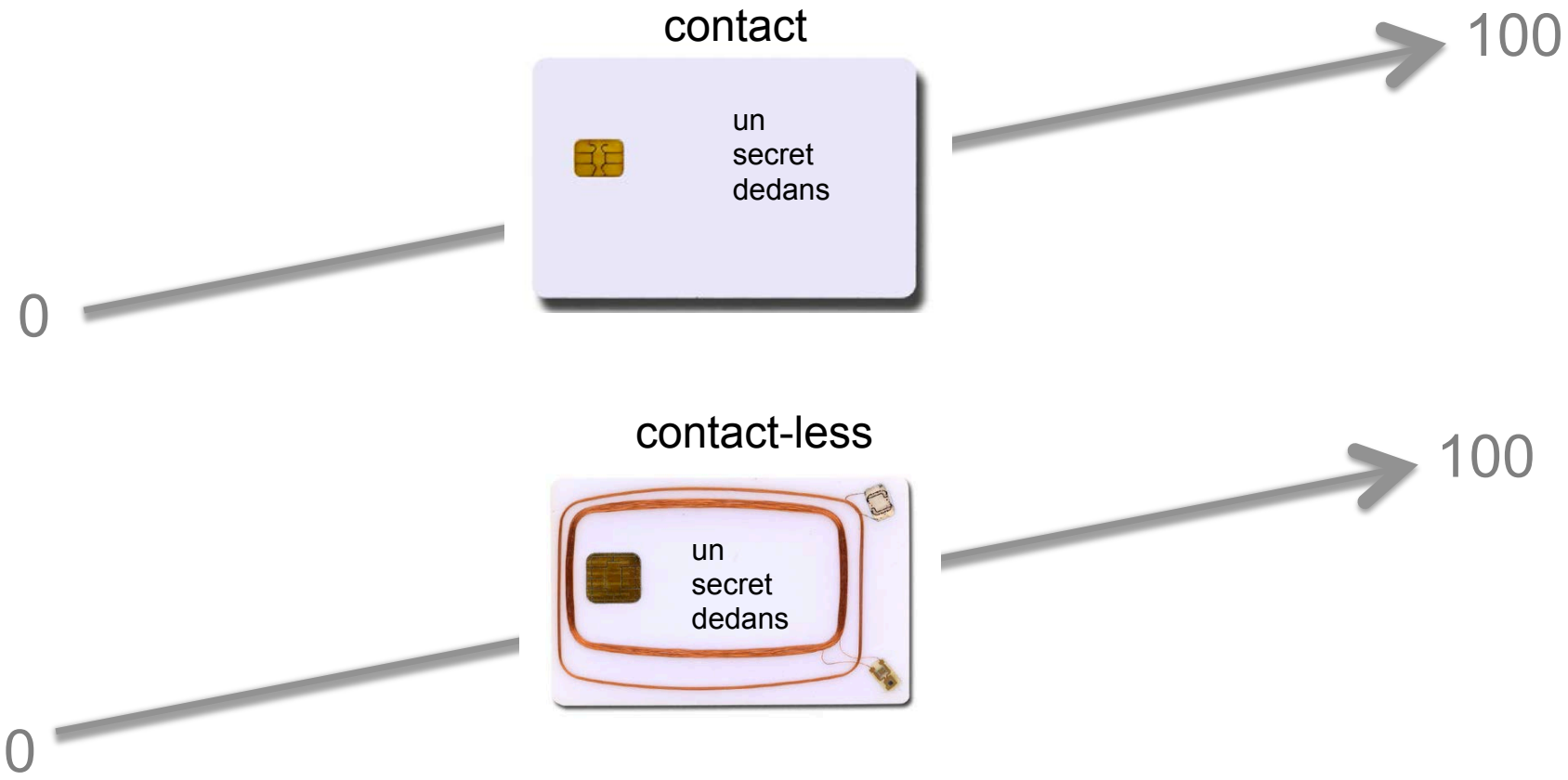


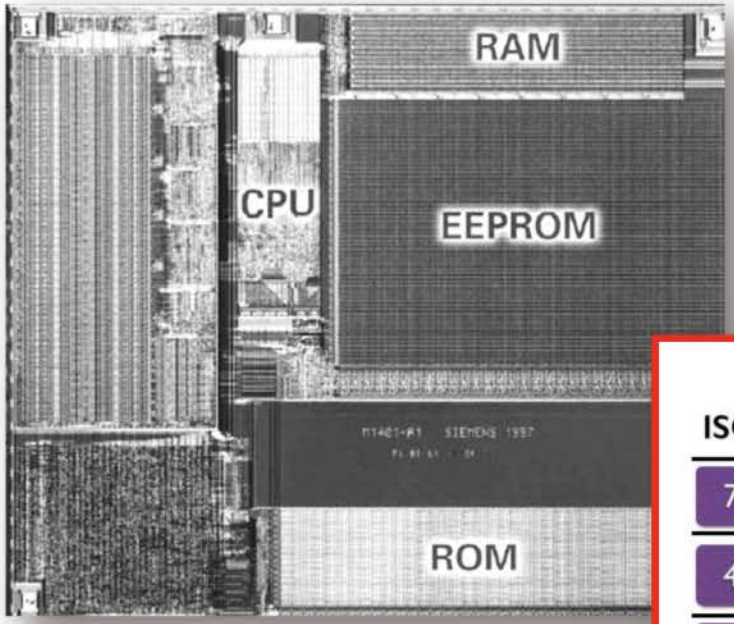


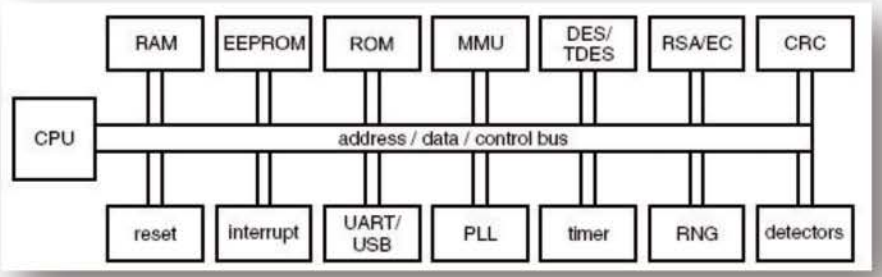


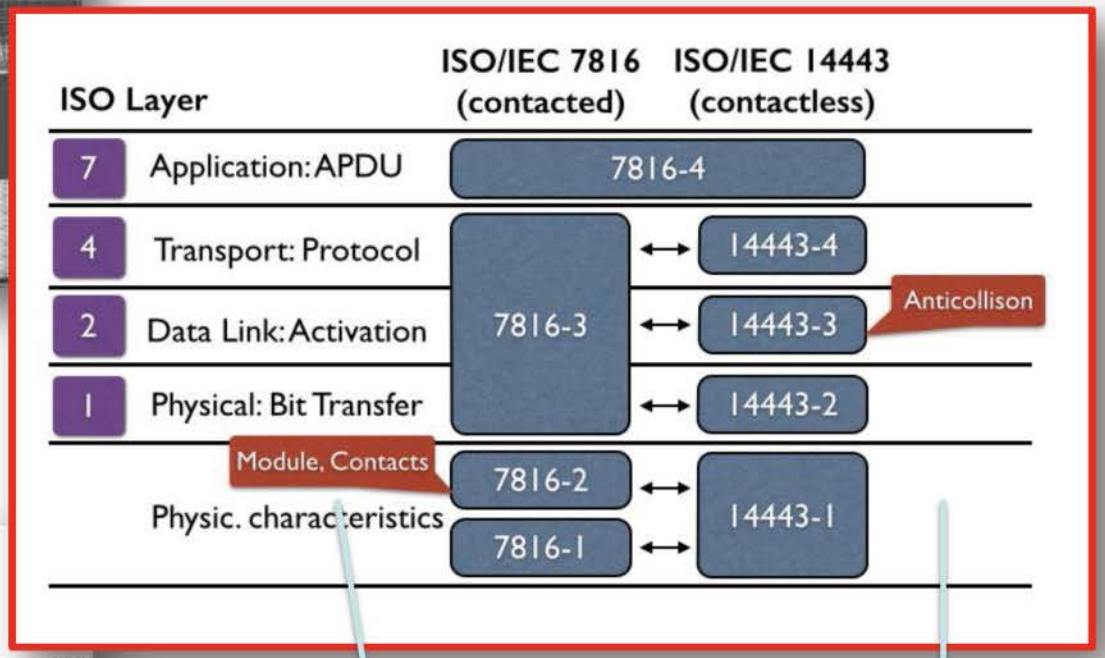


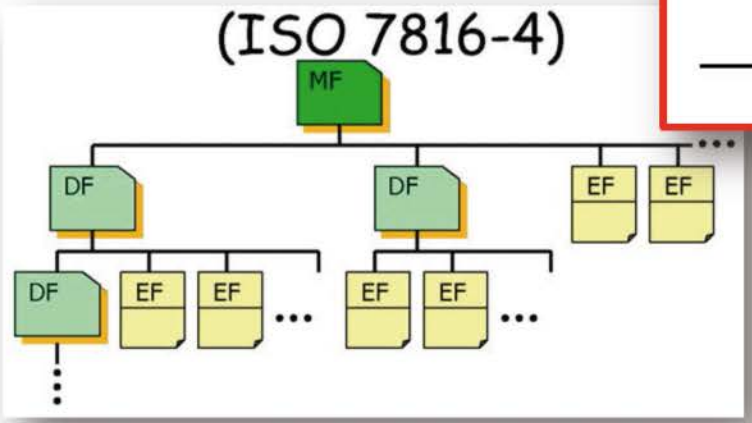
Attention


contact
un
secret
dedans
0
100
contact-less
un
secret
dedans
0
100

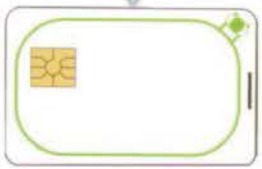

RAM
CPU
EEPROM
ROM


RAM
EEPROM
ROM
MMU
DES/ TDES
RSA/EC
CRC
CPU
address / data / control bus
reset
interrupt
UART/ USB
PLL
timer
RNG
detectors


ISO Layer
ISO/IEC 7816 (contacted)
ISO/IEC 14443 (contactless)
7 Application: APDU
7816-4
4 Transport: Protocol
14443-4
2 Data Link: Activation
7816-3
14443-3
Anticollison
1 Physical: Bit Transfer
14443-2
Module, Contacts
7816-2
Physic. characteristics
7816-1
14443-1


(ISO 7816-4)
MF
DF
DF
EF
EF
DF
EF
EF
EF
EF


C1–VCC
C2–RST
C3–CLK
C4–
C5–GND
C6–VPP
C7–I/O
C8–



STELAU

Pourtant …

tjs pas de CNIe  tout sur FB

le GIXEL … c'est fini

IAS-ECC … c'est fini

nb IGC RGS dans l'admin. = 3

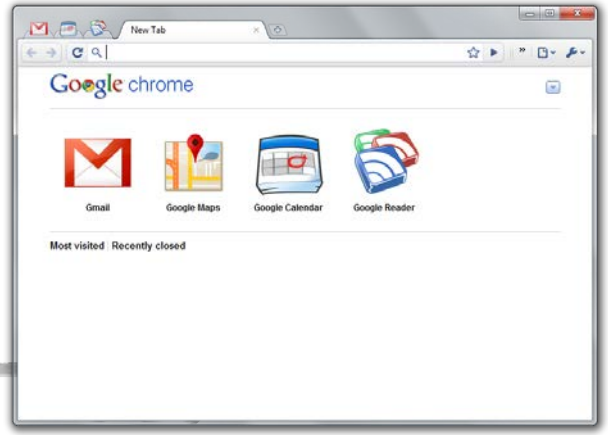
normes poussées par l'ANSSI = 0

normes poussées par la/le BSI = 3

PACE EAC IDEAS

1974 : Roland Moreno

1977 : Michel Hugon



Electronique / Biométrique

- Le passeport électronique
  - il contient une puce RFID
  - il respecte la norme de contrôle d'accès BAC
  - la photographie n'est pas une donnée biométrique à accès restreint

- Le passeport électronique 2ème génération dit biométrique
  - c'est le passeport délivré de juin 2009 au 23 décembre 2014
  - il contient toujours une puce RFID
  - il respecte toujours la norme de contrôle d'accès BAC
  - la photographie n'est toujours pas une donnée biométrique à accès restreint
  - Il respecte les normes de contrôle d'accès EAC
  - l'empreinte digitale est une donnée biométrique à accès restreint

Electronique / Biométrique

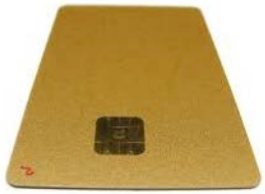
- Le passeport électronique 3ème génération
  - c'est le passeport délivré depuis le 24 décembre 2014
  - ajout du protocole de contrôle d'accès SAC

Normes et documents

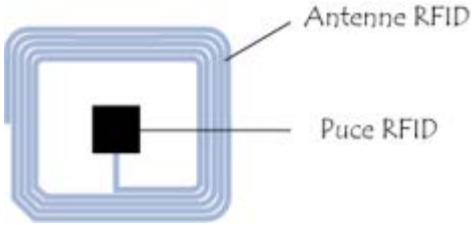
Normes	Mécanismes de sécurité	Objectifs de sécurité	Fonctions Cryptographiques	Obligatoire / Facultatif	France
OACI 9303	BAC	contrôle d'accès confidentialité des échanges	authentification (symétrique) échange de clés de session	facultatif	X
	Passive Auth.	intégrité et authenticité	signature électronique	obligatoire	X
	Active Auth.	originalité du composant	défi-réponse (asymétrique)	facultatif	
ICAO TR SAC v 1.01	PACE (SAC)	contrôle d'accès confidentialité des échanges	secret partagé + échange de clé Diffie-Hellman	obligatoire	X (depuis décembre 2014)
EAC TR03110 V 1.11	Chip Auth. v1	originalité du composant confidentialité des échanges	échange de clé Diffie-Hellman	obligatoire	X (depuis juin 2009)
	Term Auth. v1	contrôle d'accès (authentification du lecteur)	vérification de certificats (signature électronique) défi-réponse (asymétrique)	obligatoire	X (depuis juin 2009)

Puce RFID

- Mêmes fonctionnalités que les puces avec contact
  - alimentation externe
  - microprocesseur de 1 à 29Mhz
    + calculs cryptographiques
  - mémoire physique < 80Ko

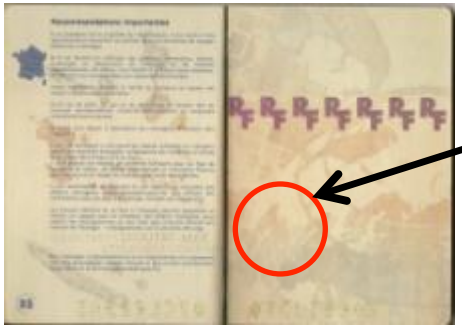


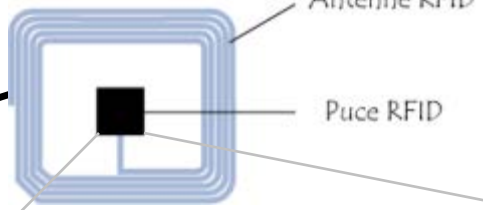
- Transmission par ondes radios
  (Radio Frequency IDentification)
  - 13,56Mhz



Contenu du passeport

- Le passeport biométrique :
  - puce RFID (ISO-IEC 14443)
  - état civil + photo + empreintes digitales + SO_D
  - contrôle d'accès BAC et EAC





bande MRZ

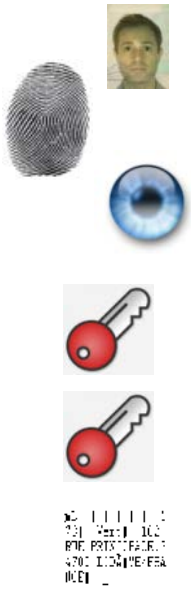
Etat civil DG1	Photo DG2	Empreintes DG3	Iris DG4	EF.SOD

a[_.XP<FRASPECIM
EN<<NATACHA<<<<<
<<<<<<<<<<<<<<<<
<07CL729051FRA73
07122F1707085<<<
<<<<<<<<<<<00
lL\._._&_.<DIREC
TION DES LIBERTÃ
▌S PUBLIQUES ET
DES AFFAIRES JUR
IDIQUES_&. ..._
D\.▌.▌.▌.▌.▌..1
78▌..Vert▌.'102<
RUE PRINCIPALE<3
4700<LODÃ▌VE<FRA
NCE▌..

Contenu du passeport : les «Data Group»

DG	Contenu	Contrôle d'accès	Obligatoire / Facultatif
EF.CARDACCESS			Obligatoire
EF.COM	« Sommaire des données »	BAC ou SAC	Obligatoire
DG1	Données imprimées	BAC ou SAC	Obligatoire
DG2	Biométrie : Visage	BAC ou SAC	Obligatoire
DG3	Biométrie: Empreintes	BAC + EAC	Obligatoire
DG4	Biométrie: Iris	BAC + EAC	Facultatif
…		BAC ou SAC	Facultatif
DG14	Clé publique Chip Auth	BAC ou SAC	Facultatif
DG15	Clé publique Active Auth	BAC ou SAC	Facultatif
DG16	…	BAC ou SAC	Facultatif
SOD	Security Object Data	BAC ou SAC	Obligatoire

Bob X



MRTD & IS

MRTD
Machine Readable Travel Document

PASSEPORT

IS
Inspection System

LECTEUR
système de contrôle

Hashage

- fonction à sens unique
  - d'un espace infini vers un espace fini
- 1 clair → 1 hash unique (pas de collision)

SHA-1, SHA-2, RIPEMD, MD2, MD5

Chiffrement

- chiffrement symétrique
  - 1 clé secrète partagée
  - DES, TDES, AES

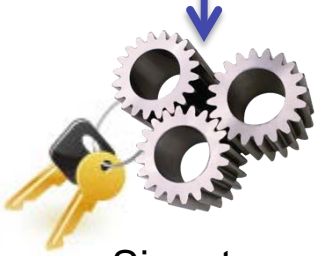
- chiffrement asymétrique
  - 1 clé privée (déchiffrement)
  - 1 clé publique (chiffrement)
  - RSA, courbes elliptiques

Signature électronique

Données

Hachage

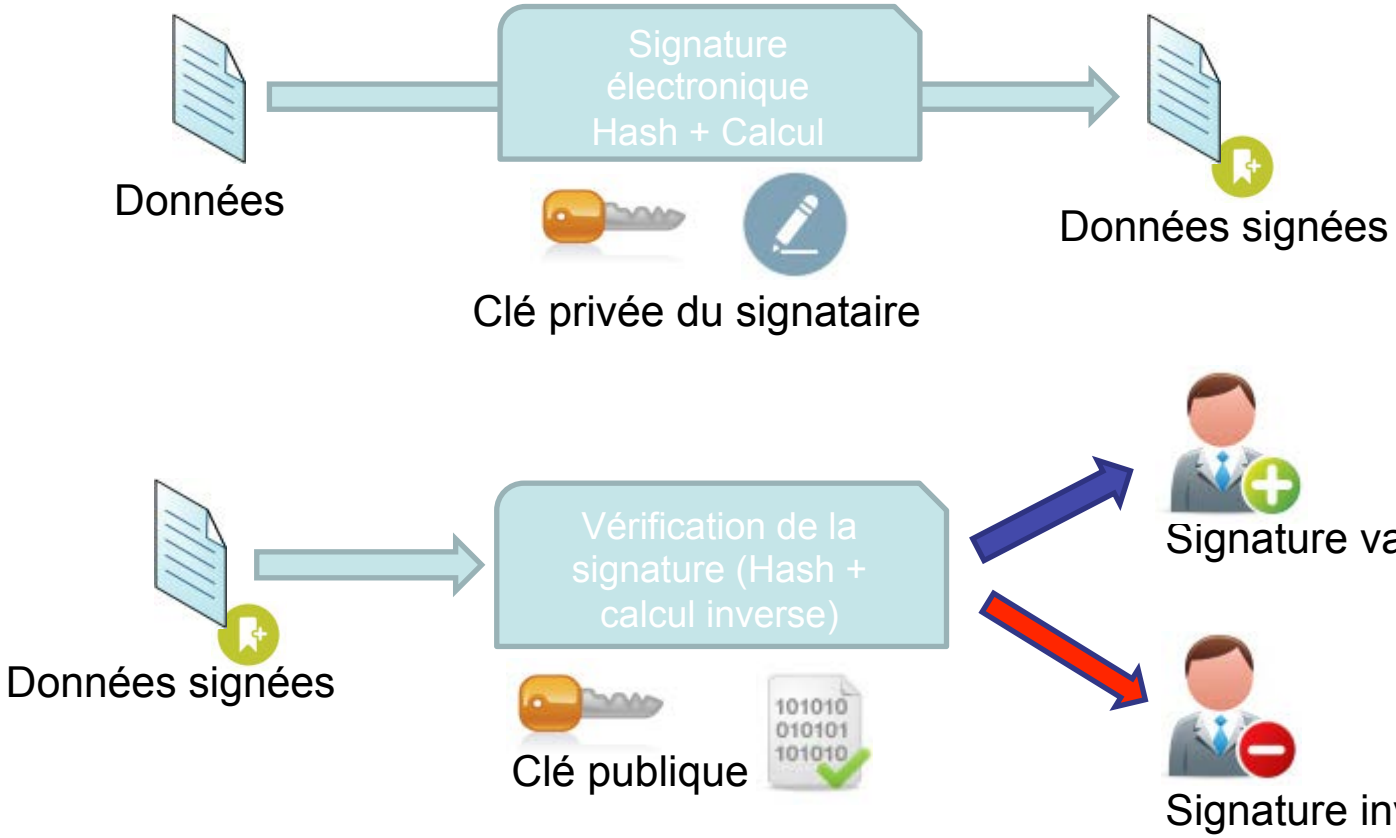
44d01545741d49914484
0832386f8e33dd182393



Signature

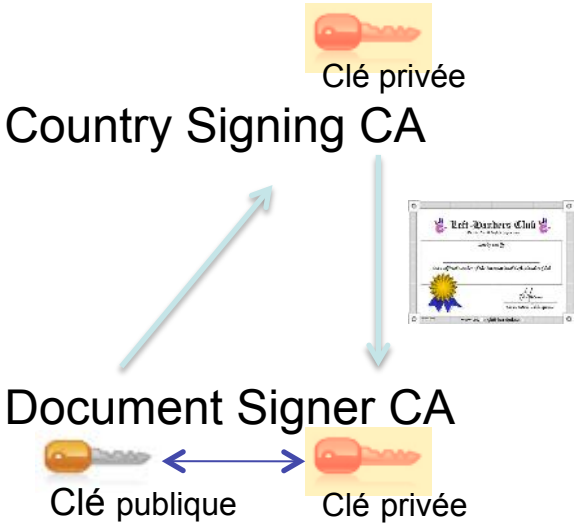
7e0950bb938539162d268b379595
44efb87b718950bf4721dd5c94f5f7
d12fc4efac9d9b5f0c81bbc1555c3d7
6610ef3080a354e60b625f5c50a23
a6bfd13ec024239ddc0b47706c9a23
11fc38e37161e87501236542732797
2469b3985721cc0feca3b04047a9c5
b559e3471a736f5e4c7b473b2e86b1
b21dd8a829828d f8d6

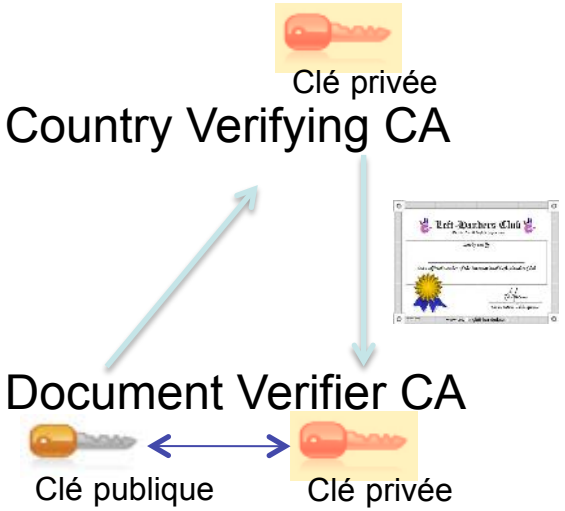
Signature électronique



IGC – Infrastructure de Gestion de Clés

- AC : Autorité de Certification
  - émet des certificats (clé publique signée)
- e-passeport : 4 AC minimum



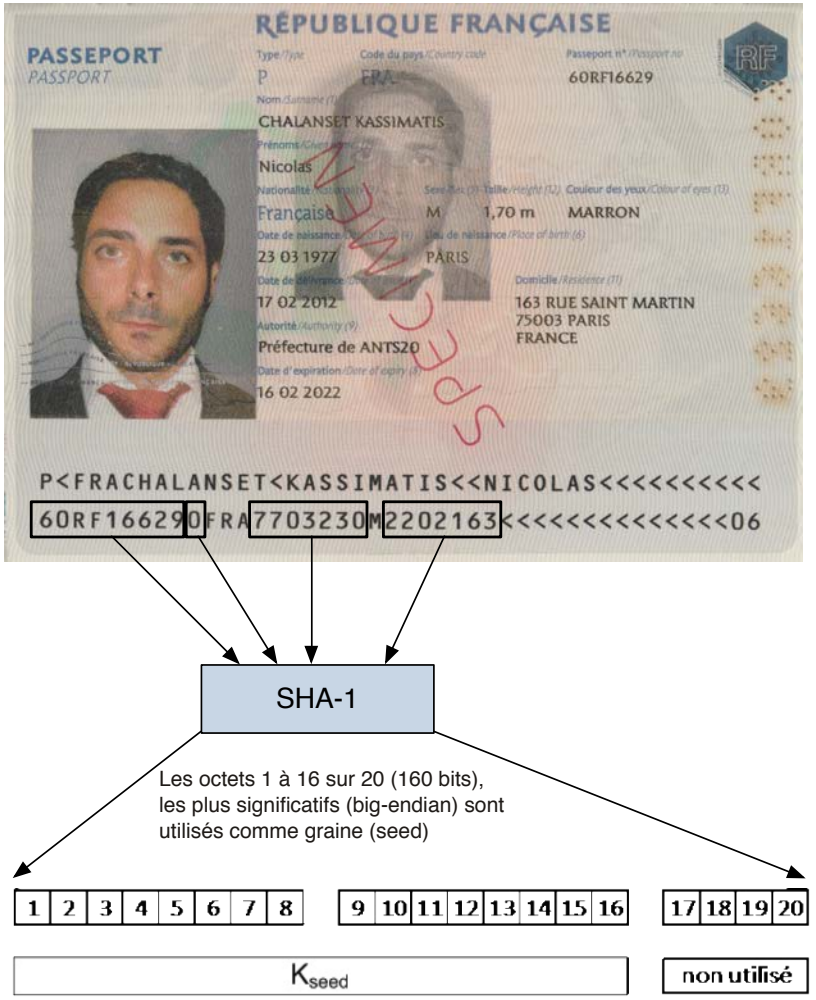


Contrôle d'accès aux données
BAC – Basic Access Control

- contrôle d'accès
  (pour accéder à la puce il faut la page VIZ du passeport)

- canal de communication sécurisé (chiffré)
  (MRTD et IS partagent une clé de session différente à chaque fois)

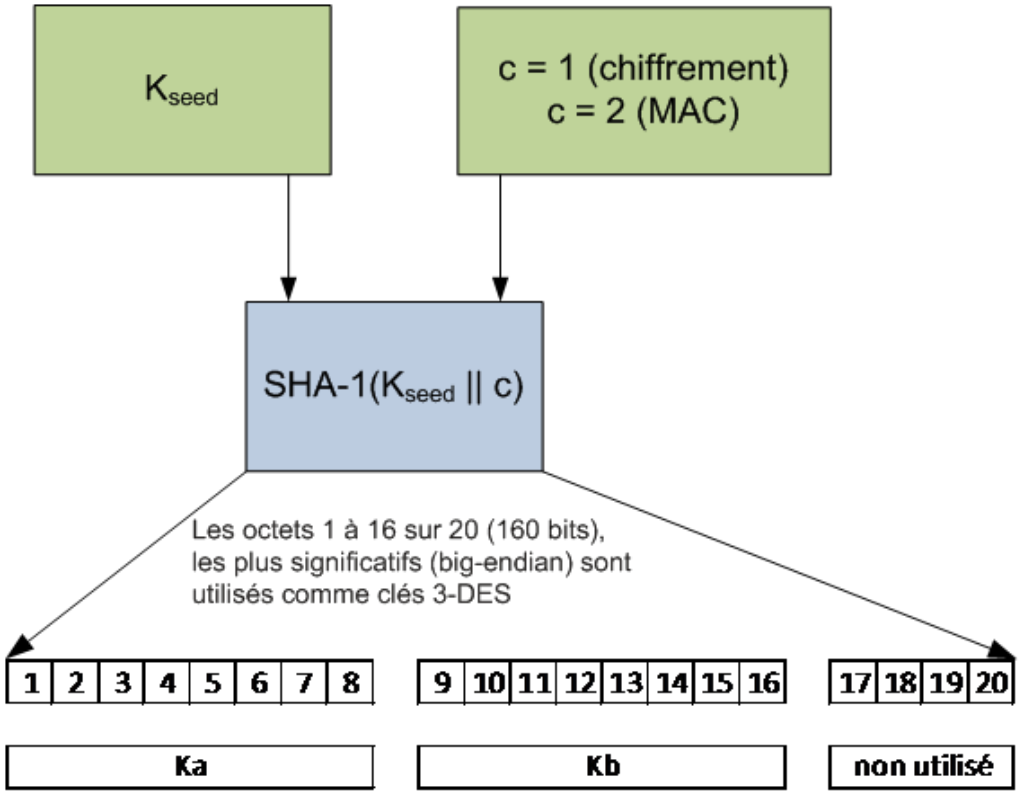
Contrôle d'accès aux données
BAC – Basic Access Control



- numéro de passeport + date de naissance + date d'expiration entropie max 73 bits

- dans certains pays, le numéro de passeport est séquentiel
  → entropie faible
  Belgique : 54 bits

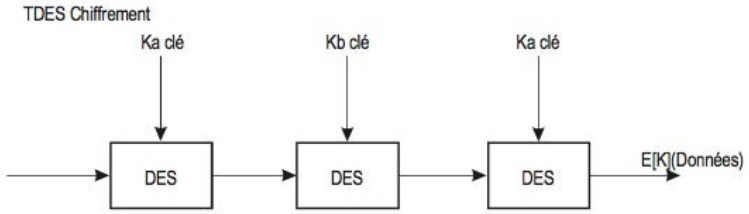
Contrôle d'accès aux données
BAC – Basic Access Control



Entre le MRTD et l'IS :

- défi-réponse symétrique (authentification)
- échange de clés de session ($K_{MRTD} \oplus K_{IS}$)
- communication chiffrée (confidentialité 3DES EDE-CBC)

- K_{ENC} = 128msb (SHA-1(K_{SEED} || 1)
- K_{MAC} = 128msb (SHA-1(K_{SEED} || 2)



Contrôle d'accès aux données
BAC – Basic Access Control

MRTD

IS

N_{MRTD}

$\{N_{IS}, N_{MRTD}, K_{IS}\}\ K_{ENC}$

$\{N_{MRTD}, N_{IS}, K_{MRTD}\}\ K_{ENC}$

- connaît : K_{ENC}
- génère N_{MRTD} ET K_{MRTD} : 64bits

- lit bande MRZ (K_{ENC})
- génère N_{IS} ET K_{IS} : 64bits

MRTD et IS partagent la clé de session $K_{SEED} = K_{MRTD} \oplus K_{IS}$

$K_E = 128msb\ (SHA{-}1(K_{SEED} \,||\, 1))$

$K_M = 128msb\ (SHA{-}1(K_{SEED} \,||\, 2))$

Contrôle d'accès aux données
SAC – Supplemental Access Control

- PACE : Password Authenticated Connection Establishment
  - mot de passe partagé MRZ (BAC)
  - échange de clé Diffie-Hellman auhentifié et chiffré

$\{N_{MRTD}\}\ K_{ENC}$ →

← $\{PK_{IS}\}\ K_{ENC}$

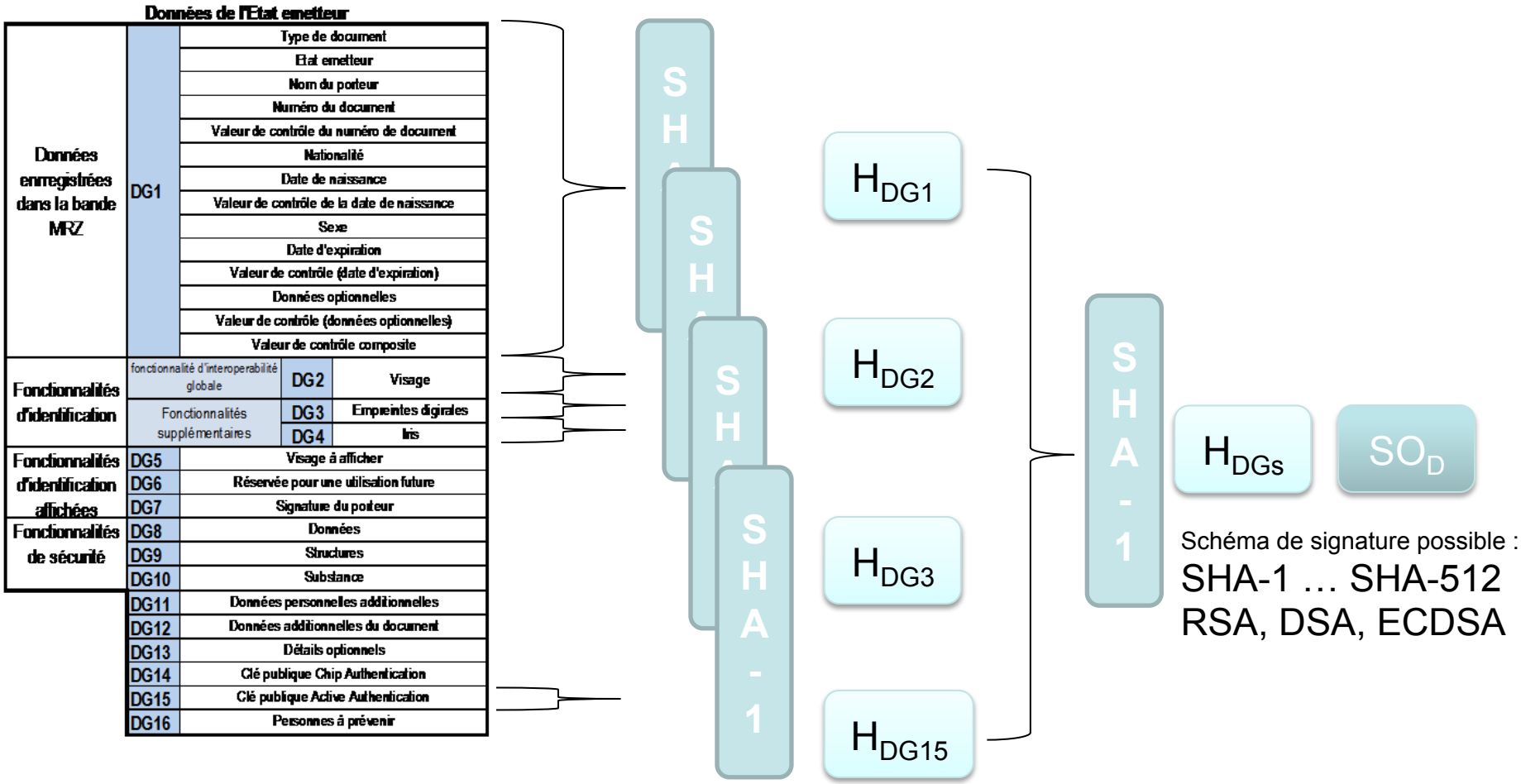
$\{PK_{MRTD}\}\ K_{ENC}$ →

- connaît : K_{ENC} et D
- génère N_{MRTD} et chiffre avec K_{ENC}
- génère D' = f(D, N_{MRTD})
- génère le bi-clé DH ou ECDH

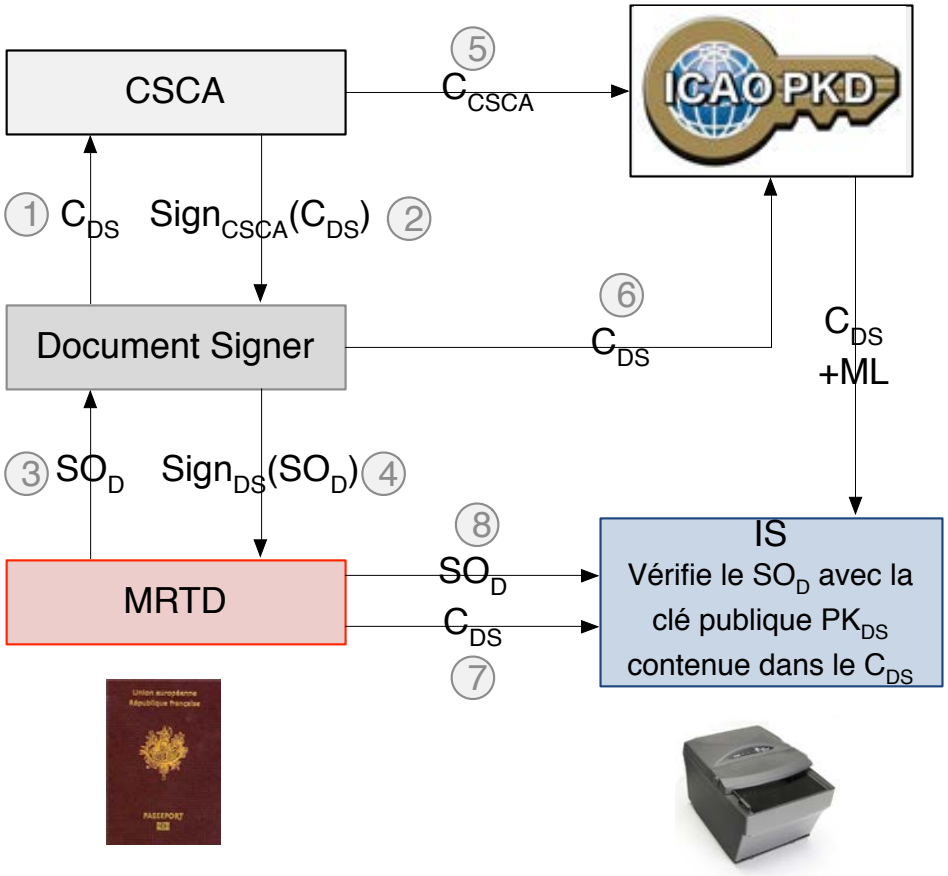
- lit bande MRZ (K_{ENC})
- lit D (EF.CARDACCESS)
- génère D' = f(D, N_{MRTD})
- génère le bi-clé DH ou ECDH

La nouvelle clé de session générée K = $\{PK_{MRTD}\}^{SK_{IS}}$ mod p est utilisée en TDES ou AES

Intégrité et authenticité des données
Passive Authentication



Intégrité et authenticité des données
Passive Authentication

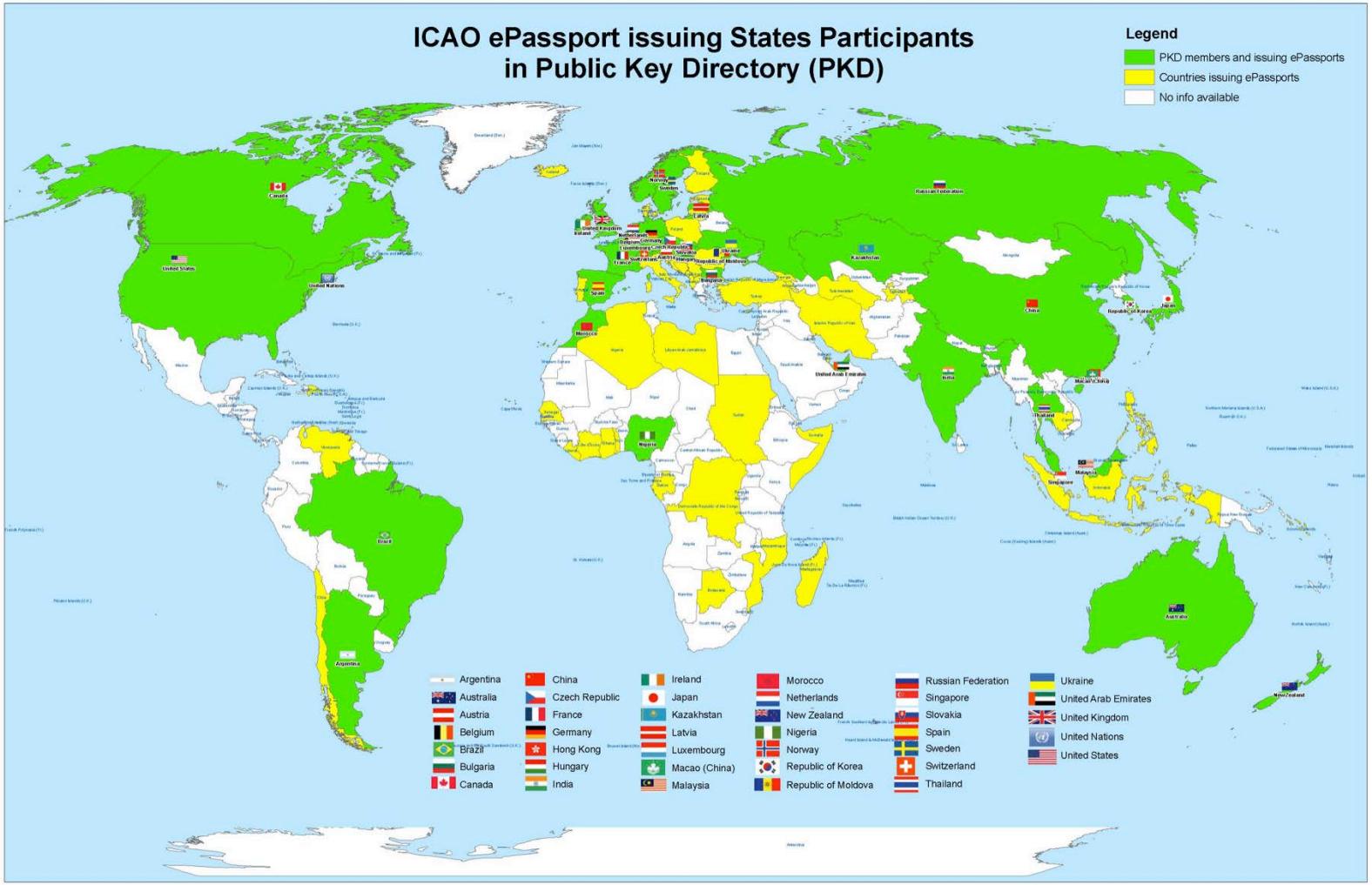


- chaîne de certification par Etat

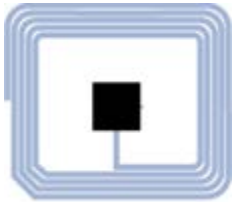
⑦ propagation des C_{DS} dans tous les lecteurs par le PKD (Public Key Directory)

- échange des C_{CSCA} par valise diplomatique et Masterlist

Intégrité et authenticité des données Public Key Directory



Originalité du composant Active Authentication



- mécanisme anti-clonage
  - défi-réponse basé sur la signature (RSA, DSA ou ECDSA)

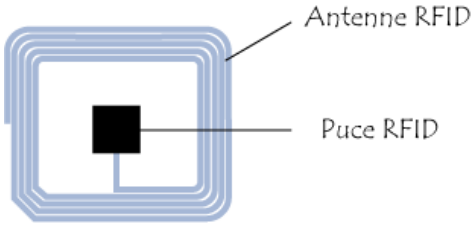
  IS → MRTD : N_{IS} (nonce = données aléatoire)
  MRTD → IS : N_{MRTD}, $H(N_{MRTD},N_{IS})$, $Sig_{MRTD}(N_{MRTD}, N_{IS})$

- clé privée conservée dans une zone protégée de la puce (coffre fort)

- clé publique (DG15) signée avec le SO_D (passive authentication)

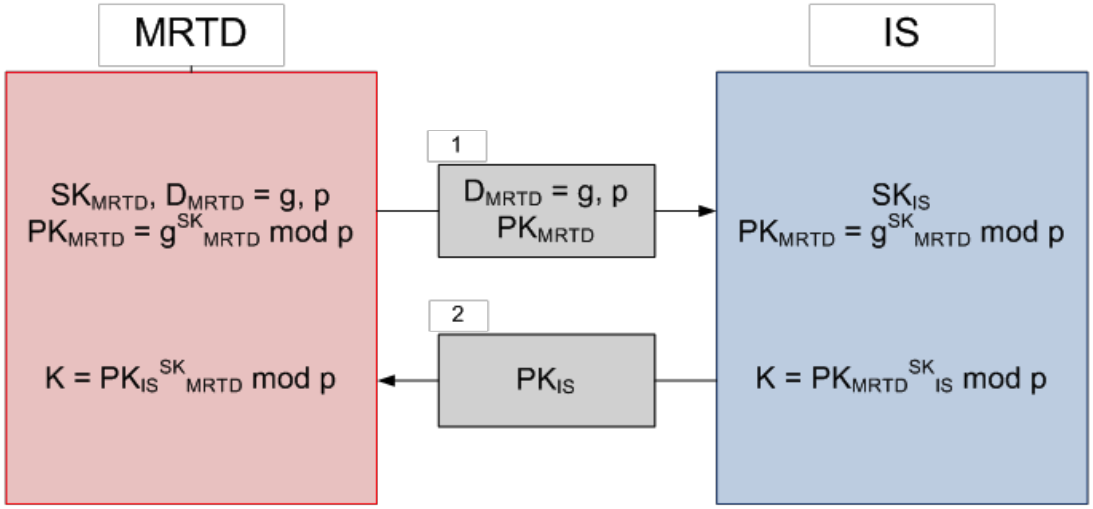
EAC – Extended Access Control
Contrôle d'accès aux empreintes

- authentification mutuelle



  - Chip Authentication
    - authenticité et originalité du composant
    - génération d'une nouvelle clé de session (confidentialité des échanges)
  - Terminal Authentication
    - authentification du lecteur auprès du passeport (i.e. lecteur autorisé à lire les empreintes)

EAC – Chip Authentication v1
Originalité du composant



- échange de clé Diffie-Hellman
- originalité du composant par vérification (passive authentication) de la signature de la clé publique (g, p)
- nouvelles clés de session TDES : K_{ENC} et K_{MAC} (dérivées de K)

EAC – Terminal Authentication v1
Authentification de l'IS

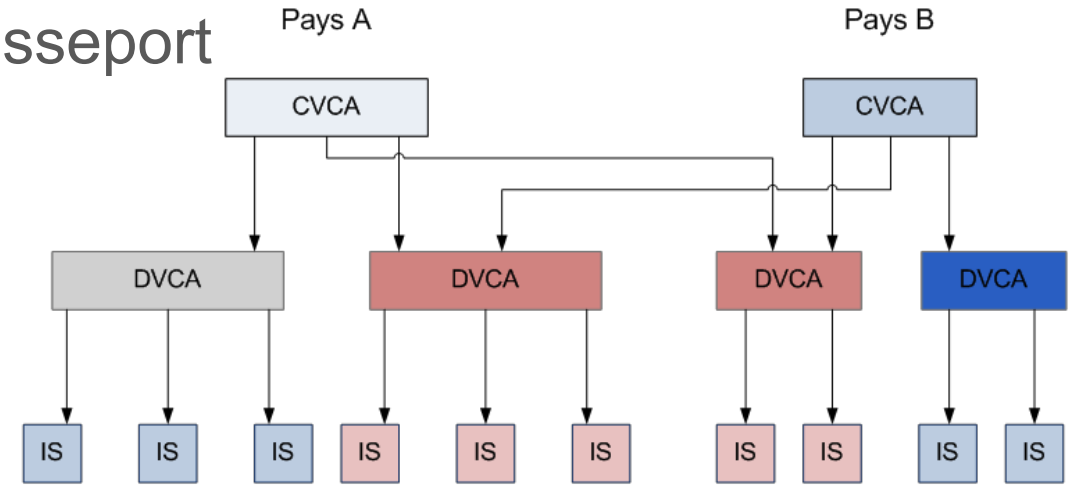
- contrôle de la chaîne de certificats C_{CV}, C_{DV}, C_{IS}
- défi-réponse

IS → MRTD: $C_{CVCA} \ldots C_{IS}$

MRTD → IS : N_{MRTD}

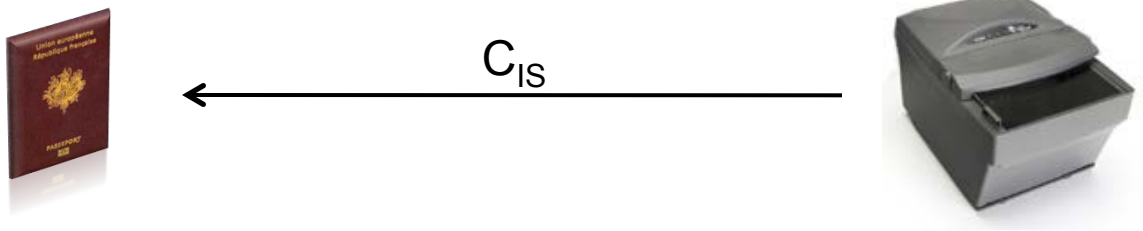
IS → MRTD: $\mathrm{Sig}_{SK_{IS}}(ID_{MRTD}, N_{MRTD}, H(PK_{IS}))$

- ID_{MRTD} = numéro de passeport
- signatures croisées entre Etats



EAC – Terminal Authentication v1
Authentification de l'IS

- pas de liste de révocation dans le passeport
- durée de vie limitée des C_{IS} (1 jour à 1 mois)
- pas d'horloge dans le passeport
  - risque en cas de vol d'un C_{IS}
  - mise à jour de la date du passeport par la date de début de validité du C_{IS}

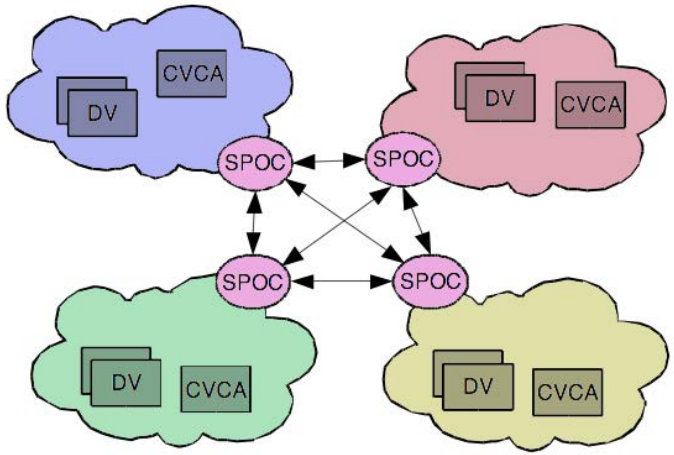


Si $date_{MRTD} < date_{CIS} \rightarrow date_{MRTD} = date_{CIS}$

  - un passeport ne voyageant pas pourra être lu par un IS dont le certificat est expiré

EAC – SPOC – Single Point Of Contact

- CSN 36 9791 (2009)
- obligatoire par la Common Policy
- permet la signature croisée des certificats DV sans connaître tous les DVCA
- autorise les IS d'un pays à lire le DG3 de passeports émis par un autre pays
- tests en cours



EAC – SPOC – Single Point Of Contact

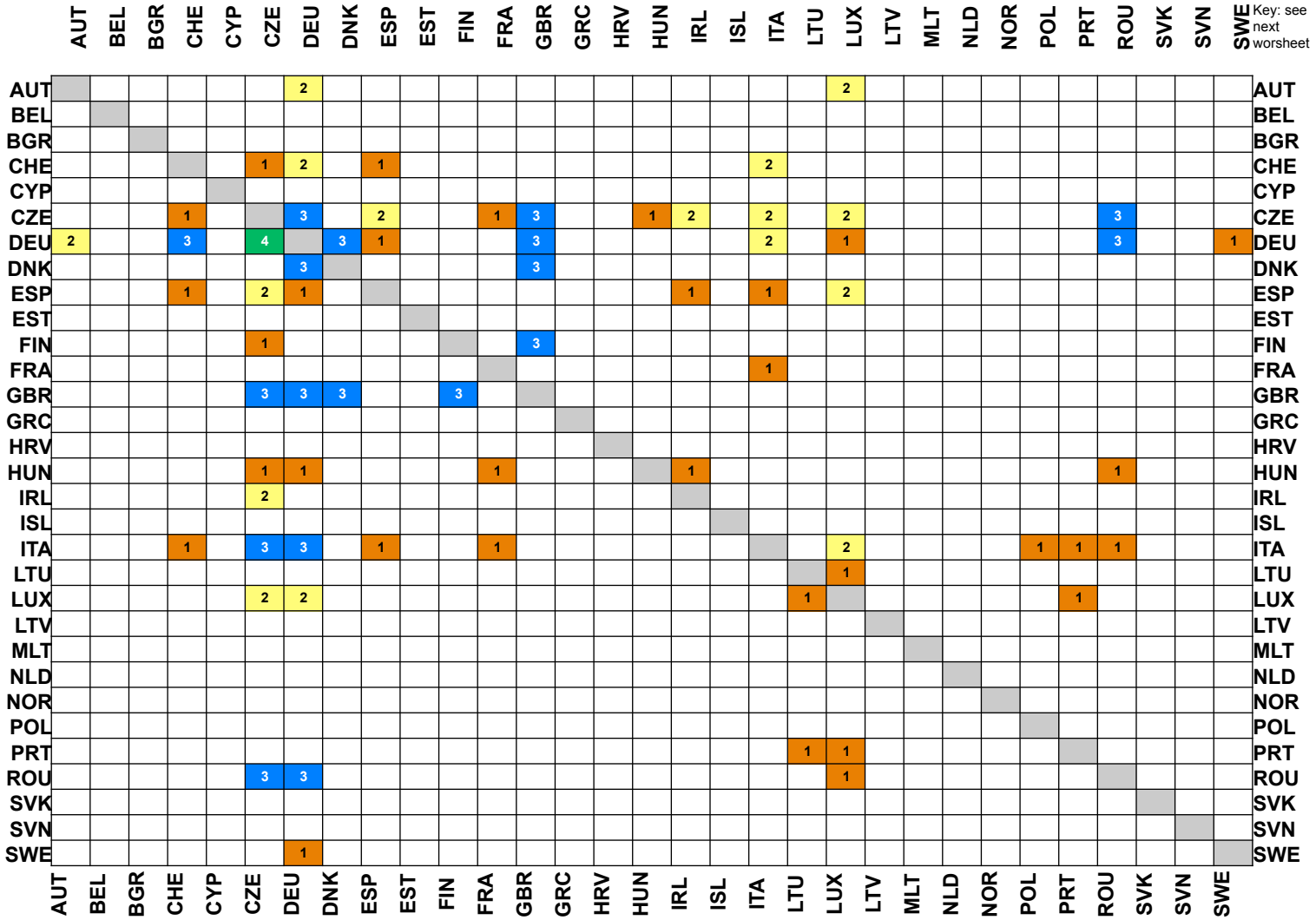
- Nouvelle autorité de certification pour 2 certificats
  - SPOC CA root
    - SPOC TLS serveur
    - SPOC TLS client

- Messages possibles
  - GeneralMessage
  - GetCACertificates
  - RequestCertificate
  - SendCertificates

- SOAP HTTPS

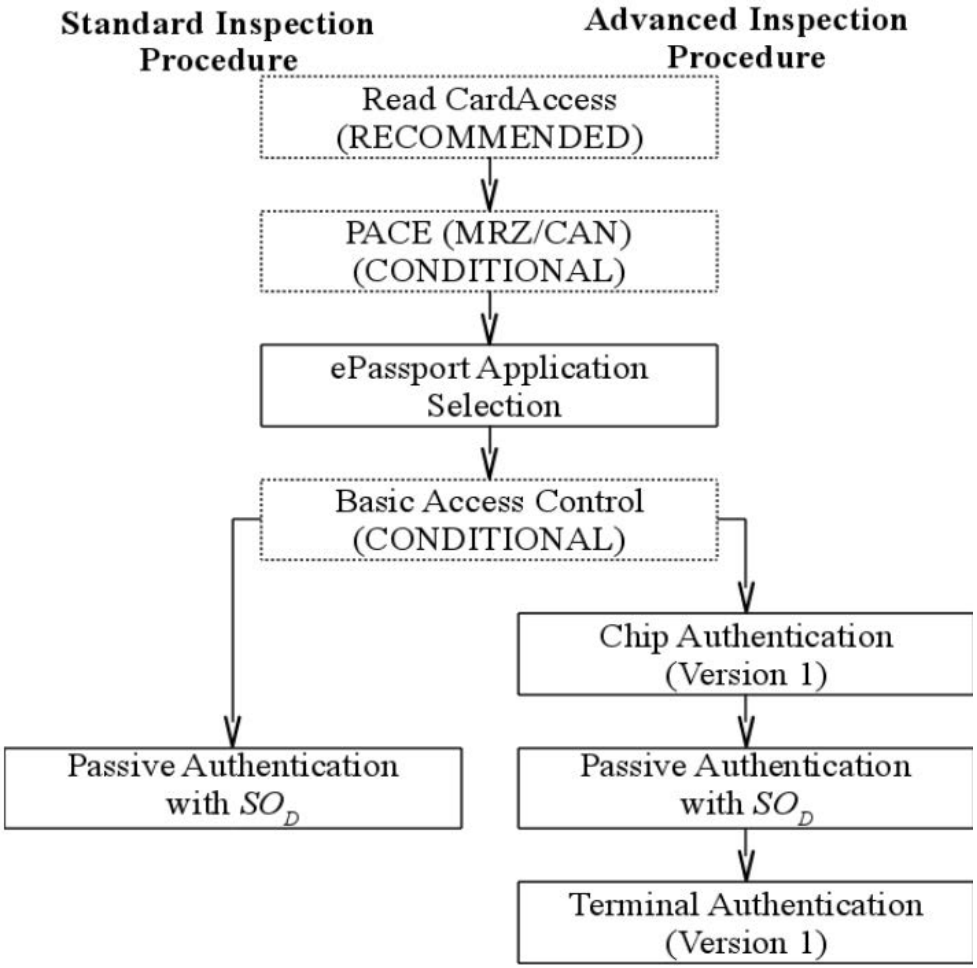
Cipher suite	Certificate and key exchange algorithm
TLS_RSA_WITH_AES_128_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE_ECDSA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA

EAC – SPOC – Single Point Of Contact



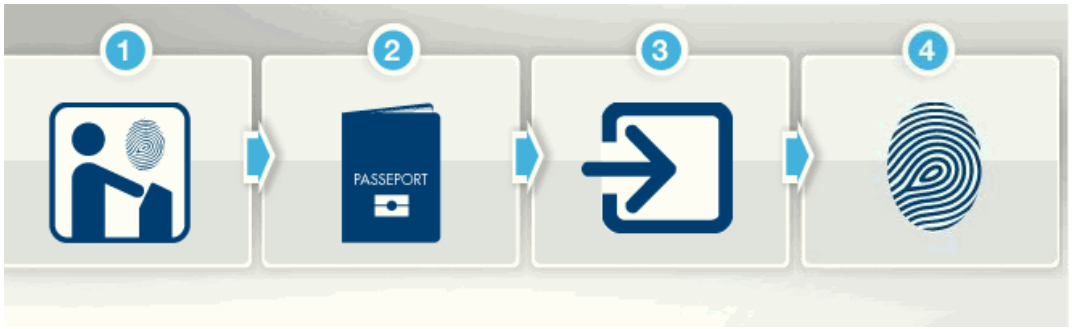
SPOC status 4/12/2014

Lecture d'un passeport



TR-03110_v2.1_P1.pdf

Parafe


1
2
3
4
PASSEPORT


PASSEPORT
PARAFE


Mineurs
Minors
Mineurs
Minors

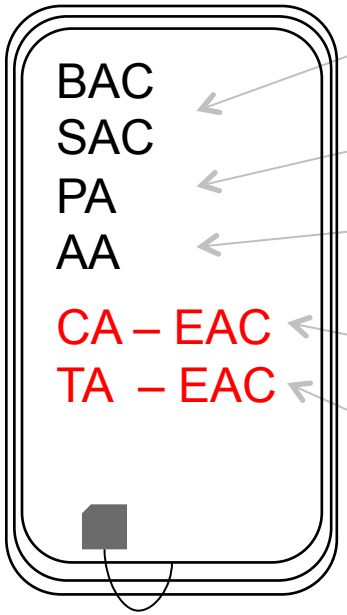
Démo
ce qu'il faut retenir

- EAC
  - mécanisme supplémentaire non obligatoire
  - copie de tous les DG à l'exception du DG3 possible
    → c'est un passeport électronique
    possible usurpation d'identité

- Encore une fois !
  - l'IS doit vérifier la cohérence entre le EF.COM, les DG et le SO_D, est-ce le cas aux frontières ?
  - l'IS est-il au courant qu'un passeport français émis après juin 2009 doit être biométrique ?

Synthèse - mécanismes de sécurité

- BAC : Basic Access Control
- PA : Passive Authentication
- AA : Active Authentication
- EAC : Extended Access Control
- CA : Chip Authentication
- TA : Terminal Authentication

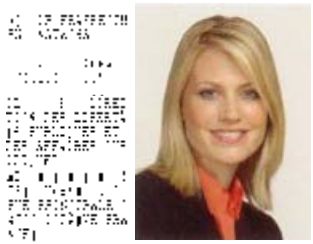


DG 1 à 16 + SO_D (sauf DG 3 & 4)

contrôle d'accès
+ confidentialité des échanges

intégrité et authenticité des données

originalité (authenticité du composant)

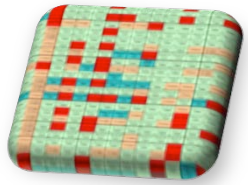


Empreintes DG 3 - Iris DG 4

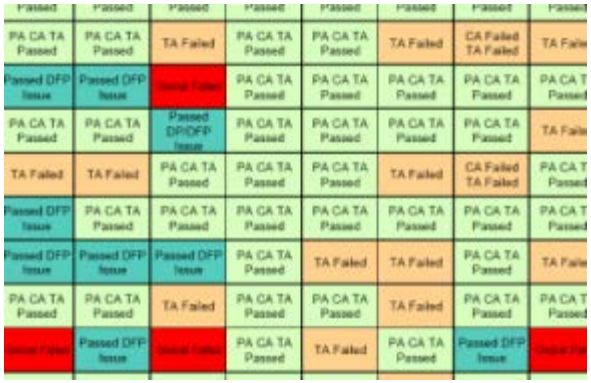
originalité (authenticité du composant)
+ confidentialité des échanges

contrôle d'accès du terminal

Panorama des attaques



- attaques théoriques
  - attaque protocolaire des cas de présence facultative ou obligatoire des mécanismes BAC, PA, AA et EAC
  - enregistrement d'un dialogue BAC légitime pour recherche MRZ exhaustive
  - attaque de la PA par utilisation de la clé publique DSCA non correctement vérifiée par la clé CSCA
  - détournement du protocole AA pour signature illégitime
  - attaque des failles de la chaîne et de la politique de certification EAC des lecteurs, pour lecture illégitime des empreintes
- attaque BAC-MRZ : la plus répandue
  - protections actives avec puce brouilleuse et coupure du circuit
  - protections passives
- attaques systèmes et réseaux des lecteurs IS
  - attaques des implémentations des lecteurs
  - fuzzing et tests sans limites des lecteurs
- attaques puce/composant
  - coordination : fondeur / masqueur / personnalisateur
  - littérature vaste et ancienne !



Chronologie des attaques

- Juillet 05 : « Clonage »
  Obtention des clés privées de certaines puces de passeports
  Marc Witteman

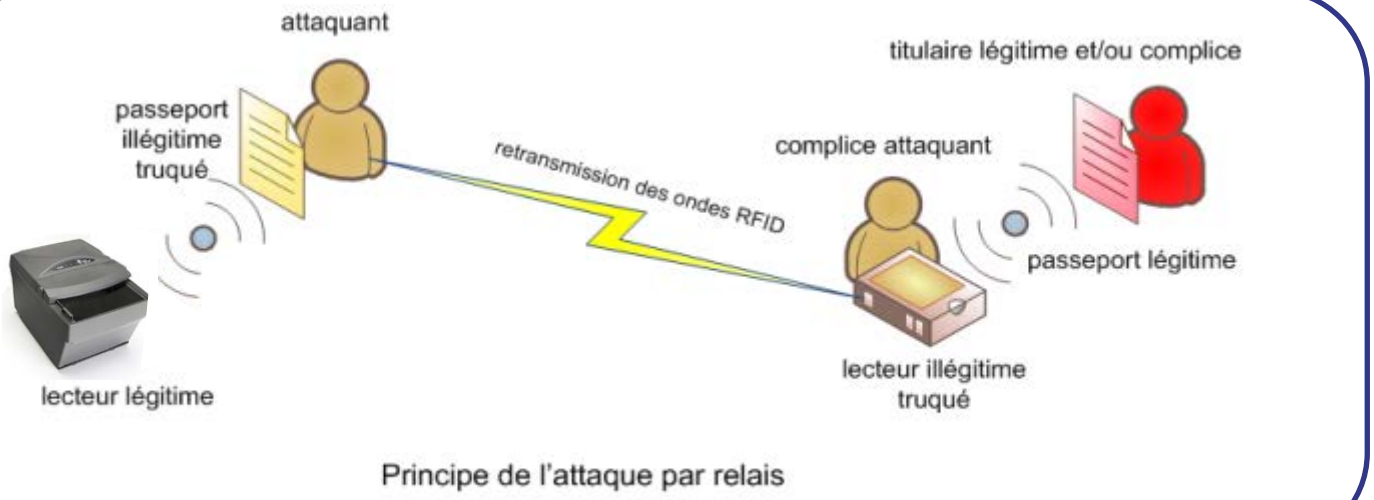
- Août 06 : « Clonage »
  Clonage des informations publiques et attaques sur les back-end
  Lukas Grunwald

- Novembre 06 : « Cracked it ! »
  Lecture illégitime du passeport à distance
  Adam Laurie & the Guardian

- Août 08 : « Falsification de passeport »
  Exploitation de faiblesses des IS pour créer des passeports auto-signés et désactiver l'Active Authentication
  vonJeek

- Aout 2010 : « Attaque sur les implémentations des IS »
  Fabrication d'une fausse puce permettant de faire « planter » l'IS et lui faire exécuter du code malveillant, indiquant que le passeport est légitime.

Attaque RFID par relais : facile !



Principe de l'attaque par relais

- mesures de protection:
  - la protection des échanges
    (cage de faraday, isolation physique, optique, sonore et mécanique)
  - le développement d'algorithme de « distance bounding »

Les faiblesses des puces

- obtention des clés privées :
  - attaque par “Differential Power Analysis” pour obtenir la clé privée du passeport contenue dans la partie privée de la puce
  - dépend essentiellement du composant choisi par le pays

- solutions :
  - rendre obligatoire l’AA pour détecter les clones
  - utiliser des composants électroniques qualifiés de qualité !
  - responsabilité des fondeurs et des autorités nationales

http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf

Les faiblesses des back-end

- lire un passeport fait appel
  à une multitude de « parser »
  - ASN.1, pkcs7, texte, JPG, JPG2000, CBEFF ISO 19785 (données biométriques)
  - terrain propice aux débordements de tampon, d'entier, ...
  - exécution de code arbitraire sur les systèmes de contrôle (IS)
  - déni de service au contrôle aux frontières

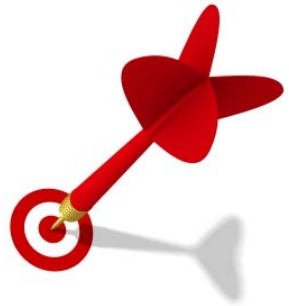
http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grunwald.pdf

Attaque sur le « BAC », une attaque ciblée

- permet sous certaines conditions la lecture de tous les DG excepté 3 & 4 (empreintes et iris)

- « faiblesse » de la source d'entropie de la clé BAC
  - n° de passeport + date de naissance + date d'expiration (24 octets) pour dériver les clés du BAC
  - prédictibilité de certaines informations
  - attaque par force brute sur le reste

- attaque réalisée sur un passeport **anglais :**
  - remise par courrier postal (interception du titre)
  - numéro de passeport séquentiel et date d'expiration prévisibles les premières années
  - date de naissance de la cible récupérable sur des réseaux sociaux



http://www.guardian.co.uk/technology/2006/nov/17/news.homeaffairs

Création de profils de passeports

- des variations dans les implémentations permettent de déterminer la « nationalité » d'un passeport avant toute authentification

- passeport australien:
  - ne respecte pas strictement la norme ISO 14443
  - permet d'énumérer les DG avant l'authentification
- passeport italien
  - n'utilise pas d'UID aléatoire
  - **permet de suivre un passeport dans l'espace et le temps**
  - comme votre **GSM Bluetooth ...** ;-)
- passeport américain
  - ne renvoi pas correctement un octet sensé être aléatoire
- intérêt réel ?

http://rfidiot.org/#Passport_profiling
http://www.bluetoothtracking.org

Les systèmes de contrôle : maillon faible

- une « liberté » dans la norme OACI permet de contourner l'Active Authentication
  - modifier l'index (EF.COM) pour tromper le système de contrôle sur le support de l'AA par le passeport
  - la norme devrait imposer de vérifier la présence du hash du DG15 dans le SO_D
- certains systèmes ne vérifient pas les chaînes de confiance lors de la Passive Authentication (certificats inconnus).
- les problèmes d'implémentation seront une source importante de risques (comme d'habitude...)

http://freeworld.thc.org/thc-epassport/
http://www.jmrtd.org
https://www.os3.nl/2008-2009/epassport_eng

Démo
ce qu'il faut retenir

- Active Authentication
  - absente du passeport français… dommage
- Passive Authentication
  - vérifier l'implémentation des contrôles réalisés dans les IS Parafe, 4en1, autres outils

une recette n'est pas uniquement fonctionnelle sur de vrais passeports

- clonage d'un passeport
  - l'IS doit vérifier la cohérence entre le EF.COM, les DG et le SO_D, est-ce le cas aux frontières ?
  - l'OS et/ou sa vitesse peuvent être testés (JavaCard vs Natif)