Programme TRIP de l'OACI

Séminaire régional Cotonou

Bénin 12/14 février 2019

Contrôle des e-MRTD aux postes frontières

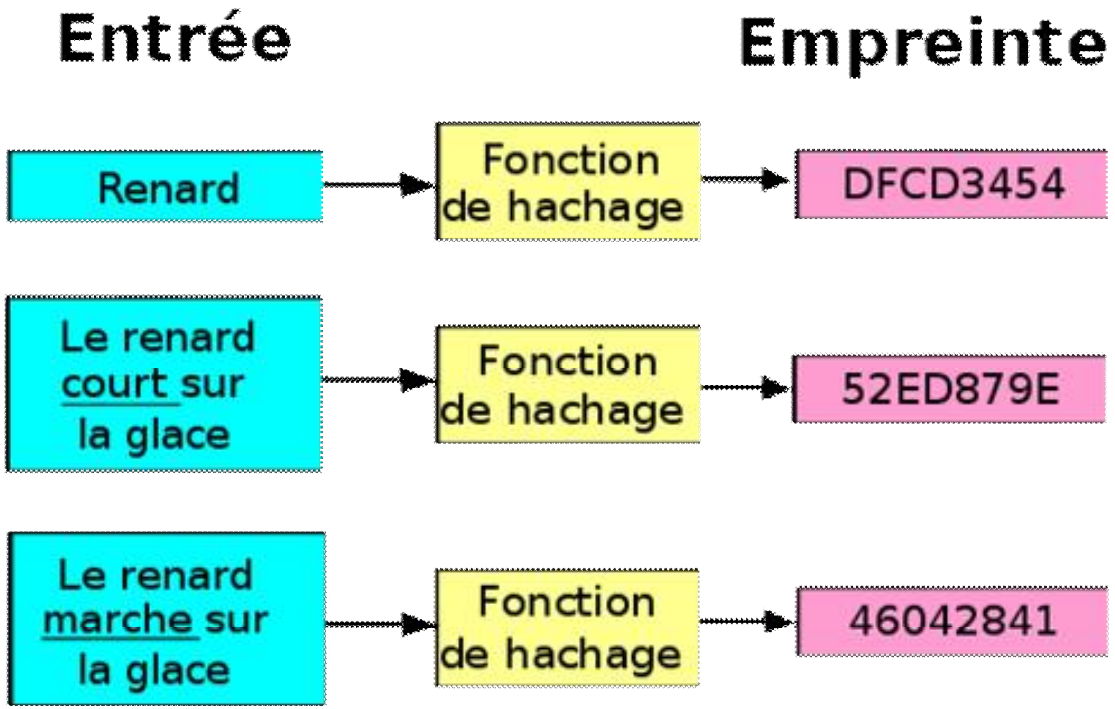
Expérience du Royaume du Maroc

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*

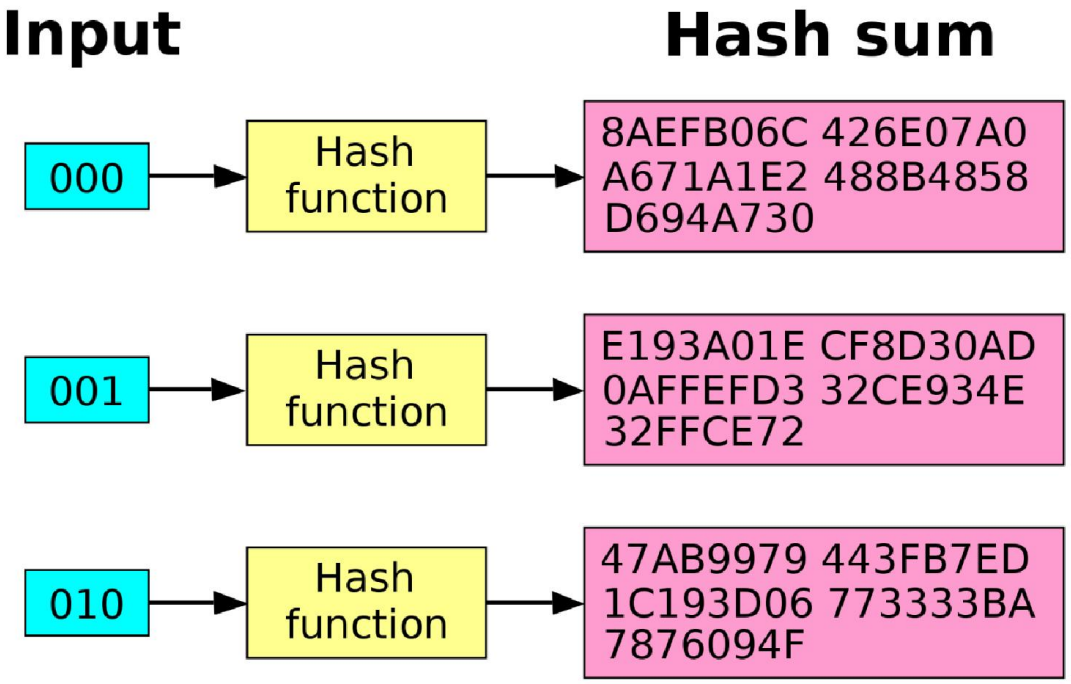
Fonction de hachage

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.

Fonction de hachage - Effet d'avalanche

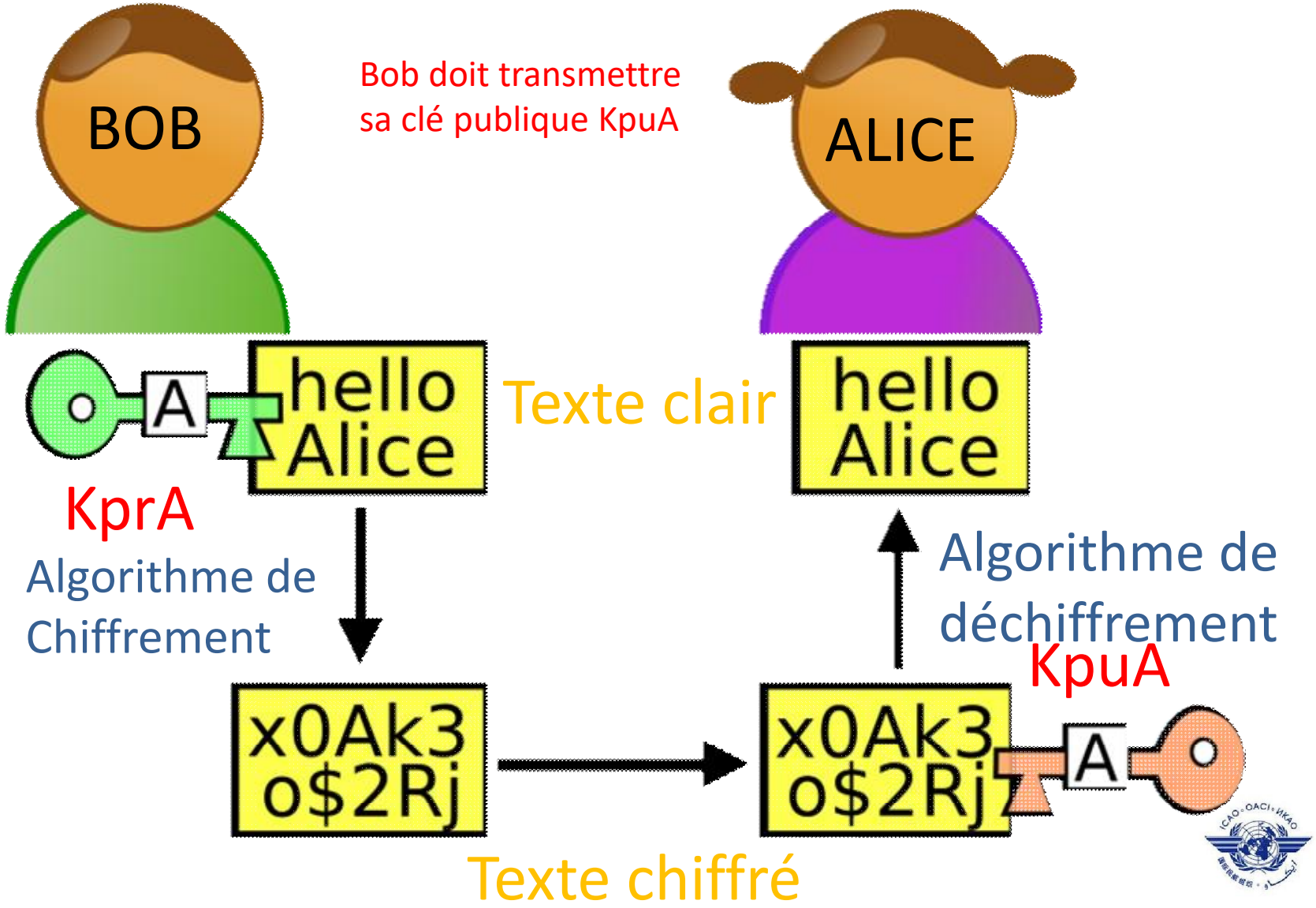
- Un changement mineur entraîne un résultat complétement différent;
- Garantit que le message original n'a pas été changé



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.

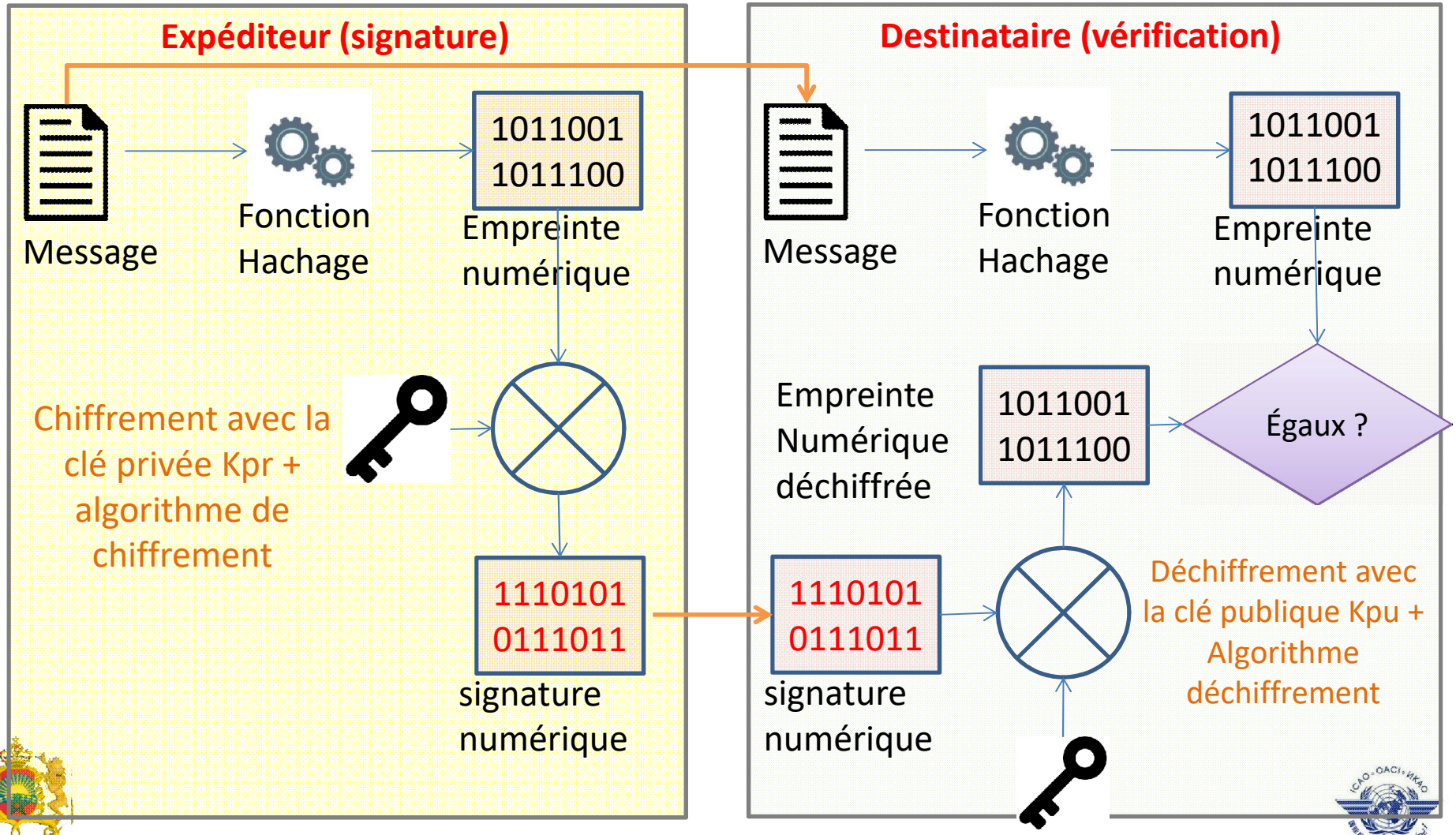
Cryptographie asymétrique



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

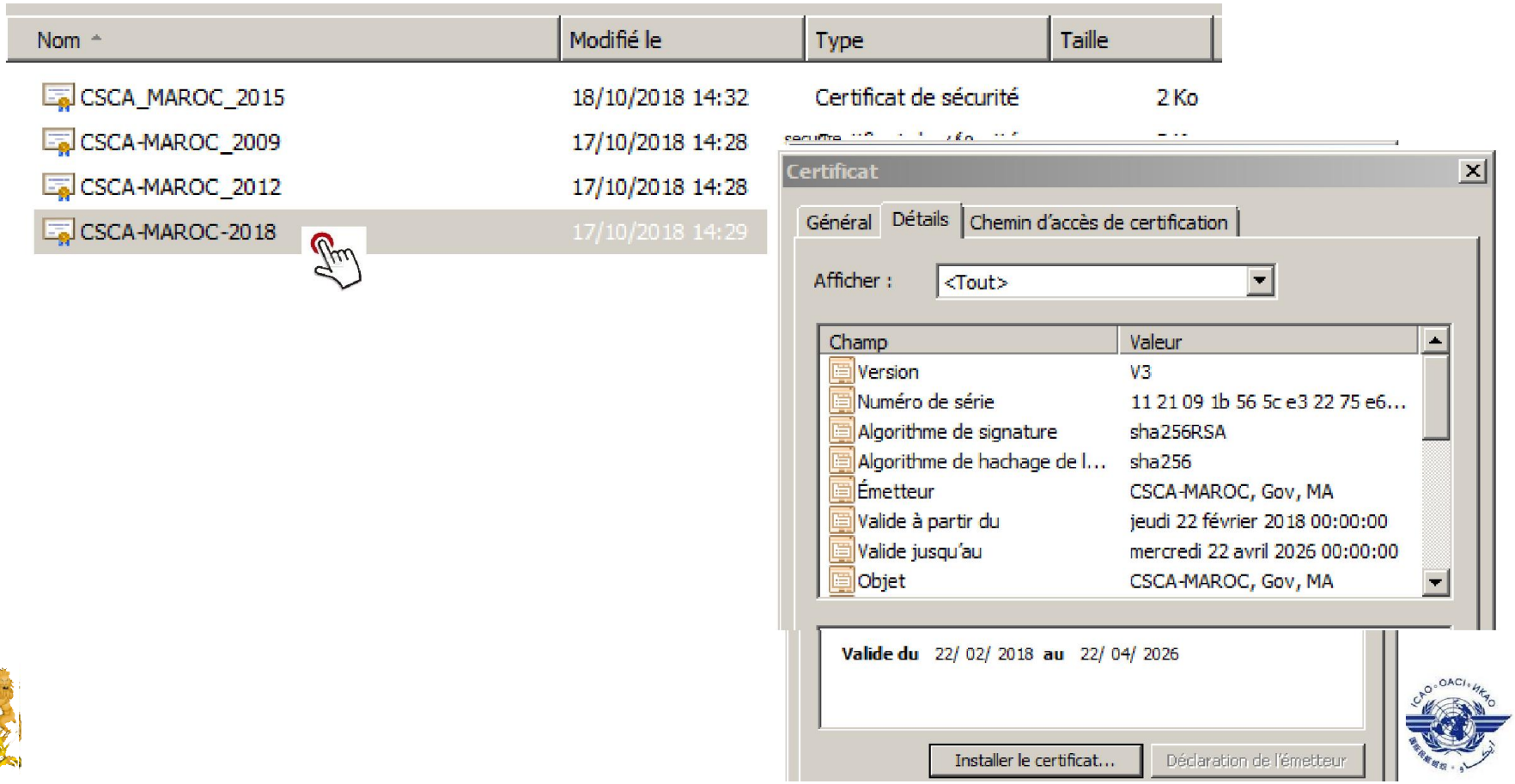


Signature et certificats numériques

- 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.

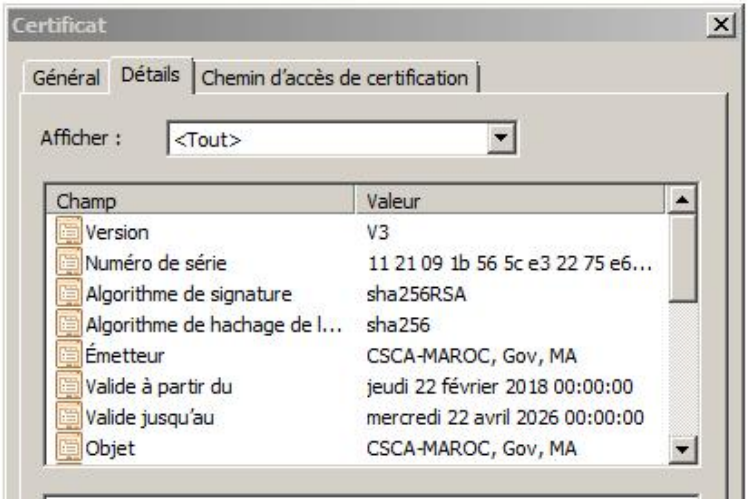
Qu’est ce qu’un certificat?

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



Qu’est ce qu’un certificat?

- Similaire à un certificat traditionnel



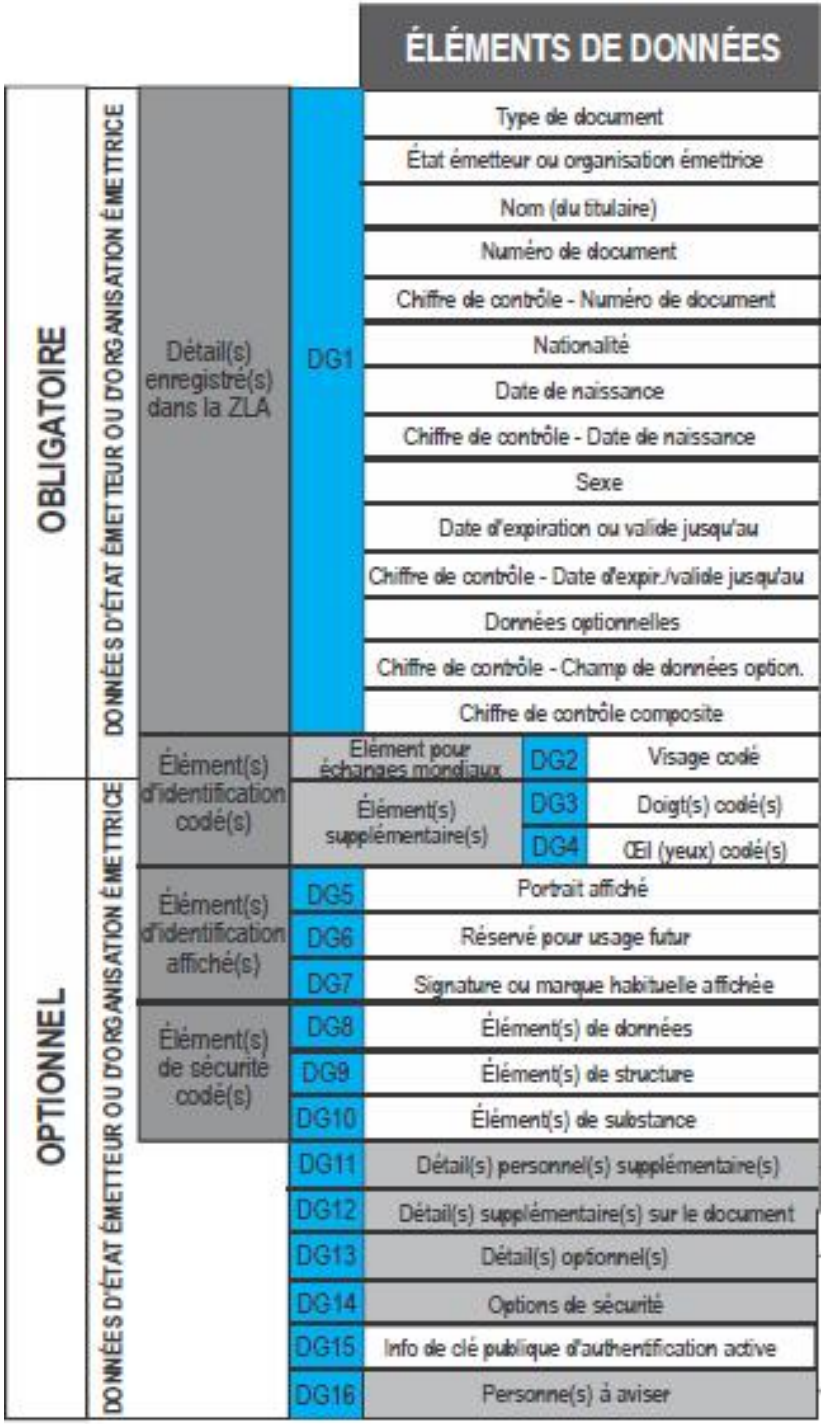
- Il est délivré à un bénéficiaire par une autorité de confiance qui signe le certificat.

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 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 chaine 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 chaine 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/publique) 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 national.
- 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

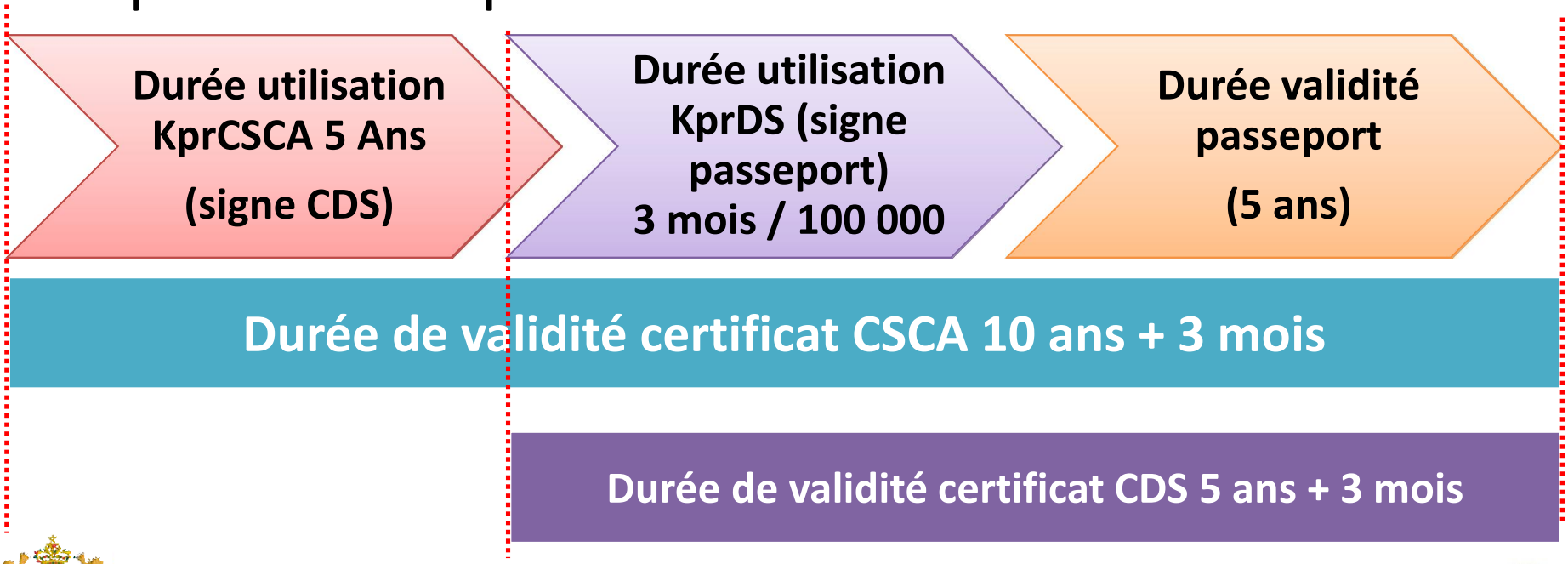
- **Système d'inspection** vérifie la signature numérique, valide la chaine de certification pour vérifier l'authenticité et l'intégrité des données électroniques stockées dans le eMRTD (authentification passive).
- Le système d'inspection effectue les opérations suivantes:

PKI - Système d'inspection

1. Il lit l'objet de sécurité du document (SOD).
2. Il construit et valide la chaine 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



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.

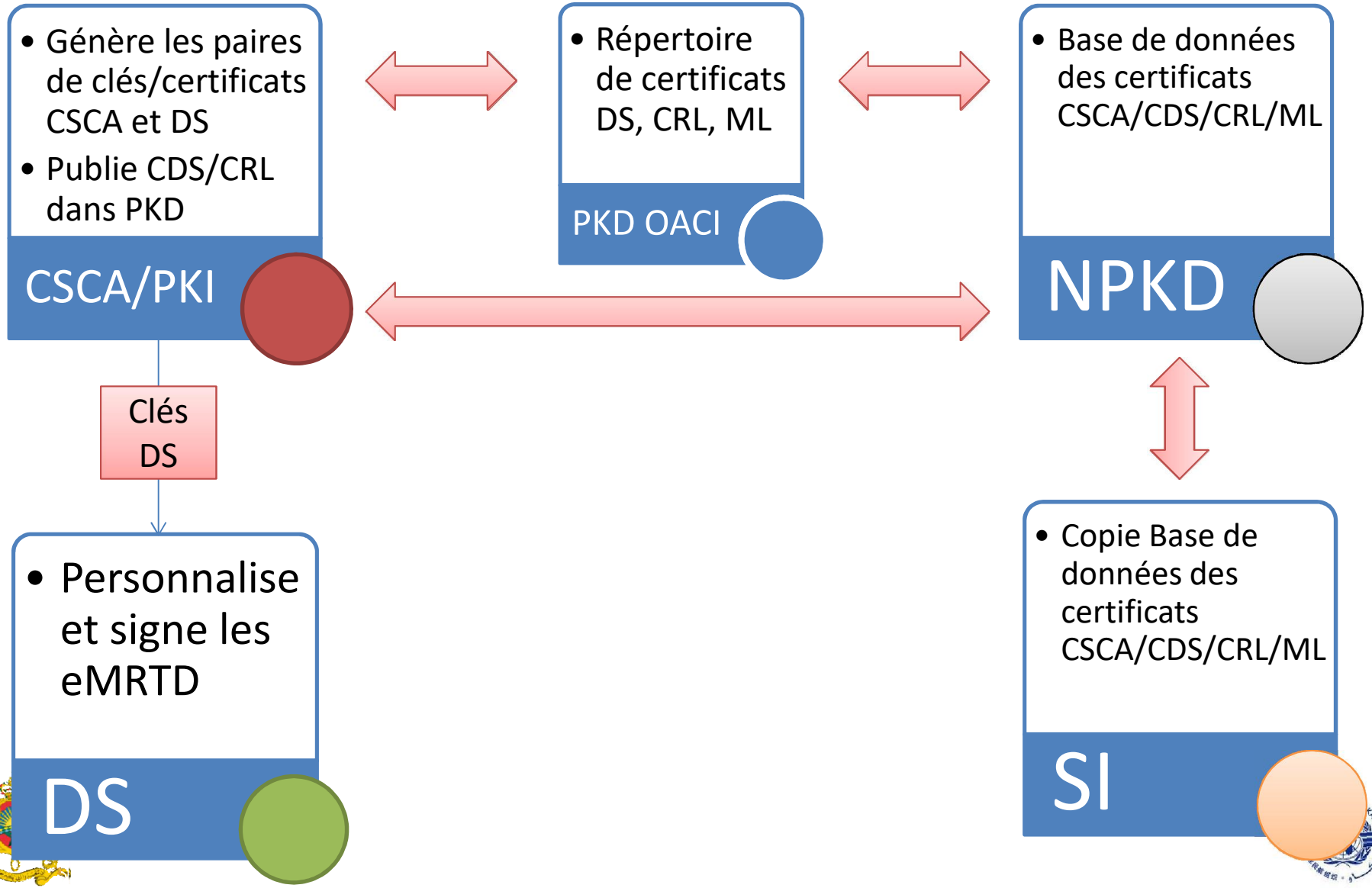
Mécanismes de distribution des clés doc 9303 – partie 12

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

Tableau 2. Distribution principale et secondaire

	Certificats d'ACSN	*Certificats de signataire de document*	*CRL (vides et non vides)*	*Certificats de signataire de liste de contrôle*	*Listes de contrôle*	*Certificats de signataire de liste d'écarts*
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


• Génère les paires de clés/certificats CSCA et DS
• Publie CDS/CRL dans PKD
CSCA/PKI
• Répertoire de certificats DS, CRL, ML
PKD OACI
• Base de données des certificats CSCA/CDS/CRL/ML
NPKD
Clés DS
• Personnalise et signe les eMRTD
DS
• Copie Base de données des certificats CSCA/CDS/CRL/ML
SI

Système de Gestion des Postes frontières au MAROC

Le Système 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

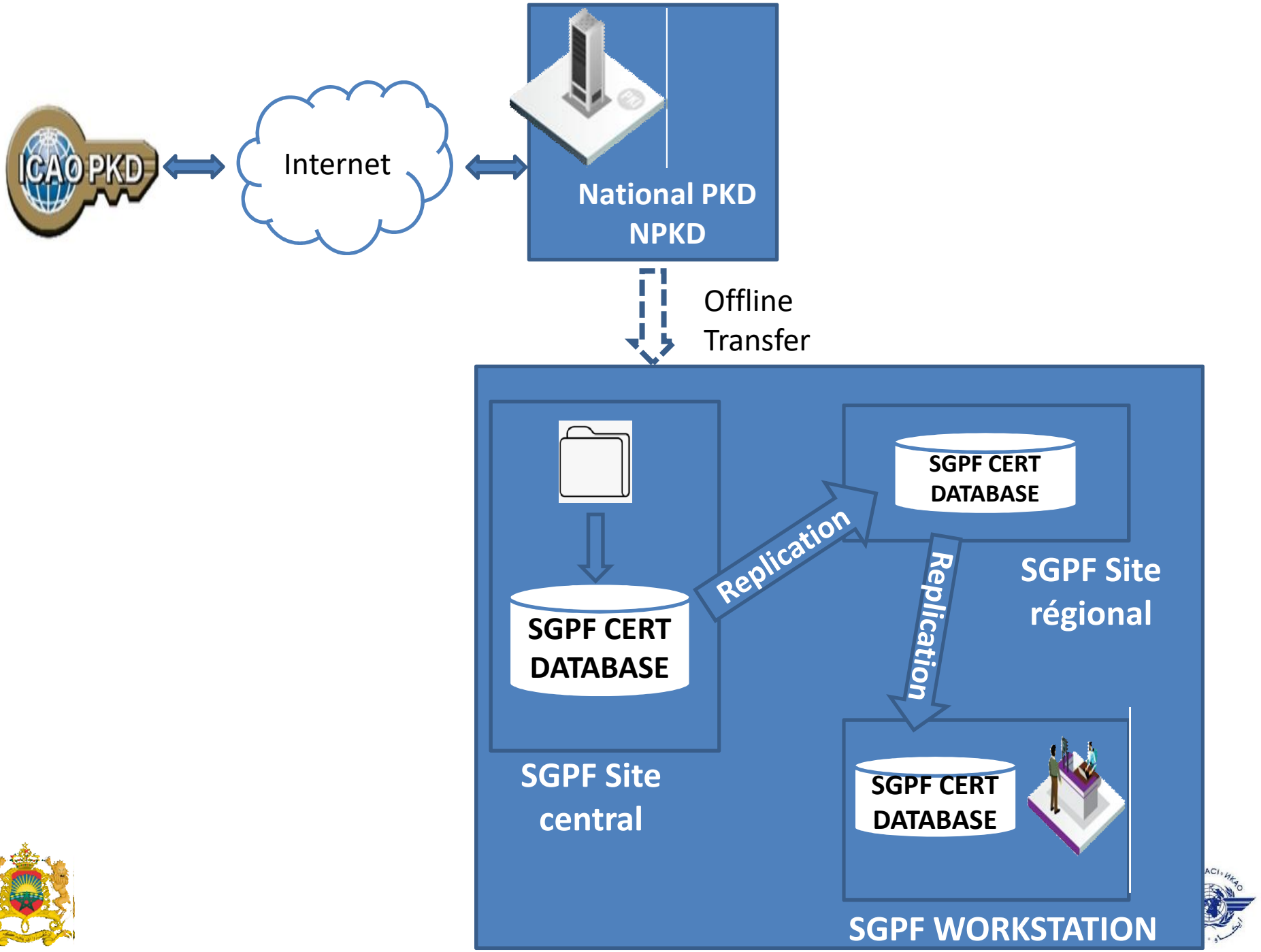
Système de dispatching des certificats « Inspection System »

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.


ICAO PKD
Internet
National PKD
NPKD
Offline
Transfer
SGPF CERT
DATABASE
Replication
SGPF Site
régional
Replication
SGPF CERT
DATABASE
SGPF Site
central
SGPF CERT
DATABASE
SGPF WORKSTATION

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?

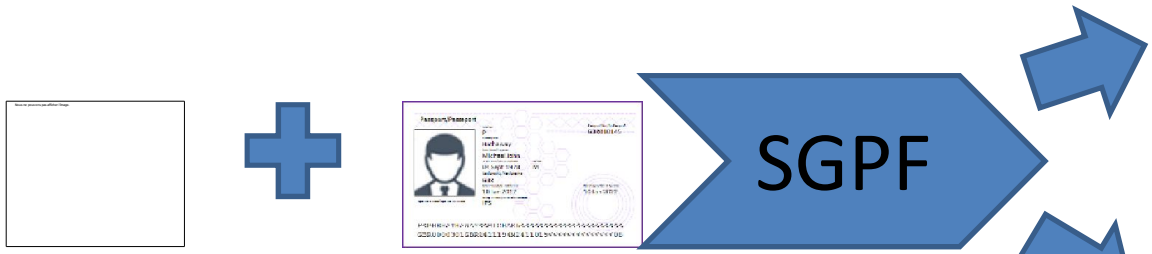
- **Active Authentication (AA):**Protocole d'authentification dont l'objectif est de permettre au lecteur de contrôler que la puce n'a pas été clonée.
- **Extended Access Control (EAC)**: Ce contrôle d'accès ajoute des fonctionnalités pour vérifier l'authenticité de la puce (authentification de la puce)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

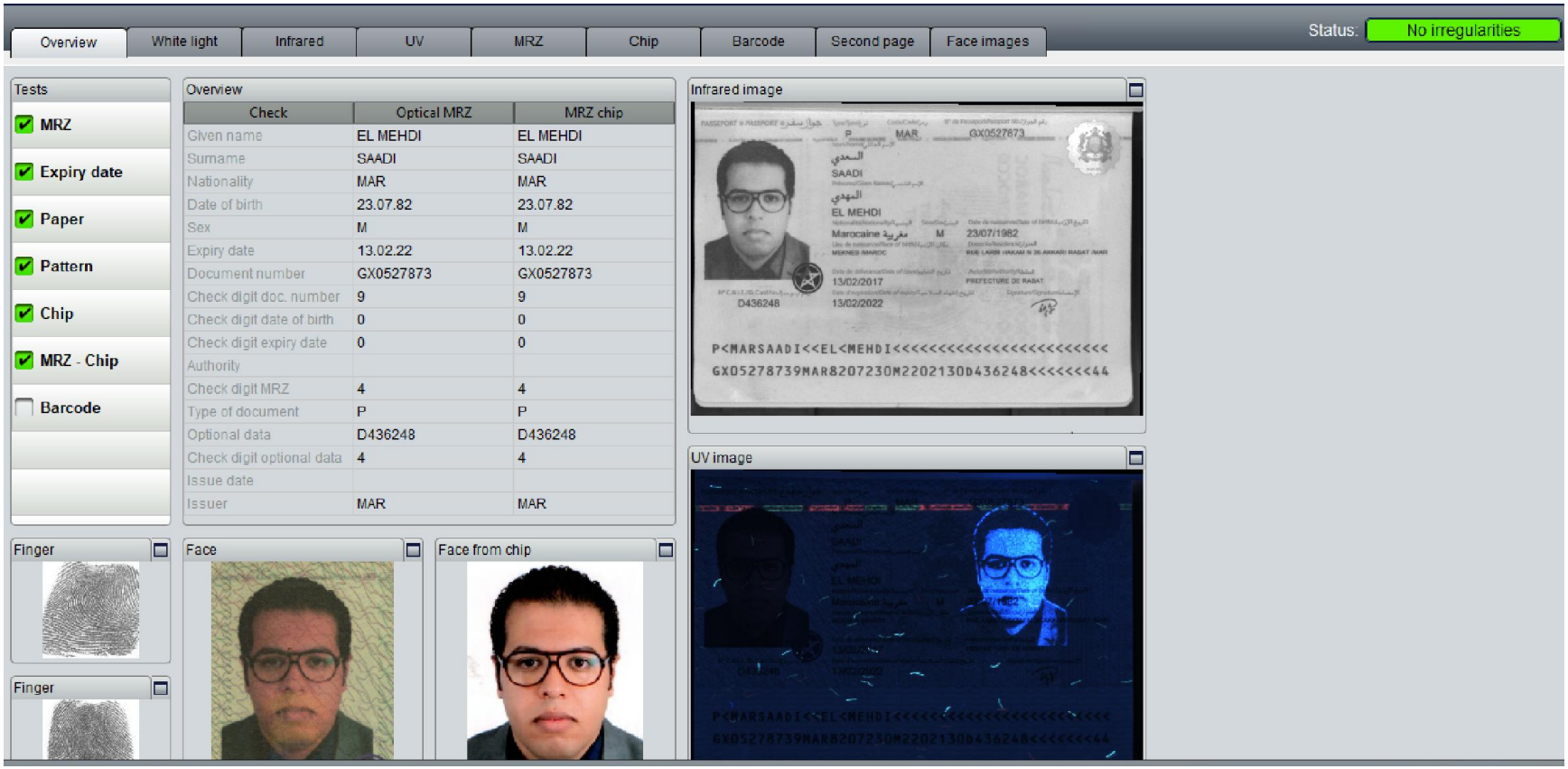
- **Supplemental Access Control (SAC/PACE)** Le protocole PACE (Password Authenticated Connection Establishment) est un mécanisme de contrôle d'accès à la puce qui permet d'établir une connexion sécurisée entre la puce et le système d'inspection avec authentification par mot de passe (calcul de clés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

Résultats des vérifications au niveau des Postes Frontières

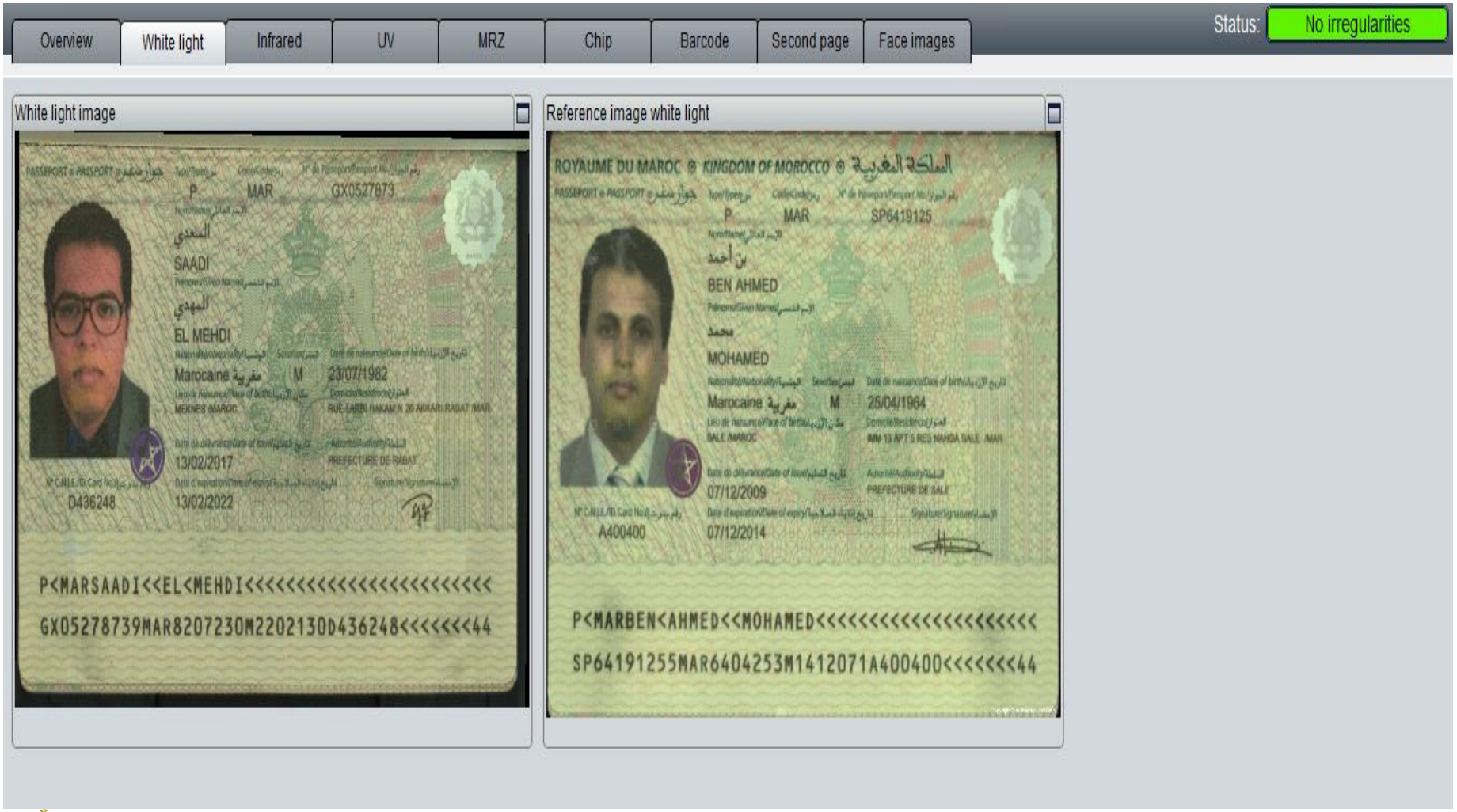
les résultats devraient être interprétés par une application sur le système d'inspection et fournir une réponse simple à l'agent des services frontaliers.



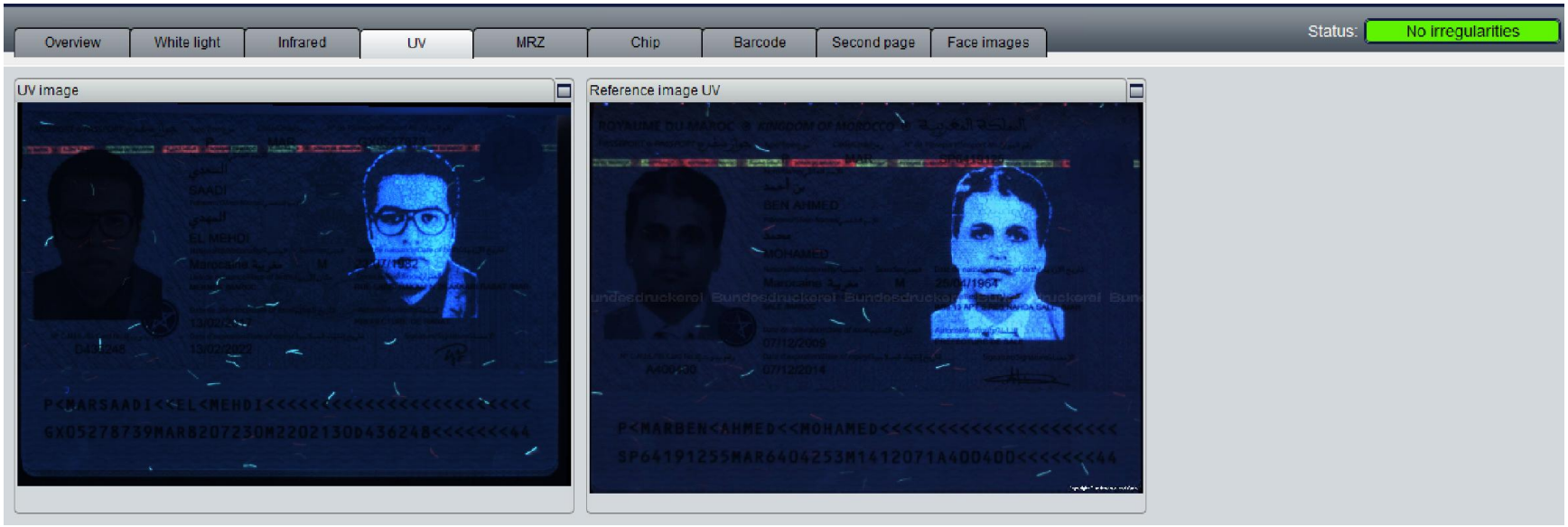
Cas pratique



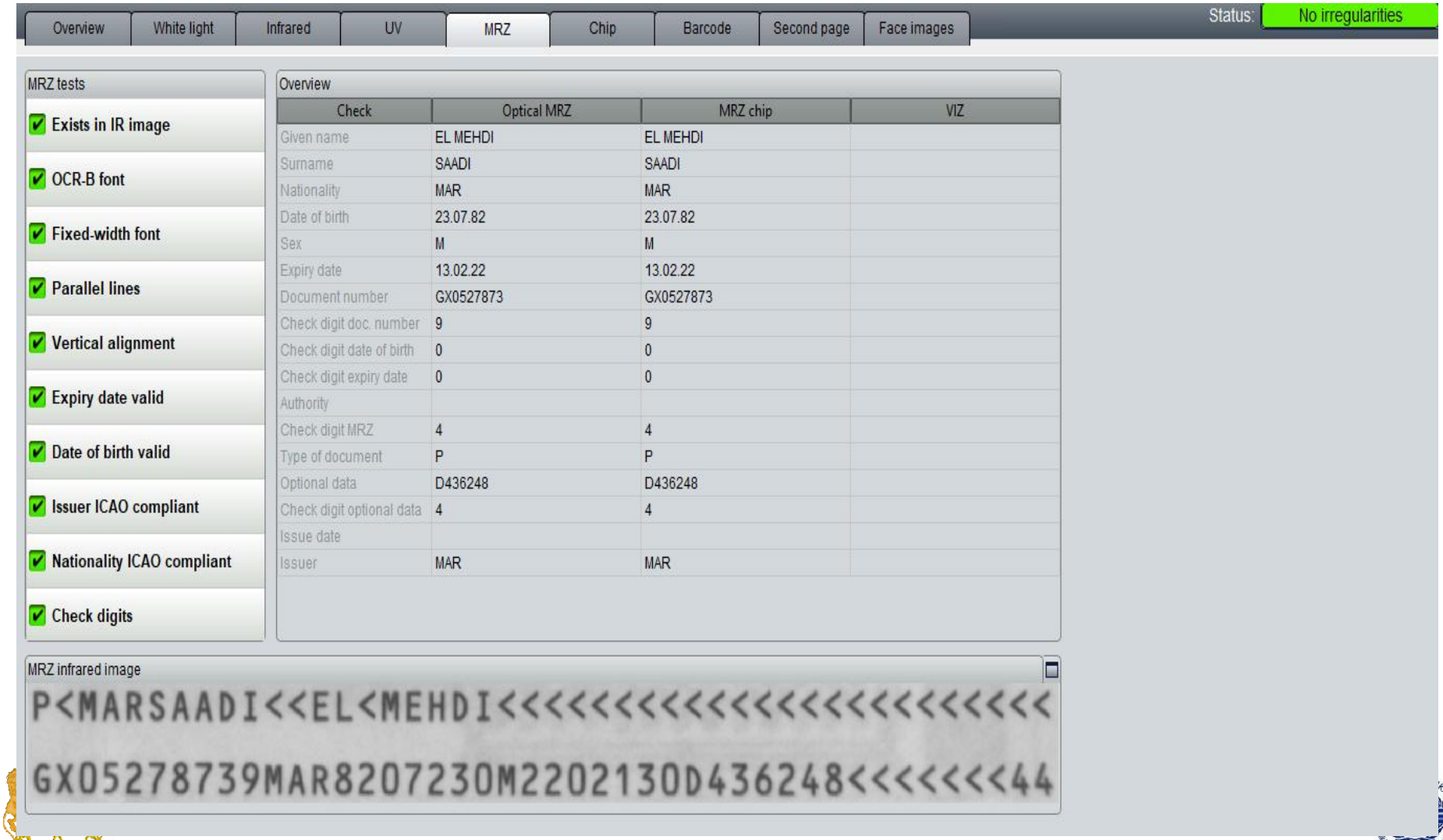
Cas pratique



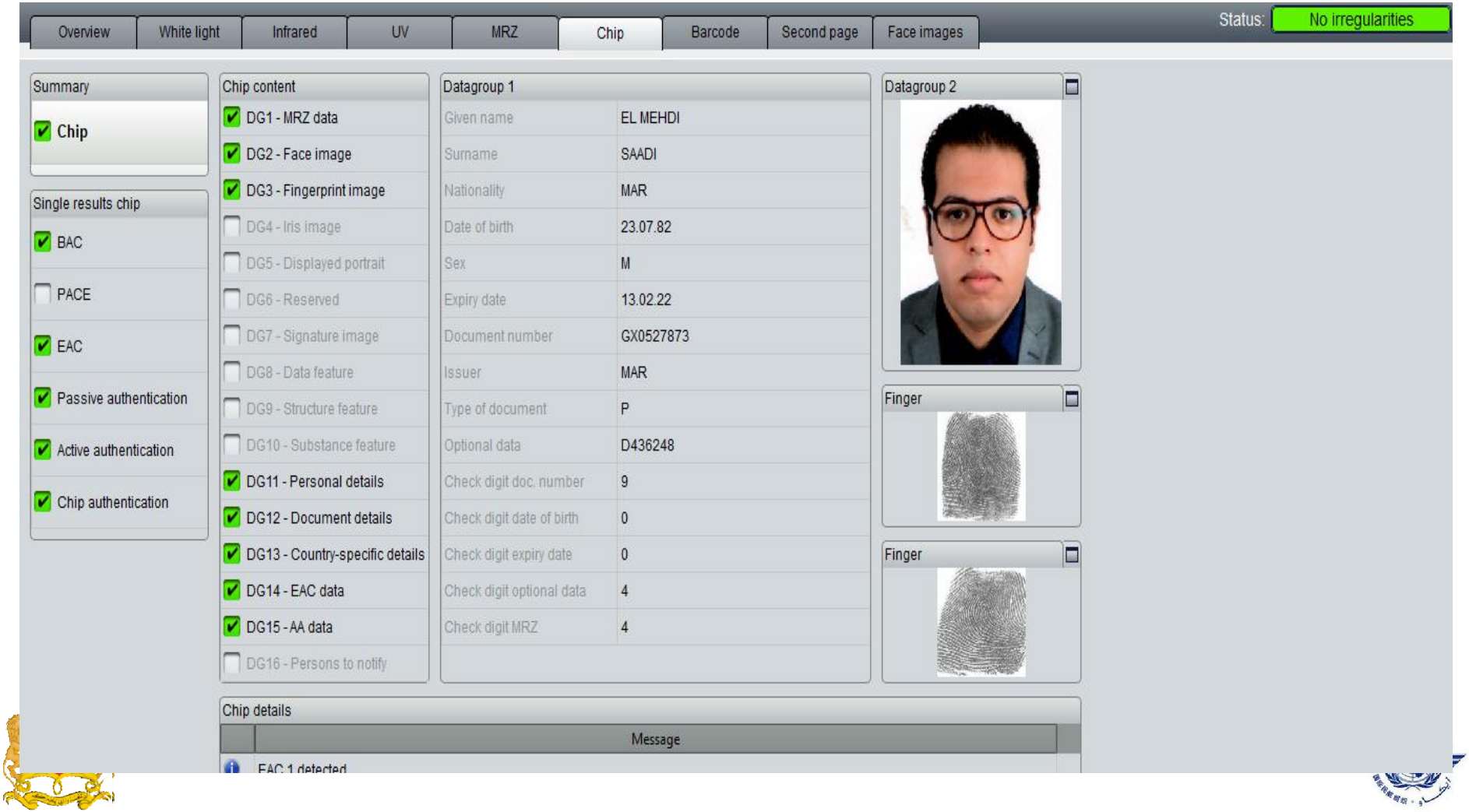
Cas pratique



Cas pratique



Cas pratique



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