



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

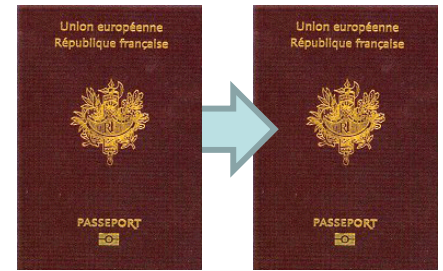
Le Passeport Biométrique

Benoit LEGER – CISSP – ISO 27001-LD



Qu'est ce qui change ?

- Le passeport électronique :
 - c'est le passeport aujourd'hui délivré depuis 2,5 ans
 - 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 biométrique :
 - c'est le passeport aujourd'hui délivré depuis 1 mois
 - il contient toujours une puce RFID
 - il respecte les normes de contrôle d'accès BAC et **EAC**
 - **l'empreinte** est une donnée biométrique à **accès restreint**
- Attention aux **différences** entre données biométriques :
 - l'empreinte digitale (bio. avec trace)
 - la photo (sexe, âge, couleur des yeux, couleur de la peau)
 - CNIL : avec ou sans trace (la photo est-elle sans trace ?)



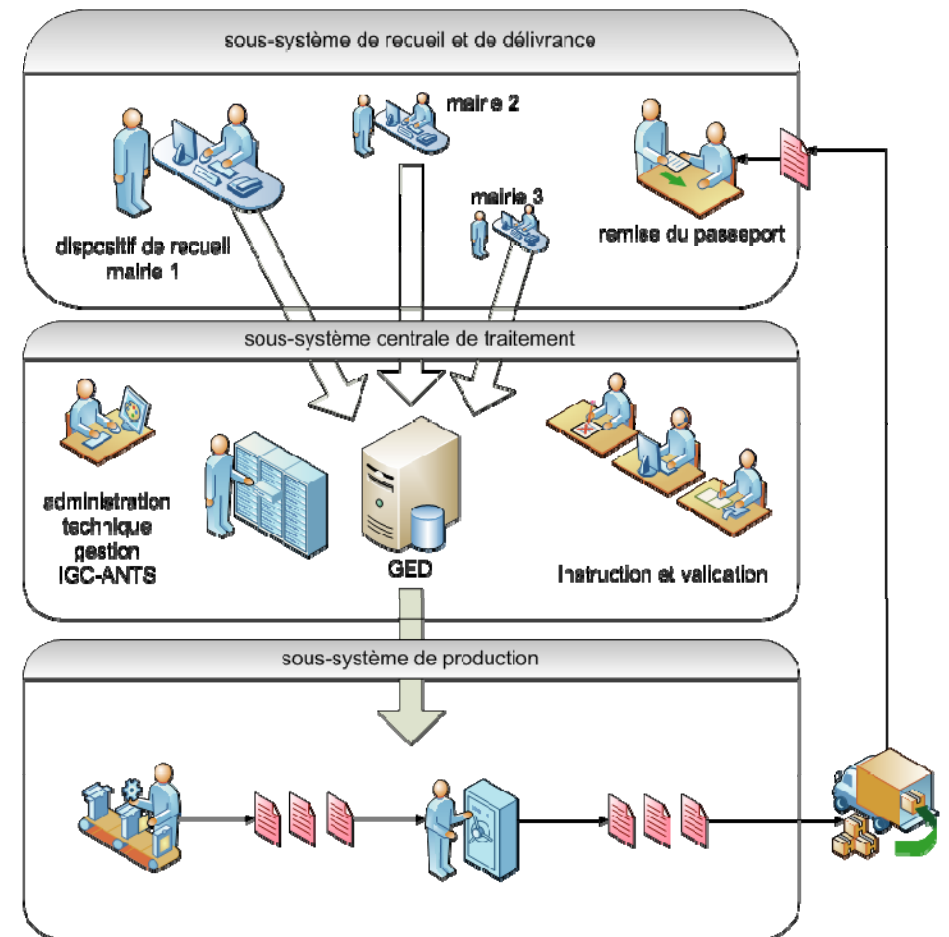
PsP-Bio : règlements et normes



- Textes :
 - engagements européens :
un passeport biométrique pour le **28 juin 2009**
(article 6 du règlement CE n° 2252/2004 du **13 décembre 2004**)
 - le règlement (CE) établit les spécifications techniques des passeports et des documents de voyage (MRTD)
 - décision de la Commission du **28 février 2005** établissant les spécifications techniques relatives à l'intégration de l'image de face
 - spécifications techniques supplémentaires pour le stockage et la protection des empreintes digitales, nouvelle décision du **28 juin 2006**
 - DCSSI - Normes et standards – PSSI & SMSI
 - Travaux de normalisation du BIG : Brussels Interoperability Group
 - Décrets nationaux - Obligations CNIL
Haut fonctionnaire de défense - Marchés publics
- Normes :
 - OACI doc. 9303 partie I
 - volume I (éléments physiques)
 - volume II (puce électronique)
 - EAC TR03110 v 1.1 – Extended Access Control

Obtenir un passeport biométrique

- Démarche identique :
 - dépôt de la demande en mairie avec empreintes et photo
 - instruction, validation et délivrance en préfecture
 - remise en mairie au lieu de dépôt



MRTD et IS

MRTD

Machine Readable Travel Document



PASSEPORT



IS

Inspection System

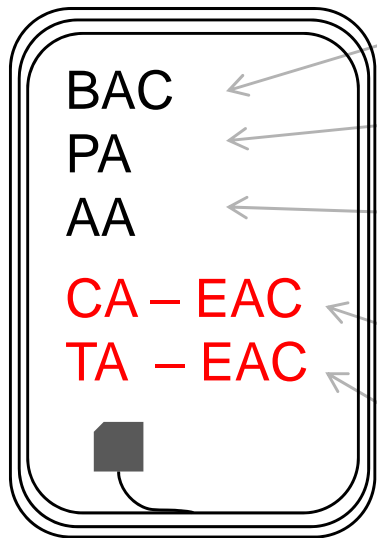


LECTEUR

système de contrôle

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

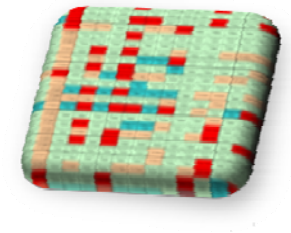
originalité (authenticité du composant)

+ confidentialité des échanges

contrôle d'accès du terminal



Panorama des attaques

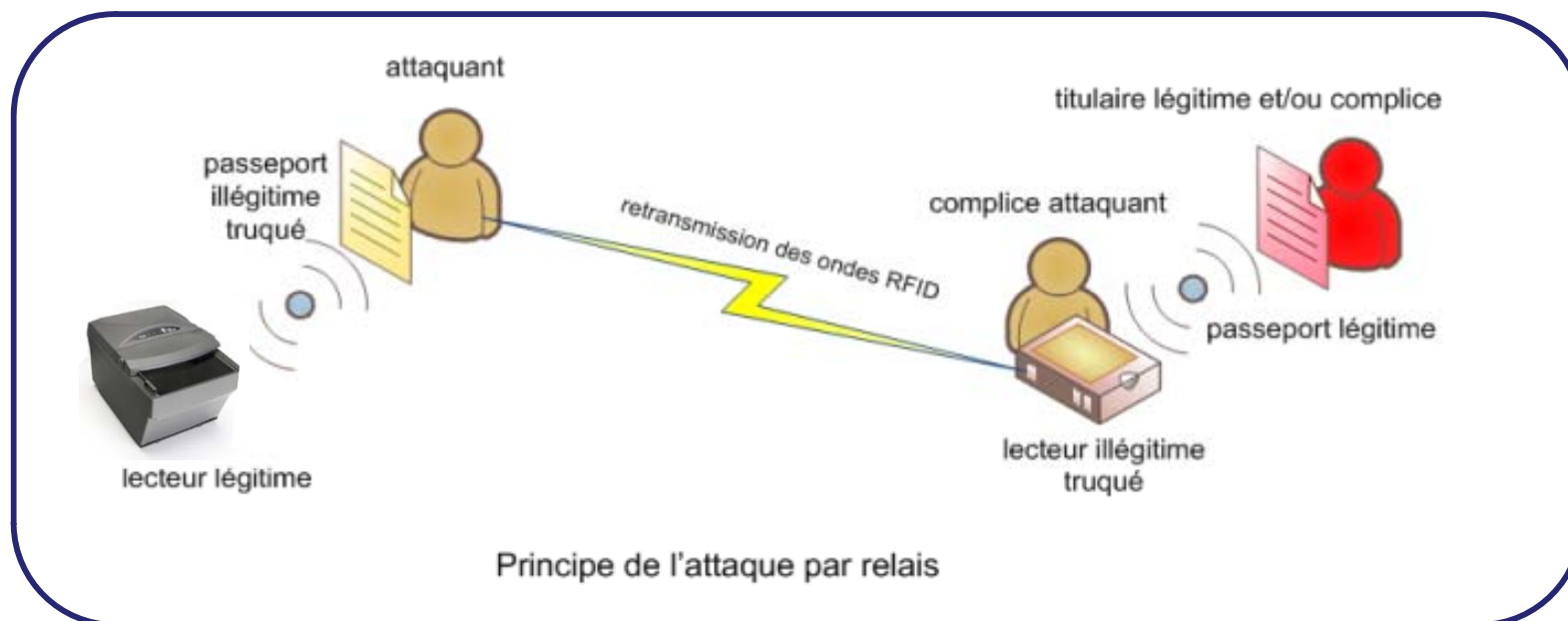


- attaques théoriques
 - attaque protocolaire des cas de présence facultative ou obligatoire des mécanismes BAC, PA, AA et EAC
 - enregistrement d'un dialogue BAC légitime pour recherche MRZ exhaustive
 - attaque de la PA par utilisation de la clé publique DSCA non correctement vérifiée par la clé CSCA
 - 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 !

Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed
PA CA TA Passed	PA CA TA Passed	TA Failed	PA CA TA Passed	PA CA TA Passed	TA Failed	CA Failed TA Failed	TA Failed
Passed DFP Issue	Passed DFP Issue	Issue Issue	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	PA CA T Passed
PA CA TA Passed	PA CA TA Passed	Passed DPROFF Issue	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	TA Failed
TA Failed	TA Failed	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	TA Failed	CA Failed TA Failed	PA CA T Passed
Passed DFP Issue	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	PA CA TA Passed	PA CA T Passed
Passed DFP Issue	Passed DFP Issue	Passed DFP Issue	PA CA TA Passed	TA Failed	TA Failed	PA CA TA Passed	TA Failed
PA CA TA Passed	PA CA TA Passed	TA Failed	PA CA TA Passed	PA CA TA Passed	TA Failed	PA CA TA Passed	PA CA T Passed
Issue Issue	Passed DFP Issue	Issue Issue	PA CA TA Passed	TA Failed	PA CA TA Passed	Passed DFP Issue	Issue Issue



Attaque RFID par relais : facile !



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

Questions ?





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

Mécanismes de sécurité des passeports biométriques

Nicolas Chalanset – CISSP – ISO 27001LD



Données du passeport

Data Group

DG	Contenu	Contrôle d'accès	Obligatoire / Facultatif
DG1	Données imprimées	BAC	Obligatoire
DG2	Biométrie : Visage	BAC	Obligatoire
DG3	Biométrie: Empreintes	BAC + EAC	Obligatoire
DG4	Biométrie: Iris	BAC + EAC	Facultatif
...		BAC	Facultatif
DG14	Clé publique Chip Auth	BAC	Facultatif
DG15	Clé publique Active Auth	BAC	Facultatif
DG16	...	BAC	Facultatif
SOD	Security Object Data	BAC	Obligatoire

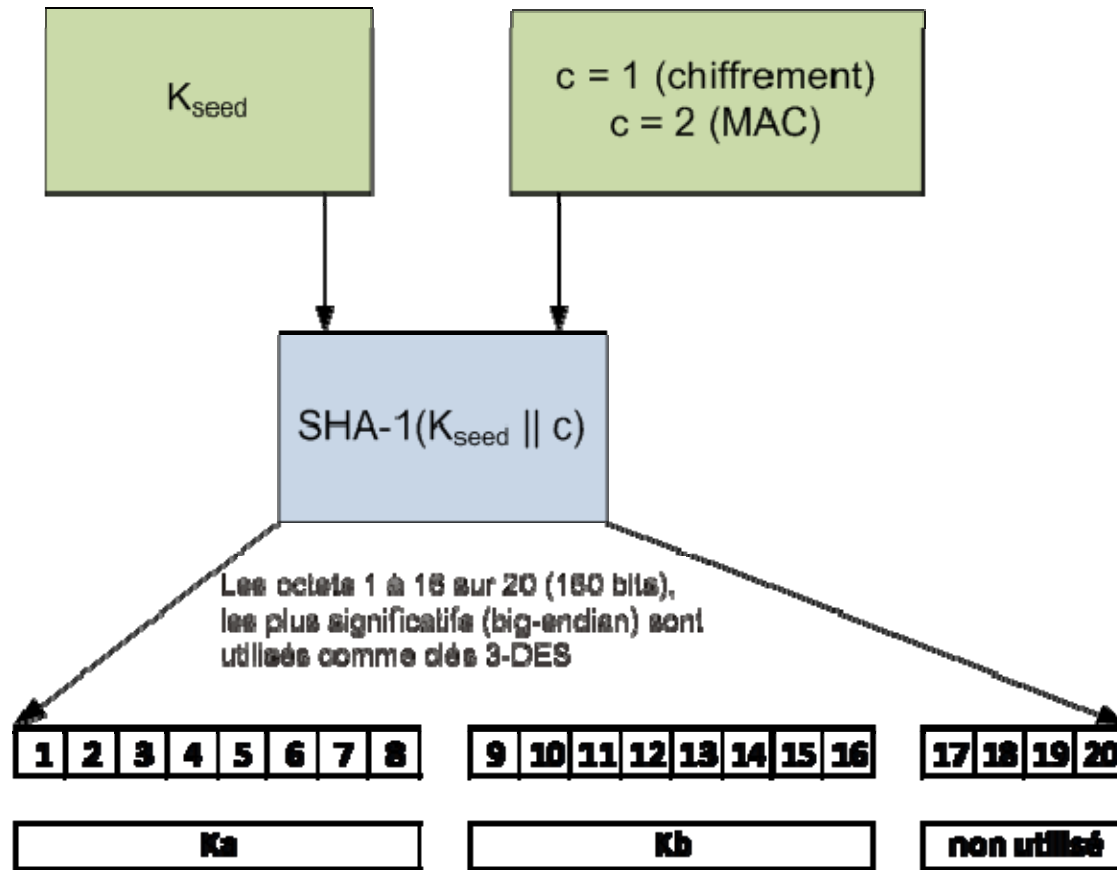
Bob X



XC 111111 1
 231 23456 100
 8765 43210 123456
 5432 109876543
 1001 1111111111
 1001

Contrôle d'accès aux données

BAC – Basic Access Control



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

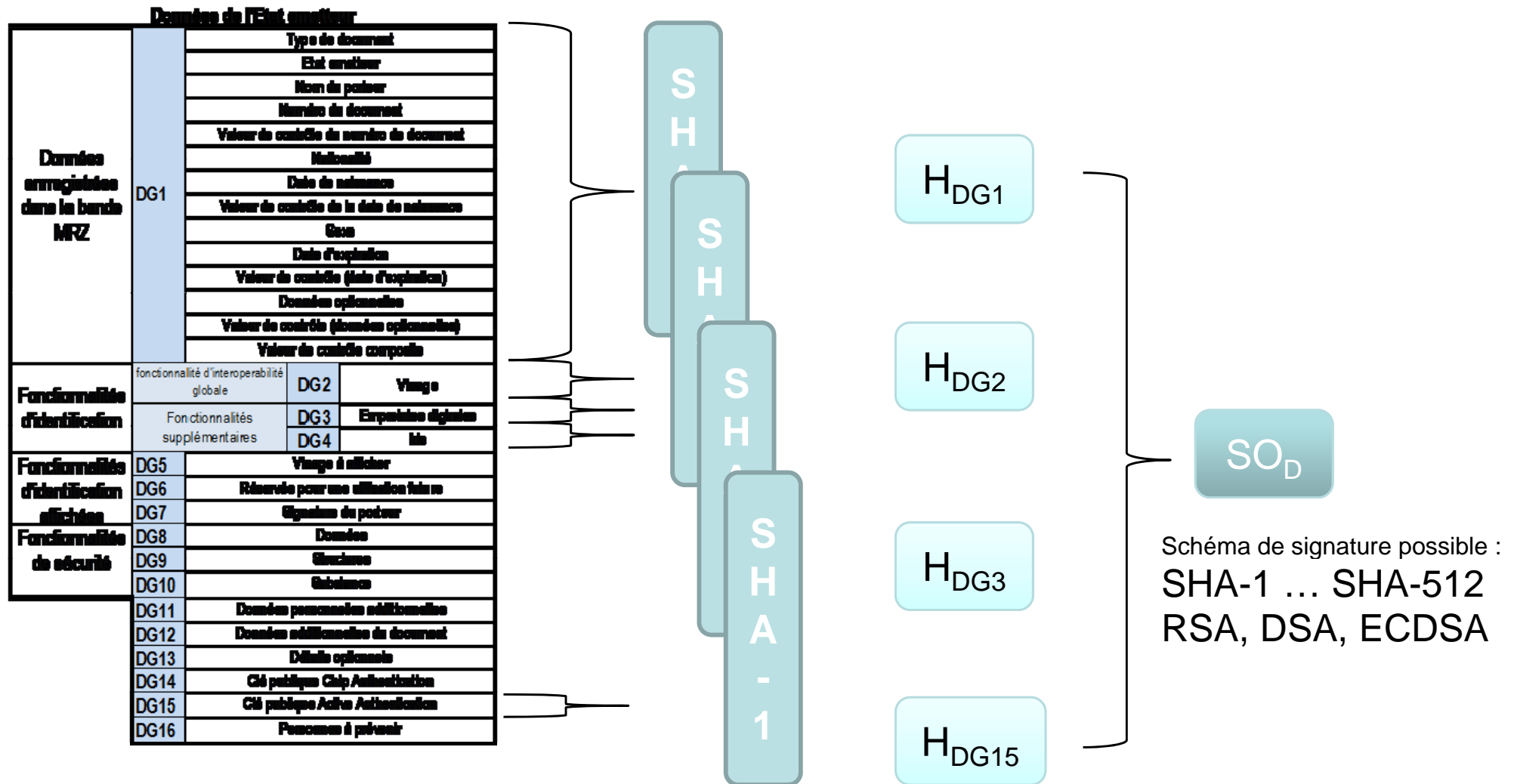
MRTD \rightarrow IS : N_{MRTD}

IS \rightarrow MRTD : $\{N_{IS}, N_{MRTD}, K_{IS}\}_{K_{ENC}}, \text{MAC}_{K_{MAC}}(\{N_{IS}, N_{MRTD}, K_{IS}\}_{K_{ENC}})$

MRTD \rightarrow IS : $\{N_{MRTD}, N_{IS}, K_{MRTD}\}_{K_{ENC}}, \text{MAC}_{K_{MAC}}(\{N_{MRTD}, N_{IS}, K_{MRTD}\}_{K_{ENC}})$

Intégrité et authenticité des données

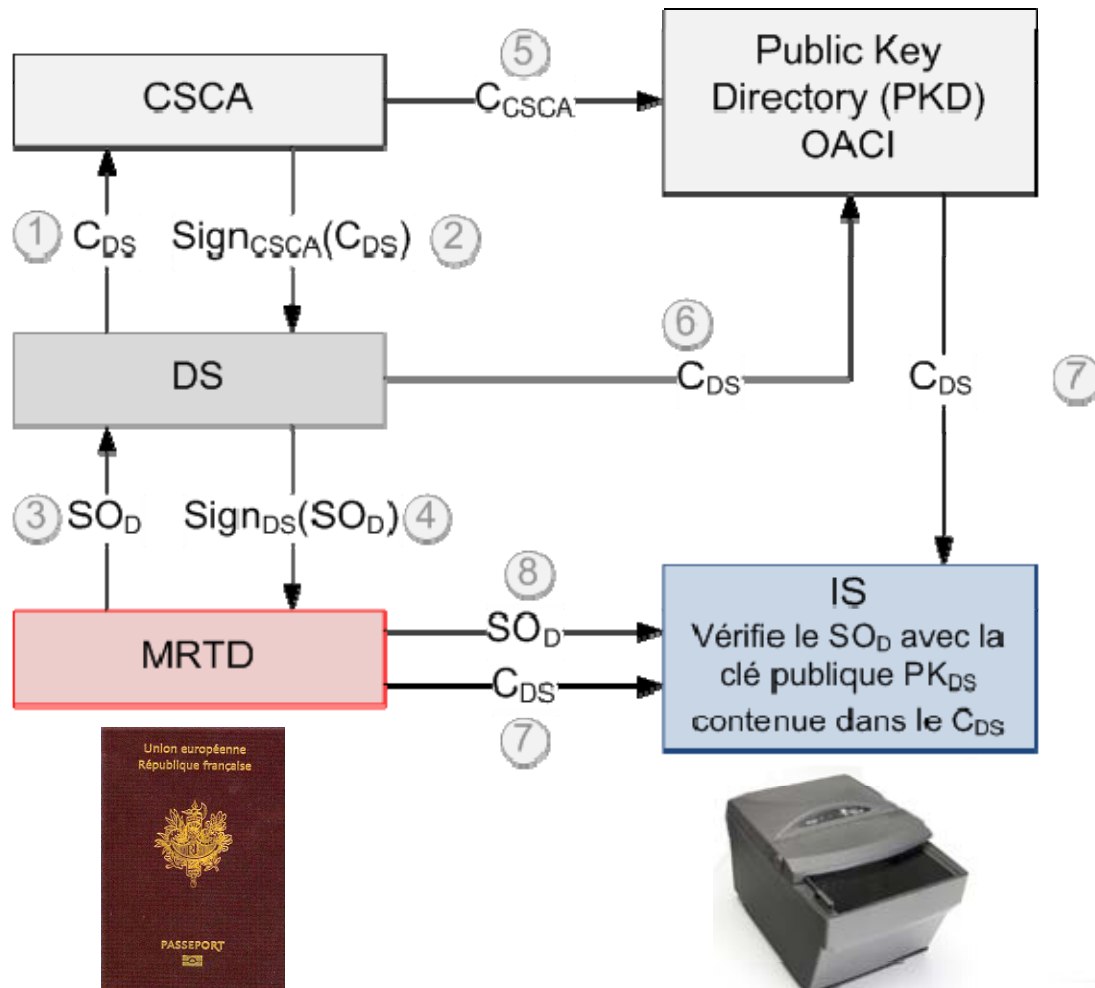
Passive Authentication



RFC3447 (PKCS #1) : RSASSA-PSS et RSASSA-PKCS1_v15
 FIPS 186-2 (DSA), X 9.62 (ECDSA), FIPS 180-2 (SHA-x)

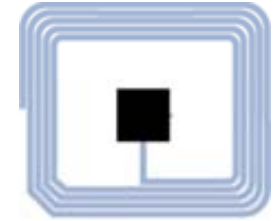
Intégrité et authenticité des données

Passive Authentication



- chaîne de certification par Etat
- propagation des C_{DS} dans tous les lecteurs par le PKD (Public Key Directory)
- échange des C_{CS} par valise diplomatique

Originalité du composant Active Authentication



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

IS \rightarrow MRTD : N_{IS} (nonce aléatoire)

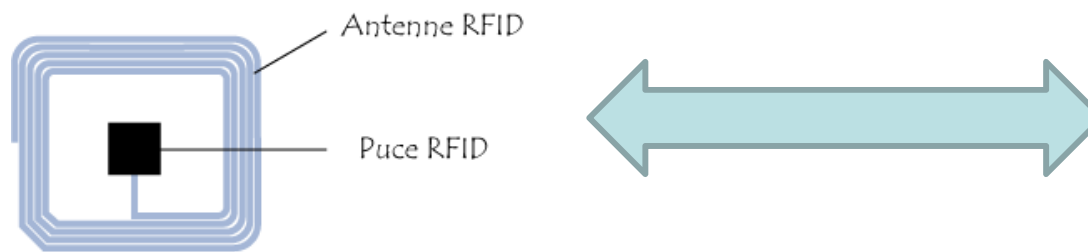
MRTD \rightarrow IS : $\text{Sig}_{\text{MRTD}}(M1, N_{IS})$

- **détournements possibles**
 - traçabilité des porteurs par signature d'une information de type lieu et date. Dans ce cadre, le passeport signerait son passage à un endroit précis.
 - les Etats pourraient contrôler et suivre les passages des citoyens
 - à leur insu, si ce mécanisme est implémenté sans le BAC

Contrôle d'accès aux empreintes

EAC - Extended Access Control

- Authentification mutuelle



- Chip Authentication

- **authenticité** et **originalité** du composant
 - génération d'une clé de session (confidentialité des échanges)

- Terminal Authentication

- authentification du lecteur auprès du passeport (i.e. lecteur autorisé à lire les empreintes)

Contrôle d'accès du terminal

Terminal Authentication



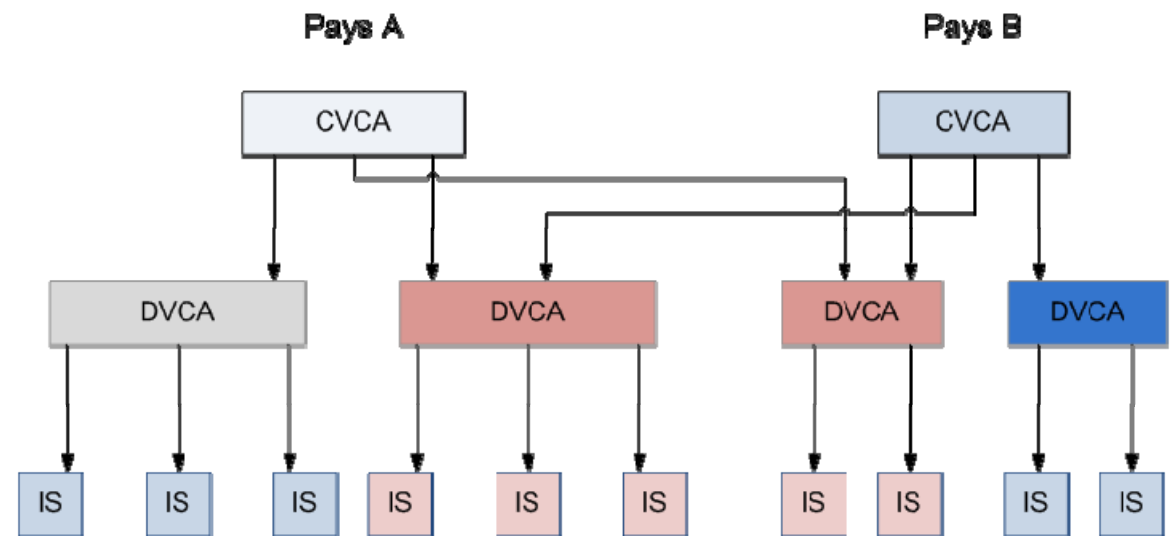
- contrôle de la chaîne de certificats C_{CV} , C_{DV} , C_{IS}
- défi-réponse

IS \rightarrow MRTD: $C_{CVCA} \dots C_{IS}$

MRTD \rightarrow IS : N_{MRTD}

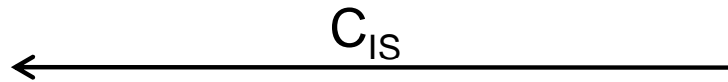
IS \rightarrow MRTD: $\text{Sig}_{SK_{IS}}(ID_{MRTD}, N_{MRTD}, H(PK_{IS}))$

- Signatures croisées entre Etat



EAC – Terminal Authentication

- **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}



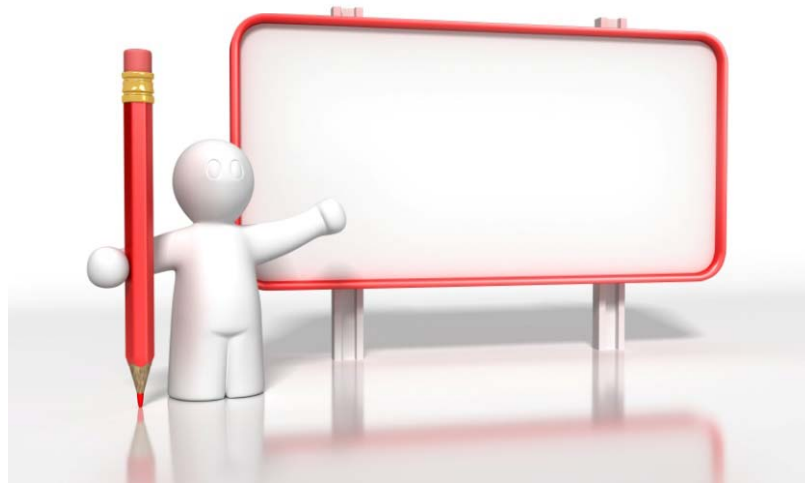
Si $date_{MRTD} < date_{CIS} \rightarrow date_{MRTD} = date_{CIS}$

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

Synthèse

Normes	Mécanismes	Objectifs de sécurité	Fonctions Cryptographiques	Obligatoire / Facultatif
OACI 9303	BAC	contrôle d'accès confidentialité des échanges	défi-réponse (symétrique) échange de clés de session	facultatif
OACI 9303	Passive Auth.	intégrité et authenticité	signature numérique	obligatoire
OACI 9303	Active Auth.	originalité du composant	défi-réponse (asymétrique)	facultatif
EAC TR03110 v 1.1	Chip Auth.	originalité du composant confidentialité des échanges	échange de clé Diffie-Hellman	obligatoire
EAC TR03110 v 1.1	Terminal Auth.	contrôle d'accès (authentification du lecteur)	vérification de certificats défi-réponse (asymétrique)	obligatoire

Démo !





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



Synthèse des « attaques » sur les passeports biométriques

Jean-Philippe Teissier – CISSP associé

Chronologie des attaques



- **Juillet 05** : « Clonage »
Obtention des clés privées de certaines puces de passeports
Marc Witteman
- **Août 06** : « Clonage »
Clonage des informations publiques bit à bit hardware
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

Les faiblesses des puces

- Obtention des clés privées :
 - Attaque par “Differential Power Analysis” pour obtenir la clé privée du passeport contenue dans la puce
 - Dépend essentiellement du composant choisi par le pays
- « Dump » des informations publiques :
 - Copie bit à bit des informations « publiques » du composant d'un passeport allemand
- Solutions :
 - Rendre obligatoire l'AA pour détecter les clones
 - Utiliser des composants électroniques qualifiés de qualité !
 - Responsabilité des fondeurs et des autorités nationales



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

<http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.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
 - Prédicibilité 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 comme maillon faible de la chaîne

- 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/>
https://www.os3.nl/2008-2009/epassport_eng

Démo !

