

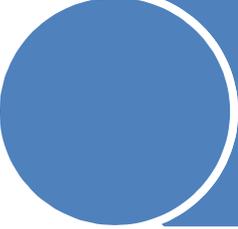
Programme TRIP de l'OACI
Séminaire régional Cotonou
Bénin 12/14 février 2019

Contrôle des e-MRTD aux
postes frontières

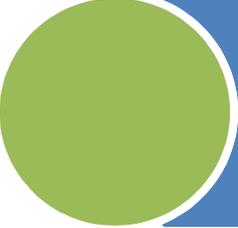
Expérience du Royaume du Maroc



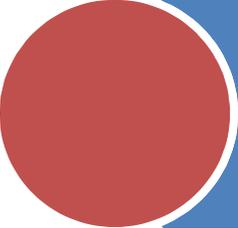
Sommaire



**Principes fondamentaux de
cryptographie appliqués aux eMRTD**



Chaîne de confiance (infrastructures PKI)

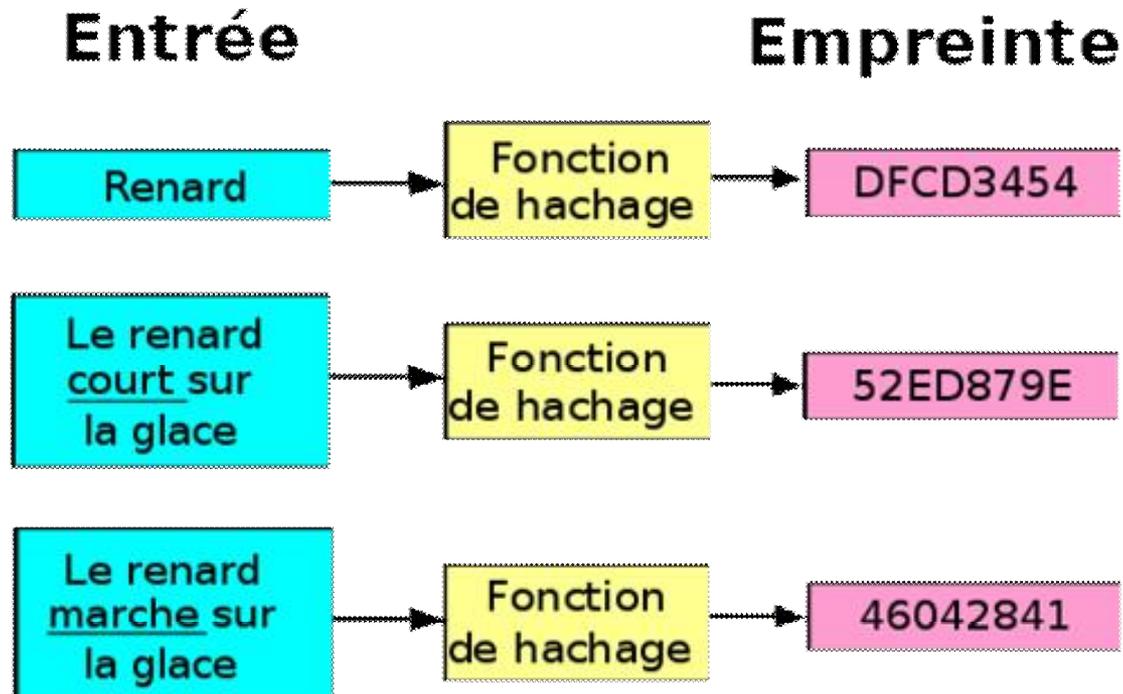


**Système de contrôle des passeports
au Royaume du Maroc**



Fonction de hachage

- Une **fonction de hachage** est une fonction mathématique à **sens unique** qui associe un code de **taille fixe** à un message de **taille variable**.



(Valeur de hachage ou empreinte numérique/
Message digest, Digest, Hash)



Fonction de hachage

3 propriétés importantes :

- On ne peut pas reconstruire le message à partir de son empreinte numérique ;
- Il est impossible de modifier un message sans changer son empreinte numérique ;
- 2 messages différents ne peuvent pas avoir la même empreinte numérique.

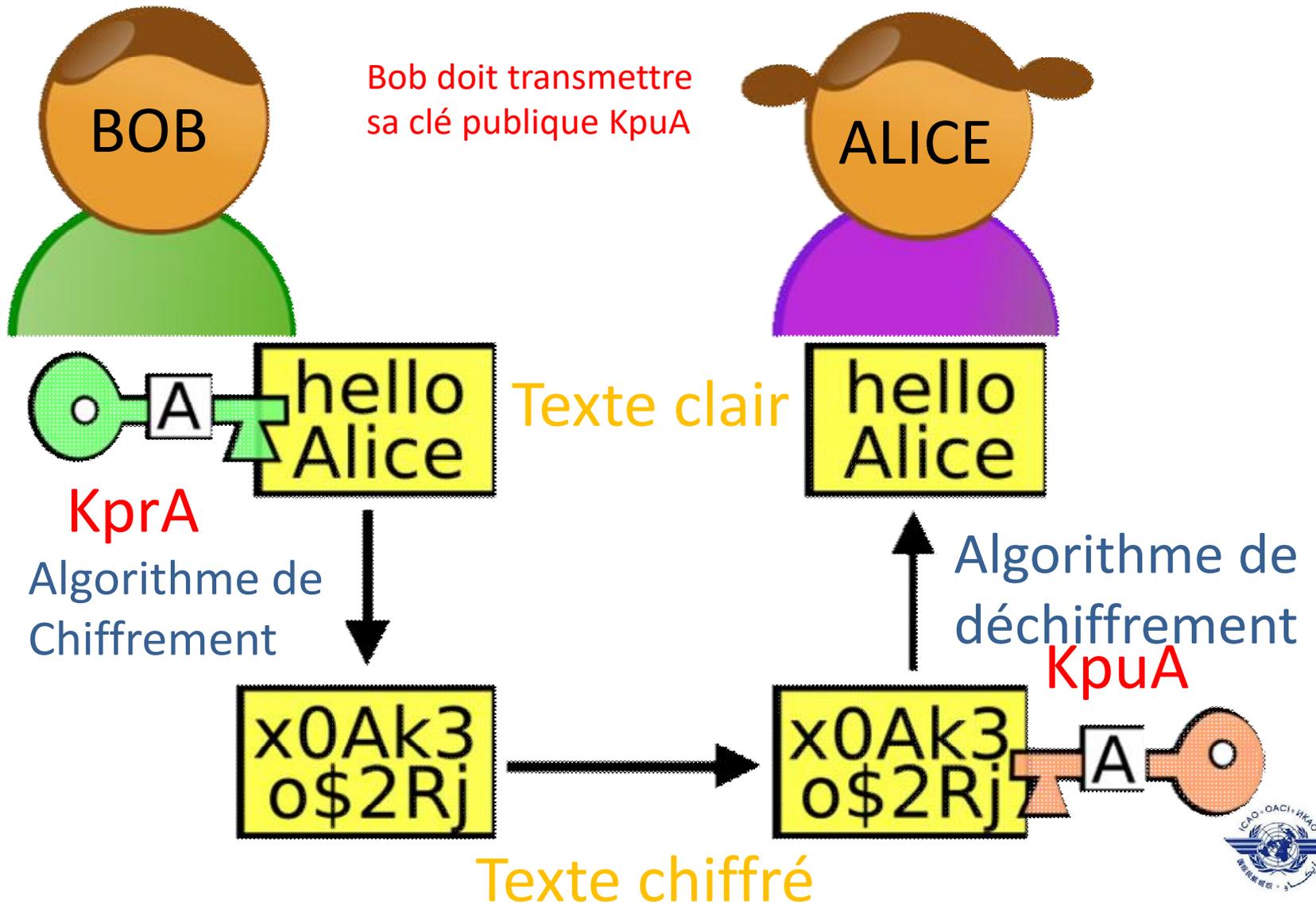


Cryptographie asymétrique

- ❑ Utilise une paire de clés mathématiquement liées:
 - Kpr (clé privée secrète)
 - Kpu (clé publique diffusée)
- ❑ Propriétés :
 - Un message chiffré par la clé privée Kpr sera lisible par tous ceux qui possèdent la clé publique Kpu qui lui correspond et vice-versa,
 - Il est impossible de déduire la clé privée Kpr à partir du message chiffré ou de la clé publique Kpu.



Cryptographie asymétrique

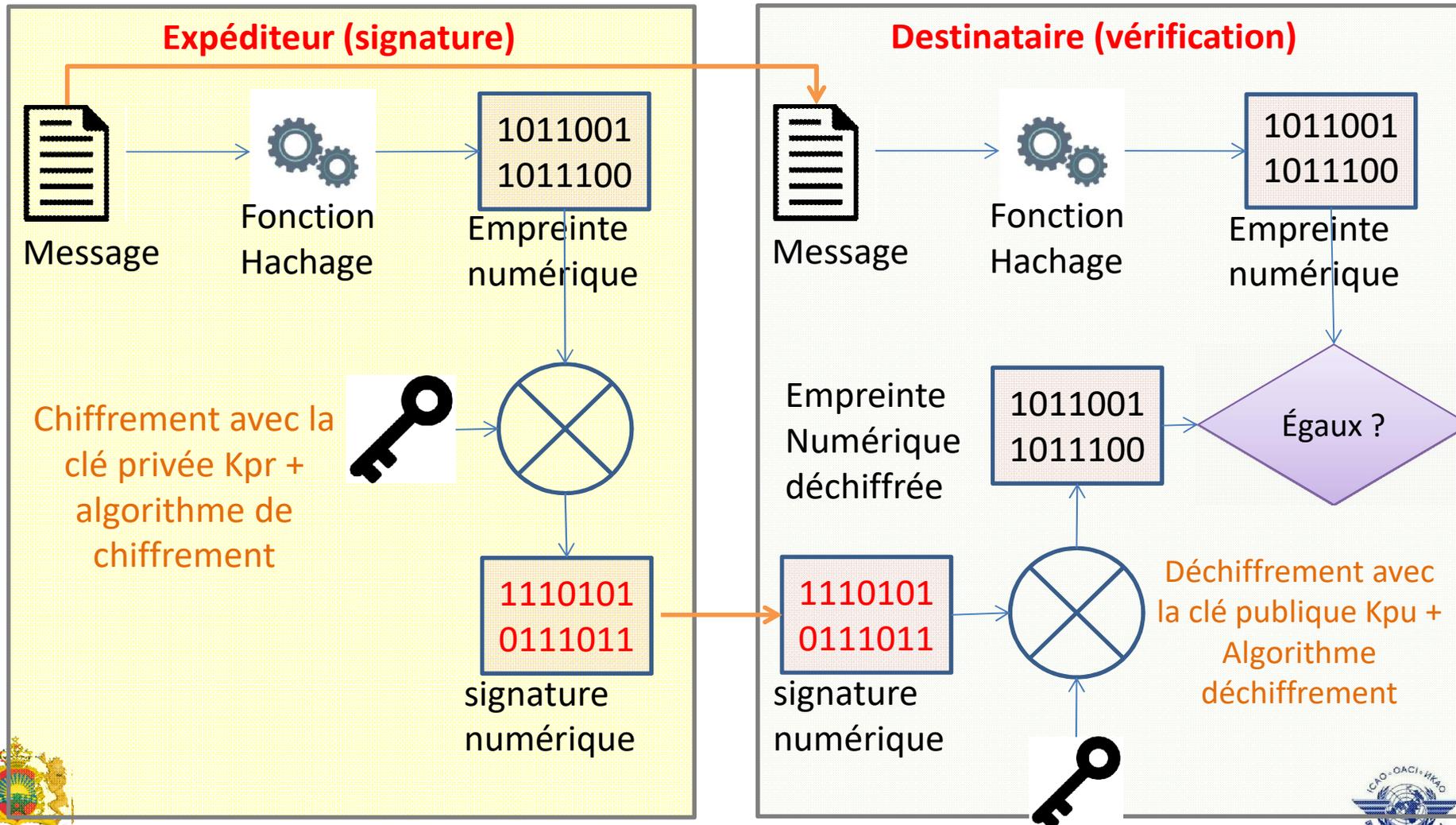


Signature numérique

- La **signature numérique** est un mécanisme cryptographique permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur.



Signature numérique



Signature et certificats numériques

- Problème = Comment savoir si la clé publique Kpu est bien celle du signataire? Comment la transmettre par un canal sécurisé?
- Les certificats numériques résolvent cette question.
- Un certificat électronique peut être vu comme une carte d'identité numérique. Il est utilisé pour identifier et authentifier une entité, mais aussi pour chiffrer des échanges.



Qu'est ce qu'un certificat?

- ❑ Un fichier qui contient des données utilisées pour la sécurité et l'identification

Nom ^	Modifié le	Type	Taille
 CSCA_MAROC_2015	18/10/2018 14:32	Certificat de sécurité	2 Ko
 CSCA-MAROC_2009	17/10/2018 14:28		
 CSCA-MAROC_2012	17/10/2018 14:28		
 CSCA-MAROC-2018	17/10/2018 14:29		



Certificat

Général | Détails | Chemin d'accès de certification

Afficher : <Tout>

Champ	Valeur
Version	V3
Numéro de série	11 21 09 1b 56 5c e3 22 75 e6...
Algorithme de signature	sha256RSA
Algorithme de hachage de l...	sha256
Émetteur	CSCA-MAROC, Gov, MA
Valide à partir du	jeudi 22 février 2018 00:00:00
Valide jusqu'au	mercredi 22 avril 2026 00:00:00
Objet	CSCA-MAROC, Gov, MA

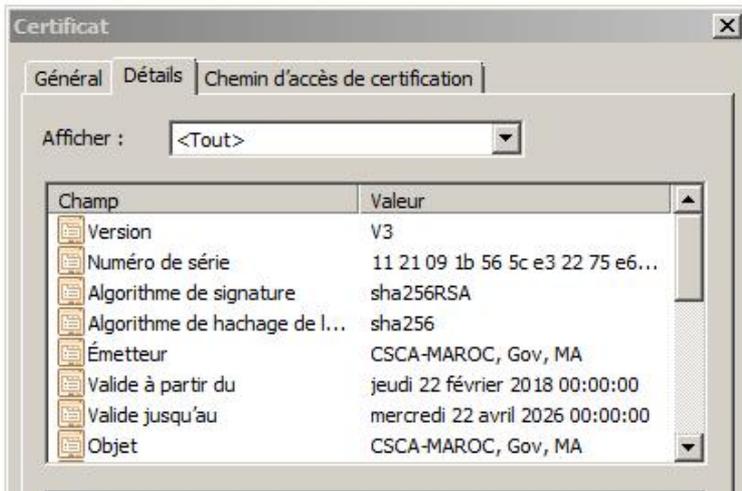
Valide du 22/ 02/ 2018 **au** 22/ 04/ 2026

Installer le certificat... Déclaration de l'émetteur



Qu'est ce qu'un certificat?

□ Similaire à un certificat traditionnel



Champ	Valeur
Version	V3
Numéro de série	11 21 09 1b 56 5c e3 22 75 e6...
Algorithme de signature	sha256RSA
Algorithme de hachage de l...	sha256
Émetteur	CSCA-MAROC, Gov, MA
Valide à partir du	jeudi 22 février 2018 00:00:00
Valide jusqu'au	mercredi 22 avril 2026 00:00:00
Objet	CSCA-MAROC, Gov, MA



ONSSA COPIE

OFFICE NATIONAL DE SÉCURITÉ SANITAIRE DES PRODUITS ALIMENTAIRES
DIRECTION REGIONALE DE MARRAKECH TENSIFT AL HAOUZ ET TAOLA AZILAL
Service vétérinaire préfectoral de MARRAKECH

المكتب الوطني للتجارة الصحية للمنتجات الغذائية
المديرية الجهوية لمراكش تانسيفت الحوز و تادلة أزلال
المصلحة البيطرية الإقليمية بمرآكش

الاعتماد على المستوى الصحي للمؤسسات و المقاولات في القطاع الغذائي
باستثناء منتجات الصيد البحري و تربية الأحياء المائية بالمياه البحرية
Agrément sur le plan sanitaire des établissements et entreprises du secteur alimentaire
hors produits de pêche maritime et de l'aquaculture marine
Article 5 de la loi n° 28-07 رقم القانون رقم 5 س 04

Suite à la visite sanitaire du:	07/07/2014	تبعاً للزيارة الصحية بتاريخ :
L'établissement / l'entreprise :	صالبرو SALIPRO	المؤسسة / المقاولات :
Sis(e) à :	Km 15,5 route d'Ouarzazate , vers chouiter	الكاتبة بـ : كلم 5,15 طريق وارزات نحو الشويطر , مراكش
Est agréé sur le plan sanitaire pour l'exercice de(s) activité(s) :	Entreposage des produits animaux et d'origine animale à des températures positives et négatives	ترخص على المستوى الصحي فزاوله النشاط أو الأنشطة المتعلقة (ة) بـ : تخزين المنتجات الحيوانية أو من أصل حيواني ضمن درجات حرارة سلبية و ايجابية
Sous le numéro :	EF.19.25.14	تحت رقم :

Marrakech le, 15/10/2014 مراكش في، 15/10/2014

Cachet officiel et signature : الطابع الرسمي و الإمضاء :

□ Il est délivré à un bénéficiaire par une autorité de confiance qui signe le certificat.



Qu'est ce qu'un certificat?

- ❑ Un certificat numérique contient des informations :
 - L'identité du bénéficiaire
 - L'identité de l'autorité de certification
 - La période de validité du certificat
 - La clé publique et les informations sur les algorithmes cryptographiques utilisés
 - L'empreinte numérique signée par l'autorité qui prouve que le certificat vient d'une source sûre et n'a pas été altéré...etc



Application aux eMRTD

- ❑ Certaines informations du passeport sont enregistrées dans la CI dans un format normalisé (structure de données logique ou SDL)
- ❑ Le Doc 9303-partie 10 décrit les informations obligatoires et optionnelles à inclure dans les 16 blocs de données de la SDL (Datagroups ou DG)



		ÉLÉMENTS DE DONNÉES			
OBLIGATOIRE	DONNÉES D'ÉTAT ÉMETTEUR OU D'ORGANISATION ÉMETTRICE	Détail(s) enregistré(s) dans la ZLA	DG1	Type de document	
				État émetteur ou organisation émettrice	
				Nom (du titulaire)	
				Numéro de document	
				Chiffre de contrôle - Numéro de document	
				Nationalité	
				Date de naissance	
				Chiffre de contrôle - Date de naissance	
				Sexe	
				Date d'expiration ou valide jusqu'au	
				Chiffre de contrôle - Date d'expir./valide jusqu'au	
				Données optionnelles	
				Chiffre de contrôle - Champ de données option.	
				Chiffre de contrôle composite	
OPTIONNEL	DONNÉES D'ÉTAT ÉMETTEUR OU D'ORGANISATION ÉMETTRICE	Élément(s) d'identification codé(s)	Élément pour échanges mondiaux	DG2	Visage codé
			Élément(s) supplémentaire(s)	DG3	Doigt(s) codé(s)
				DG4	Œil (yeux) codé(s)
	DONNÉES D'ÉTAT ÉMETTEUR OU D'ORGANISATION ÉMETTRICE	Élément(s) d'identification affiché(s)	DG5	Portrait affiché	
			DG6	Réserve pour usage futur	
			DG7	Signature ou marque habituelle affichée	
	DONNÉES D'ÉTAT ÉMETTEUR OU D'ORGANISATION ÉMETTRICE	Élément(s) de sécurité codé(s)	DG8	Élément(s) de données	
			DG9	Élément(s) de structure	
			DG10	Élément(s) de substance	
		DG11	Détail(s) personnel(s) supplémentaire(s)		
		DG12	Détail(s) supplémentaire(s) sur le document		
		DG13	Détail(s) optionnel(s)		
DG14		Options de sécurité			
DG15		Info de clé publique d'authentification active			
DG16		Personne(s) à aviser			

Éléments minimaux à stocker dans la puce du MRTD:

- DG1 → Données de la MRZ
- DG2 → Image faciale du titulaire

+ **Objet de sécurité (SOD)** nécessaire pour valider l'authenticité et l'intégrité des données de l'émetteur



Application aux eMRTD - SOD

- ❑ Un hachage de chaque DataGroup utilisé est stocké dans l'objet de sécurité du document (SOD) qui est **signé numériquement** par le signataire du document DS.
- ❑ Le système d'inspection utilise **le certificat du signataire de document CDS** pour vérifier que le contenu du SOD et de la SDL est authentique et n'a pas été modifié (authentification passive).



Comment établir la chaîne de confiance des certificats?

- L'autorité doit être digne de confiance (ONSSA au Maroc = sécurité alimentaire)
- Comment établir cette confiance?
- Les certificats numériques se basent sur une chaîne de confiance → **infrastructures à clés publiques (PKI)**



Infrastructures à clés publiques (PKI)

- ❑ L'infrastructure à clés publiques (PKI) permet de créer les paires de clés (privé/public) et de vérifier les signatures numériques des eMRTD
- ❑ La PKI comprend différentes entités ayant différents rôles parmi lesquelles:
 - L'autorité de certification signataire nationale (CSCA)
 - Le signataire de document (DS).
 - Le Système d'inspection (IS).



L'autorité de certification signataire nationale 1/2

- ❑ Chaque Etat établit une **ACSN/CSCA** comme **unique** point de **confiance nationale**.
- ❑ L' **ACSN/CSCA** génère et stocke ses paires de clés (KpuCSCA, KprCSCA) dans une infrastructure informatique **hors ligne protégée**.
- ❑ Elle génère aussi les paires de clés (KpuDS, KprDS) pour le signataire de document (imprimerie).



L'autorité de certification signataire nationale 2/2

- ❑ Elle émet aussi des listes de révocation de certificats (CRL) pour les certificats révoqués qui ne peuvent plus être utilisés.
- ❑ La clé privée KPrCSCA est utilisée pour **signer les certificats de signataire de document** (C_{DS}) ainsi que d'autres certificats (MasterLists, CRL).
- ❑ Les certificats d'ACSN (C_{CSCA}) sont utilisés pour valider les certificats de signataires de document (C_{DS}) et d'autres certificats (MasterLists, CRL)



PKI - Le Signataire de document (DS).

- ❑ Le signataire de document (DS) signe les données de l'eMRTD avec sa clé privée KprDS (signature stockée dans le SOD).
- ❑ Le certificat de signataire de document C_{DS} (contient la clé publique KpuDS qui est authentifié par la signature de l'autorité de confiance nationale CSCA) permet au système d'inspection de contrôler les eMRTD.
- ❑ Pour permettre aux Etat récepteurs de faire ce contrôle, les certificats de signataire de document (C_{DS}) DOIVENT être stockés dans chaque eMRTD (+ autres moyens)



PKI - Système d'inspection

- Système d'inspection** vérifie la **signature numérique**, valide la **chaîne de certification** pour vérifier l'authenticité et l'intégrité des données électroniques stockées dans le eMRTD (**authentification passive**).
- Le système d'inspection effectue les opérations suivantes:



PKI - Système d'inspection

1. Il lit l'objet de sécurité du document (SOD).
2. Il construit et valide la chaîne de certification depuis une ancre de confiance (C_{CSCA}) jusqu'au certificat de signataire de document C_{DS}.
3. Il vérifie que le certificat C_{DS} n'a pas été révoqué (CRL).
4. Il utilise la clé publique du signataire de document (K_{PuDS}) pour vérifier la signature du SOD.
5. il s'assure que le contenu des DataGroups de la LDS est intègre et authentique (hach du contenu est comparé avec hach de l'objet SOD).



Gestion des clés - Durée de validité

Les paires de clés CSCA et DS doivent être renouvelées régulièrement pour minimiser les risques de compromission

Durée utilisation
KprCSCA 5 Ans
(signe CDS)

Durée utilisation
KprDS (signe
passeport)
3 mois / 100 000

Durée validité
passeport
(5 ans)

Durée de validité certificat CSCA 10 ans + 3 mois

Durée de validité certificat CDS 5 ans + 3 mois



Gestion des clés - Distribution

Les certificats C_{CSCA} et C_{DS} doivent être distribués en temps utile aux Etats tiers pour leur permettre de contrôler les eMRTD par différents moyens:

- Voie diplomatique
- Échanges bilatéraux
- Répertoire de clés publiques de l'OACI
- Puce de l'eMRTD (C_{DS})
- MasterLists



Mécanismes de distribution des clés

RCP/PKD OACI

- ❑ L'OACI assure un service de répertoire de clés publiques (RCP ou PKD) qui met à disposition des utilisateurs les certificats CDS, les CRL et les listes de contrôle enregistrés dans le PKD par les participants au PKD.
- ❑ Le RCP/PKD permet aux Etats participants de publier leur certificats (CDS, CRL, Masterlist) et de télécharger ceux des autres Etats.
- ❑ Chaque certificat de signataire de document (CDS) reste dans le PKD jusqu'à l'expiration de sa validité.



Mécanismes de distribution des clés

doc 9303 – partie 12

- ❑ Les certificats et les CRL doivent être distribués dans les systèmes de contrôle frontalier (48 heures)
- ❑ Les États émetteurs s'assurent que les certificats de signataire de document (CDS) sont distribués en les enregistrant dans l'objet de sécurité du document (SOD).
- ❑ Les États récepteurs devraient tout mettre en œuvre, par voie électronique ou autrement, pour donner suite aux CRL, notamment les CRL émises dans des circonstances exceptionnelles.



Mécanismes de distribution des clés

doc 9303 – partie 12

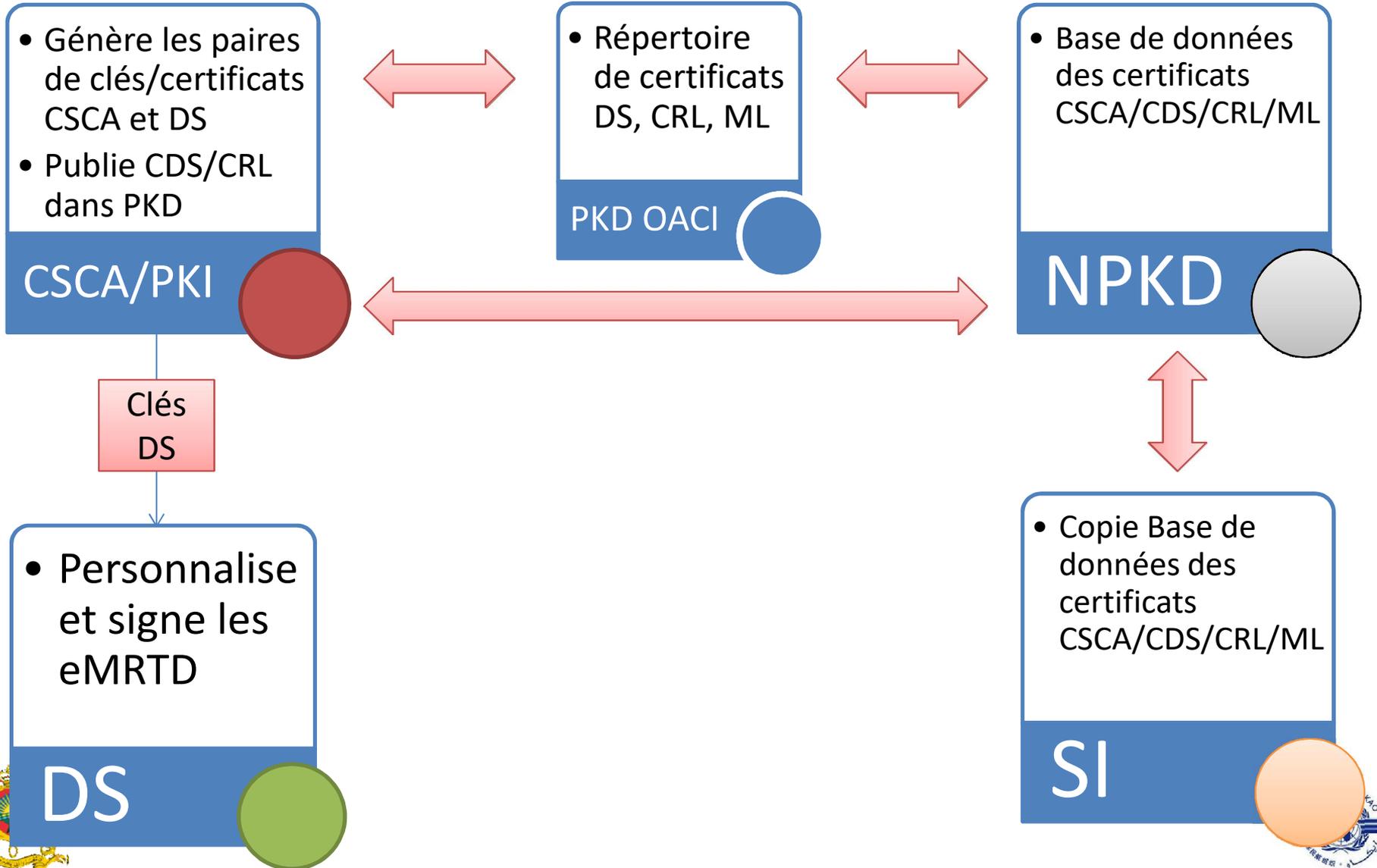
Les États émetteurs doivent distribuer aux États récepteurs les objets PKI suivants

Tableau 2. Distribution principale et secondaire

	<i>Certificats d'ACSN</i>	<i>Certificats de signataire de document</i>	<i>CRL (vides et non vides)</i>	<i>Certificats de signataire de liste de contrôle</i>	<i>Listes de contrôle</i>	<i>Certificats de signataire de liste d'écarts</i>
Principale	Bilatérale	CI sans contact de DVLM-e	Bilatérale	Listes de contrôle	RCP/ bilatérale	Listes d'écarts
Secondaire	Listes de contrôle	RCP	RCP			



En résumé



Systeme de Gestion des Postes frontières au MAROC

Le Systeme de Gestion des Postes Frontières « SGPF » permet de:

- Normaliser et unifier les procédures de travail et les mesures de contrôle et de sécurité
- Fluidifier le passage des voyageurs
- Renforcer l'efficacité des mesures de contrôle et de sécurité.
- Lutter efficacement contre le terrorisme, l'immigration clandestine et le crime organisé et réduire considérablement la mobilité des suspects.



Architecture PKI (Public Key Infrastructure)

Ministère de l'Intérieur

Vérification du passeport

Signature du passeport

CVCA
Country Verification Certification
Authority

CSCA
Country Signing Certification
Authority

DVCA
Document Verification Certification
Authority

DSCA
Document Signing Certification
Authority

DAR-ASSIKAH

**Direction Générale de
la Sureté Nationale**

Système de dispatching des
certificats « Inspection System »

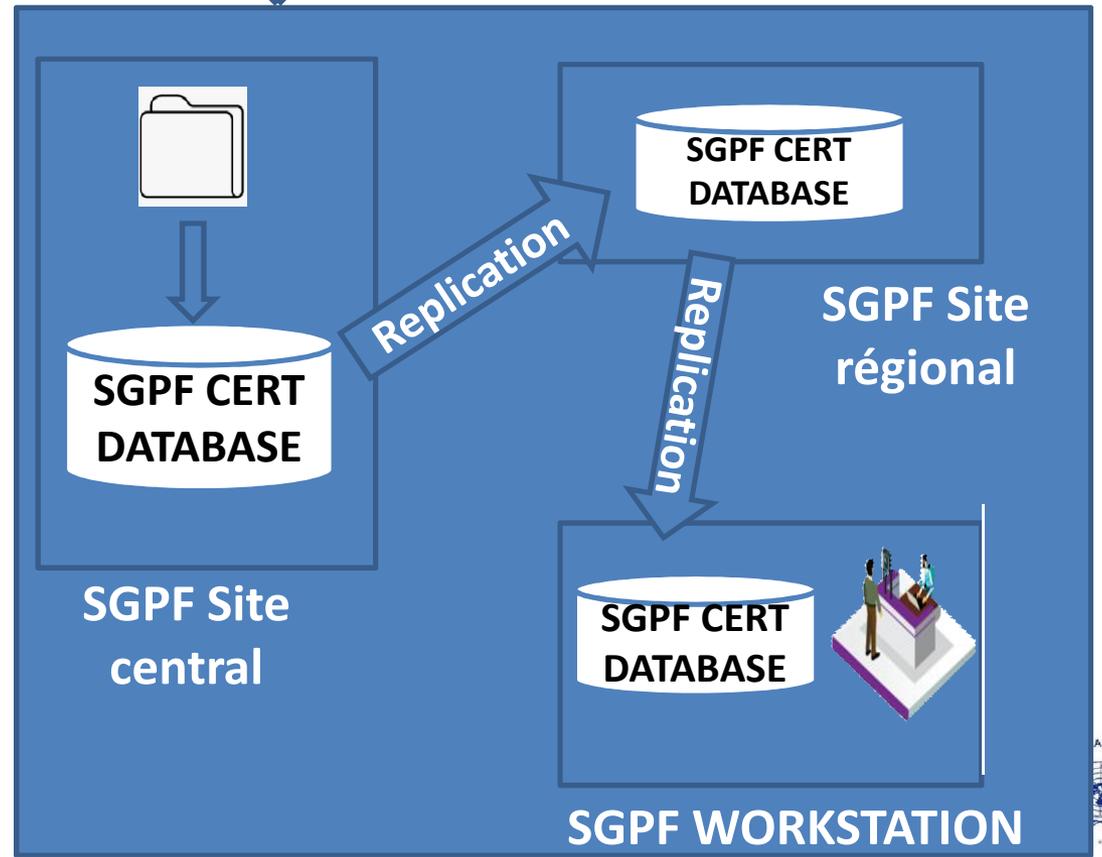
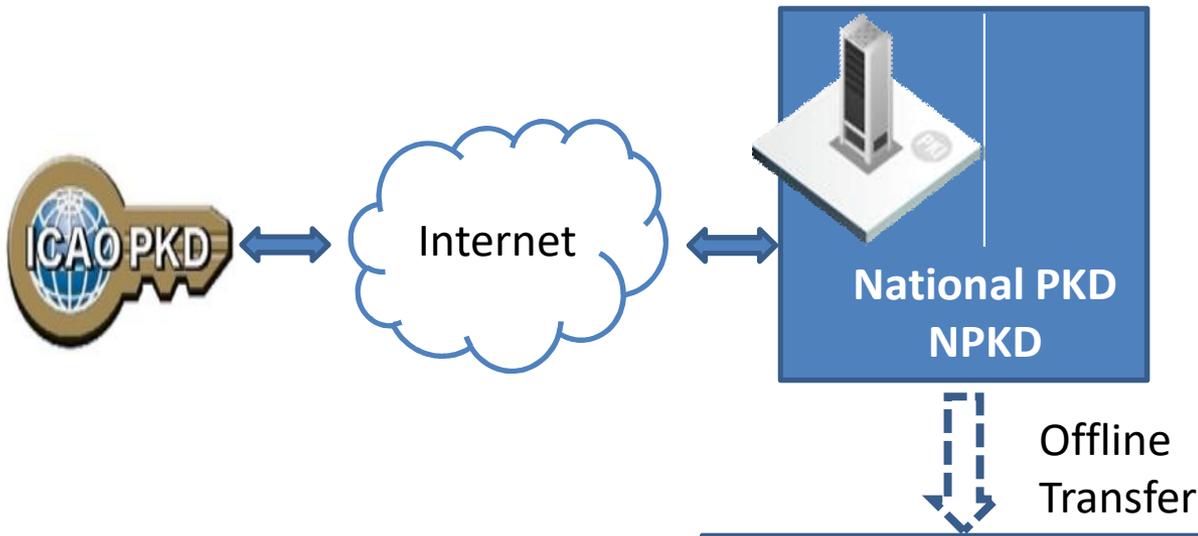


Interfaçage entre SGPF et PKD/OACI

Le système permet deux options possibles :

- ❖ Manuelle : Les certificats reçus via la voie diplomatique sont exportés manuellement et chargés dans le SGPF pour distribution vers toutes les stations de contrôle au niveau des postes frontières.
- ❖ Automatique (en cours) : Connection Internet directe avec le PKD pour récupérer les certificats publiés par les pays membres actifs de l'OACI et les distribuer automatiquement vers tous les postes frontières.





Comment le Maroc contrôle-t-il les passeports au niveau de ses Postes Frontières?

- ❑ Spécimen du passeport : une base de Template mise à jour chaque deux mois
- ❑ **Mécanismes de sécurité de la puce:**
 - **Basic Access Control (BAC)** : Lit la MRZ pour négocier une clé de session afin de chiffrer la communication entre la puce du passeport et l'appareil de lecture.
 - **Passive Authentication (PA)**: Ce protocole permet de vérifier que les données de la puce du passeport sont authentiques (vérification de la signature du SOD).



Comment le Maroc contrôle-t-il les passeports au niveau de ses Postes Frontières?

- **Active Authentication (AA):** Protocole d'authentification dont l'objectif est de permettre au lecteur de contrôler que la puce n'a pas été clonée.
- **Extended Access Control (EAC):** Ce contrôle d'accès ajoute des fonctionnalités pour vérifier l'authenticité de la puce (authentification de la puce) et du lecteur (authentification du terminal). EAC est utilisé pour protéger les empreintes digitales.



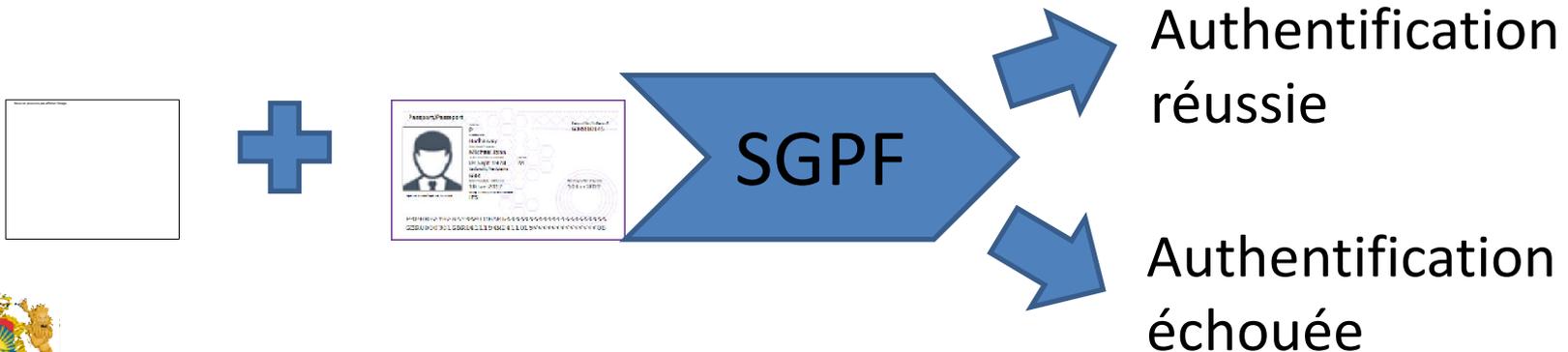
Comment le Maroc contrôle-t-il les passeports au niveau de ses Postes Frontières?

- **Supplemental Access Control (SAC/PACE)** Le protocole PACE (Password Authenticated Connection Establishment) est un mécanisme de contrôle d'accès à la puce qui permet d'établir une connexion sécurisée entre la puce et le système d'inspection avec authentification par mot de passe (calcul de clés de session).



Résultats des vérifications au niveau des Postes Frontières

les résultats devraient être interprétés par une application sur le système d'inspection et fournir une réponse simple à l'agent des services frontaliers.



Cas pratique

Overview White light Infrared UV MRZ Chip Barcode Second page Face images Status: **No irregularities**

Tests

- MRZ
- Expiry date
- Paper
- Pattern
- Chip
- MRZ - Chip
- Barcode

Overview

Check	Optical MRZ	MRZ chip
Given name	EL MEHDI	EL MEHDI
Surname	SAADI	SAADI
Nationality	MAR	MAR
Date of birth	23.07.82	23.07.82
Sex	M	M
Expiry date	13.02.22	13.02.22
Document number	GX0527873	GX0527873
Check digit doc. number	9	9
Check digit date of birth	0	0
Check digit expiry date	0	0
Authority		
Check digit MRZ	4	4
Type of document	P	P
Optional data	D436248	D436248
Check digit optional data	4	4
Issue date		
Issuer	MAR	MAR

Infrared image

UV image

Finger

Finger

Face

Face from chip



Cas pratique

Overview White light Infrared UV MRZ **Chip** Barcode Second page Face images Status: **No irregularities**

Summary

- Chip

Single results chip

- BAC
- PACE
- EAC
- Passive authentication
- Active authentication
- Chip authentication

Chip content

- DG1 - MRZ data
- DG2 - Face image
- DG3 - Fingerprint image
- DG4 - Iris image
- DG5 - Displayed portrait
- DG6 - Reserved
- DG7 - Signature image
- DG8 - Data feature
- DG9 - Structure feature
- DG10 - Substance feature
- DG11 - Personal details
- DG12 - Document details
- DG13 - Country-specific details
- DG14 - EAC data
- DG15 - AA data
- DG16 - Persons to notify

Datagroup 1

Given name	EL MEHDI
Surname	SAADI
Nationality	MAR
Date of birth	23.07.82
Sex	M
Expiry date	13.02.22
Document number	GX0527873
Issuer	MAR
Type of document	P
Optional data	D436248
Check digit doc. number	9
Check digit date of birth	0
Check digit expiry date	0
Check digit optional data	4
Check digit MRZ	4

Datagroup 2



Finger



Finger



Chip details

Message

 FAC 1 detected

Merci votre attention

Mehdi Saadi

Responsable formation et
assistance SGPF

Direction Générale de la
Sûreté Nationale

Ministère de l'Intérieur

Royaume du Maroc

Email: m.saadi@dgsn.gov.ma

Rachid Abdellaoui

Chef de la Division des
Passeports

Direction des Affaires
Générales

Ministère de l'Intérieur

Royaume du Maroc

Email: rabdellaoui@interieur.gov.ma

