UNIVERSITÉ DE RENNES 1

Formation PKI d'entreprise

date de la formation :

25/01/2019

lieu de la formation : Rennes

UNIVERSITÉ DE RENNES 1

partie 1 : Introduction

partie 2 : Rappels de Cryptologie

partie 3 : Certificats numériques

partie 4 : PKI / IGC

partie 5 : Bonnes pratiques IGC

Qui délivre les certificats X509 ?

- Comment être sûr qu'une clé publique reçue provient bien de l'expéditeur annoncé ?
- Comment être sûr qu'une **clé** n'a pas été **volée** ?
- Est-ce que cette clé présente des vulnérabilités ?
- Est-ce que je peux avoir **confiance** dans cette clé publique ?

Qui délivre les certificats X509 ?

- Les certificats X509 sont délivrés par des Infrastructure de Gestion de Clés (IGC ou PKI).
- Une IGC est un ensemble de moyens techniques, organisationnels et humains qui permet d'émettre des certificats X509.
- Une IGC est composée de différentes entités (ou autorités) qui ont un rôle défini dans le cycle de vie des certificats
- Une IGC est un « Ensemble de composants, fonctions et procédures dédiés à la gestion de clés cryptographiques asymétriques et de leurs certificats utilisés par des services de confiance »

Qui délivre les certificats X509 ?

Une IGC permet d'établir de fortes **garanties** afin d'être un vecteur de la **confiance** à travers l'utilisation :

- de techniques cryptographiques robustes
- de **procédures** documentées de délivrance, de gestion des identités électroniques et de contrôles de sécurité

L'IGC est le point de rassemblement de la cryptographie et des procédures.

Qui délivre les certificats X509 ?

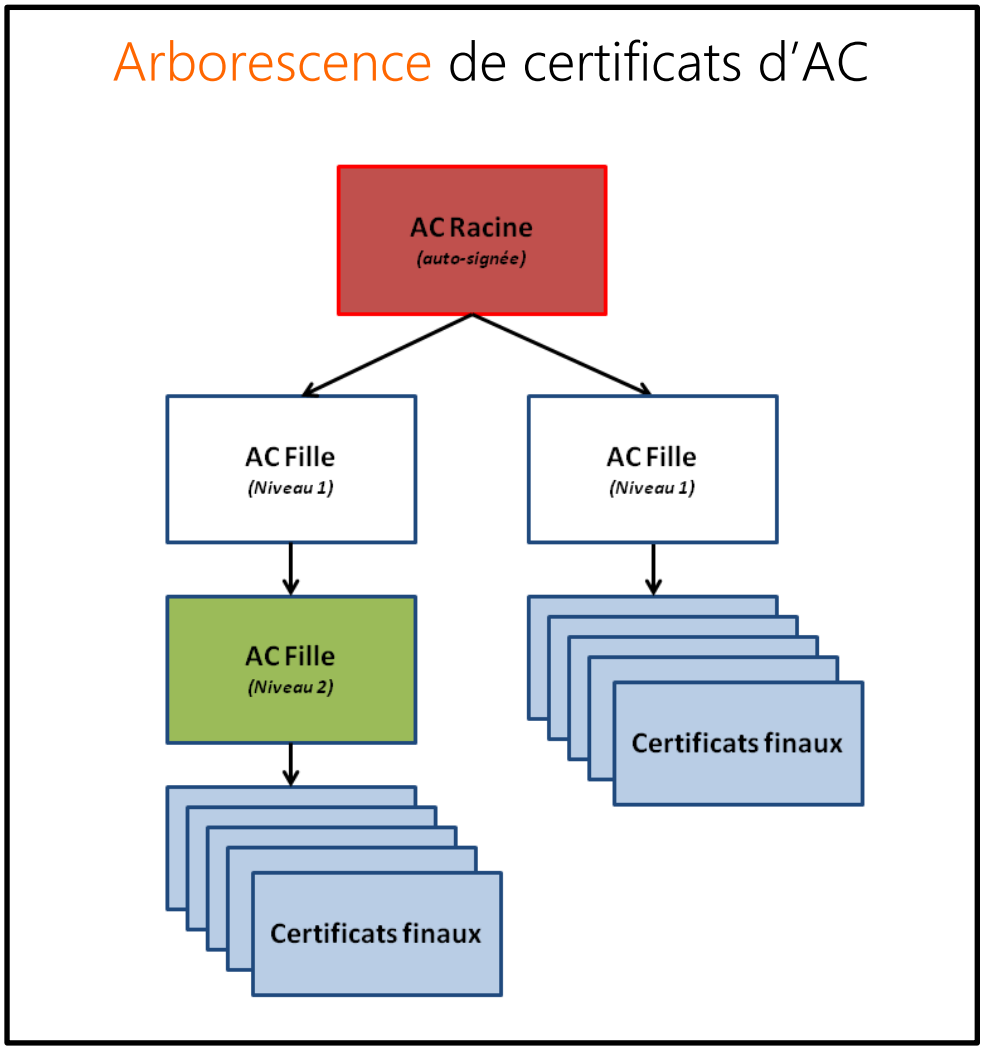
- Une IGC est décomposée sous forme d'**Autorités**
- Chaque Autorité a ses propres buts **fonctionnels** (signature de certificats, vérification des prérequis, etc.)
- Chaque Autorité définit des procédures **dédiées** pour remplir ces buts fonctionnels

Qui délivre les certificats X509 ?

- L'Autorité de Certification (AC) est la composante de l'IGC chargée de signer les certificats et LCR.

- Techniquement la partie AC d'une IGC se présente sous la forme d'une **arborescence** de certificats (chaîne de certification)
  - Chaque AC possède une paire de clés (1 clé publique & 1 clé privée).
  - Si l'on a confiance en une AC mère, on a automatiquement confiance en une AC fille.
  - Une AC peut signer le certificat d'une autre autorité de certification.
  - Le certificat de l'AC racine est auto-signé (signé par lui-même)

Qui délivre les certificats X509 ?



Qui délivre les certificats X509 ?

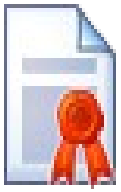
Une requête PKCS#10 est envoyée à l'AC

L'AC génère le certificat suite à la demande

AC

L'AC calcule le Hash de la requête

L'AC utilise sa clé privée pour chiffrer le hash (signature)

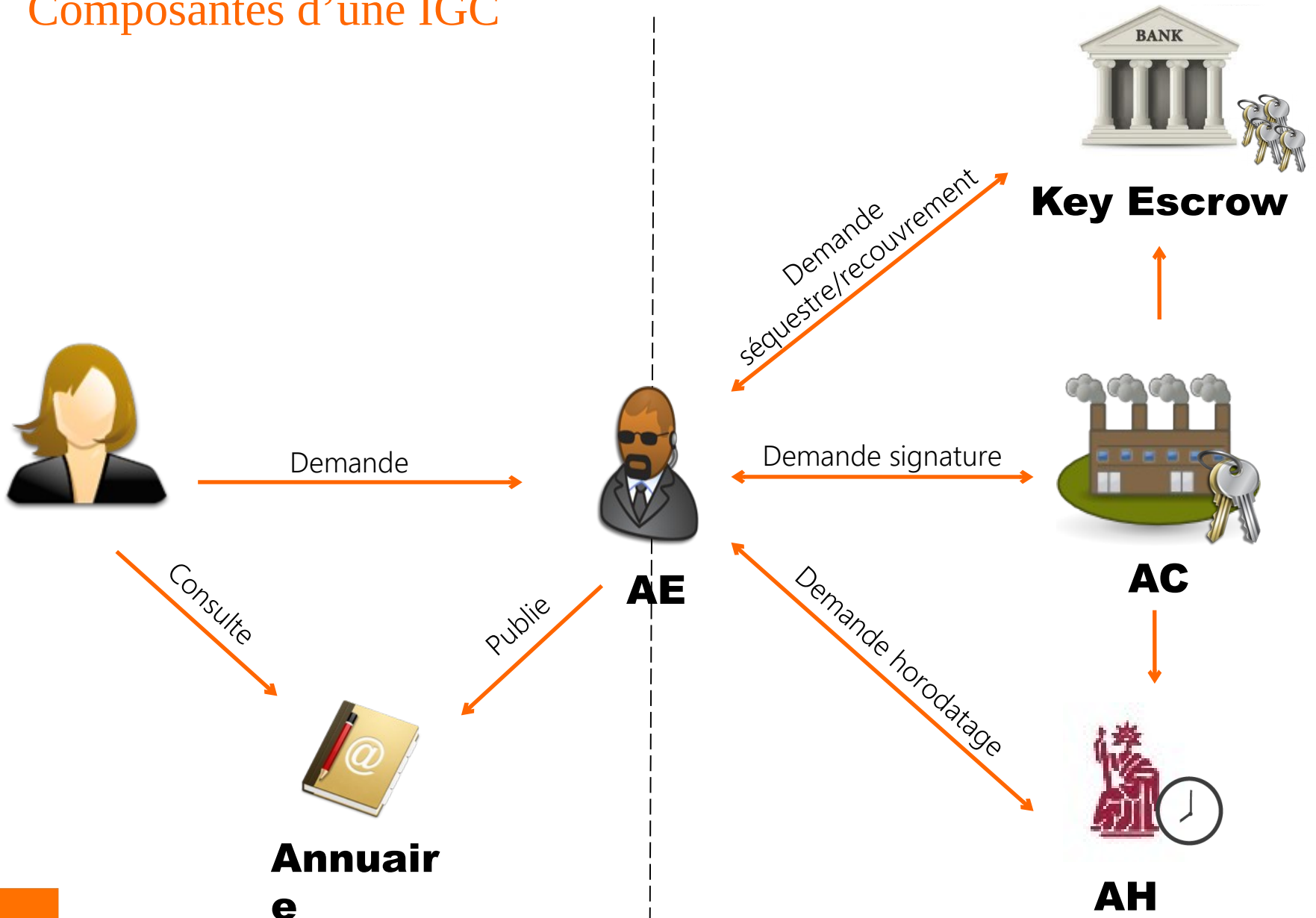


Le hash signé est ajouté à la requête pour former un certificat

Les rôles d'une IGC

- Garantir la confiance
  - Garantir la robustesse des solutions et des procédures mises en œuvre par des contrôles de sécurité fréquents
- Contrôler les demandes
  - Vérification de la légitimité et de la preuve d'identité du demandeur
- Identifier les acteurs
  - Identifier, authentifier et habiliter les différents acteurs qui interagissent dans les procédures de l'IGC en fonction de leur profil
- Gérer les certificats & les bi-clés
  - Génération, renouvellement, révocation, publication
  - Génération et distribution des bi-clés, séquestre des bi-clés

Composantes d'une IGC



Composantes d'une IGC

- Autorité de Certification (AC)
  - L'entité critique qui émet (signe) les certificats
    - signe les demandes de certificats (CSR) et les liste de révocation (LCR)
    - conserve de manière sécurisée les bi-clés de la chaîne de certification

- Autorité d'Enregistrement (AE)
  - L'entité qui enregistre les demandes de certificats et qui **vérifie** l'identité du demandeur ainsi que les critères d'attribution
    - valide les demandes de certificats
    - vérifie les identités des demandeurs et la légitimité de leur requêtes
    - s'assure du respect des procédures

Composantes d'une IGC

- Autorité de Séquestre (Key Escrow)
  - L'entité qui conserve de manière sécurisée les bi-clés d'un utilisateur
    - séquestre les bi-clés d'un utilisateur final
    - permet le recouvrement des bi-clés pour l'utilisateur ou une autorité légale

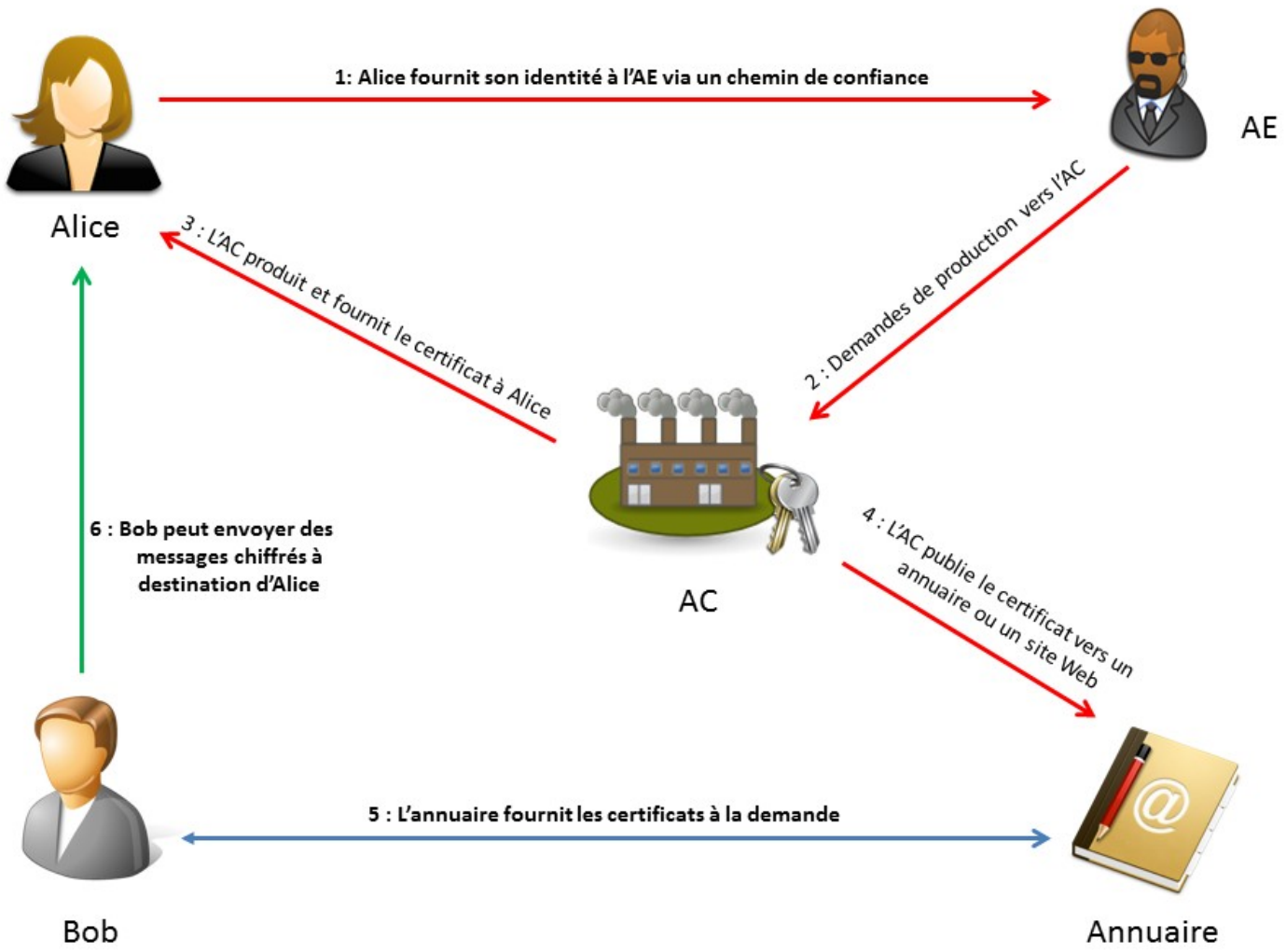
- Autorité de Validation (AV)
  - L'entité qui peut répondre au nom de l'AC pour affirmer qu'un certificat est valide ou non (révoqué, expiré, etc.)
    - met en place des service en ligne de validation de certificats (OCSP)

Composantes d'une IGC

- Autorité d'Horodatage (AH)
  - L'entité qui peut apposer des contremarques de temps signées pour justifier qu'une action a été faite à une heure précise
    - permet de certifier qu'une action a été faite à un temps précis
    - nécessaire pour la mise en place de la notarisation

- Autorité de Dépôt (LDAP)
  - L'entité qui est chargée de stocker les certificats et LCR et de les fournir à la demande
    - stocke les certificats des utilisateurs finaux ou de la chaîne de certification
    - stocke les listes de certificats révoqués
    - permet aux utilisateurs de certificats d'accéder aux certificats des autres utilisateurs ou aux LCR

Transit d'une demande de certificat

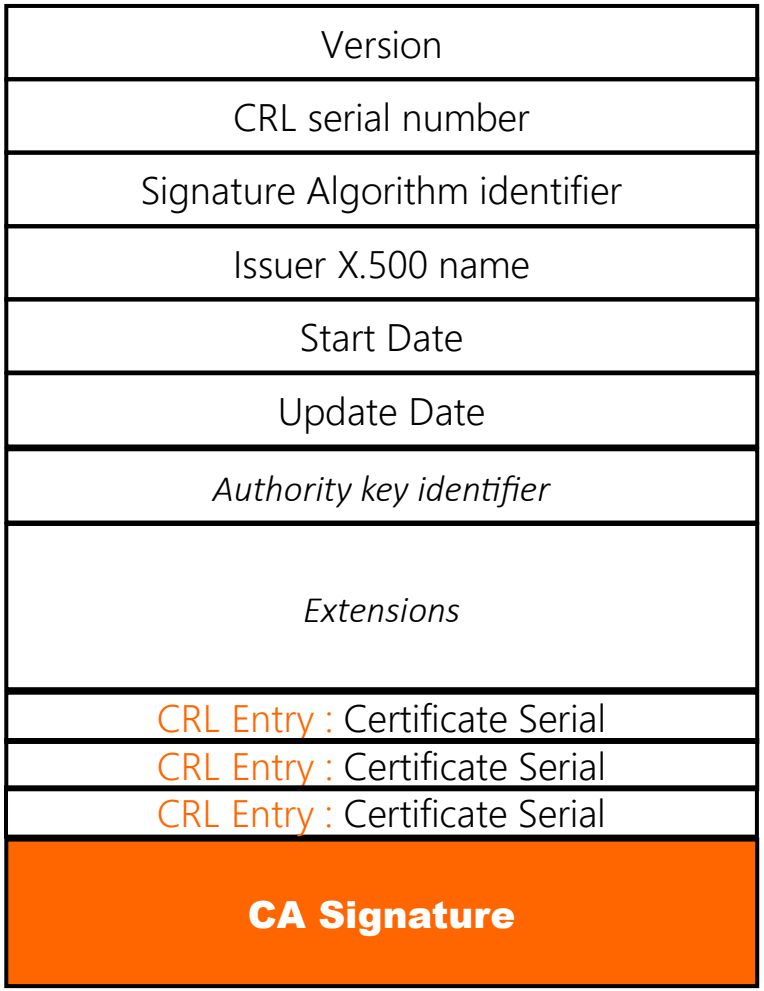


Comment gérer les certificats invalides ?

- CRL – Certificate Revocation List
  - RFC-3280.
  - liste les N° de série des certificats révoqués.
  - inconvénients : délai de mise à jour + accès CRL.

- OCSP – Online Certificate Status Protocol
  - RFC-2560.
  - protocole internet de validation d'un certificat X509.
  - alternative aux CRL.
  - avantages : pas de problématique de cache & accès plus rapide.

Quelles informations contient une CRL ?



- **Version du format de la LCR (1 ou 2)**
- **N° de série UNIQUE de la LCR**
- **Identification des algorithmes utilisés pour signer la LCR**
- **Nom X.500 de l'AC**
- **Période de validité de la LCR (date de début, date de mise à jour)**
- **Extensions de la LCR (option). Valable à partir de la version 2**
- **Entrées de la LCR : les N° de série des certificats révoqués (+ les raisons de révocation)**
- **Signature de la LCR par l 'Autorité de Certification**

Les raisons de révocation

- Non spécifiée
- Clé privée compromise
- AC compromise
- Certificat remplacé
- Cessation d'activité
- Clé privée perdue
- Privilèges retirés
- L'utilisateur ne respecte pas ses engagements vis-à-vis de l'AC (non-respect de contrat)

```
CRLReason ::= ENUMERATED {
      unspecified                (0),
      keyCompromise              (1),
      cACompromise               (2),
      affiliationChanged         (3),
      superseded                 (4),
      cessationOfOperation       (5),
      certificateHold            (6),
      removeFromCRL              (8),
      privilegeWithdrawn         (9),
      aACompromise              (10) }
```

Comment est gérée la révocation ?

- L'AC publie régulièrement une liste de certificats qu'elle a révoqués : les LCR (CRL en anglais)
- La liste de révocation est toujours signée par l'AC
- En cas d'urgence, l'AE doit pouvoir forcer l'AC à publier une liste de révocation immédiatement.
- L'AC peut publier des Delta-CRL entre deux publication de CRL

Quels sont les inconvénients des CRL ?

- Processus non automatique
  - un utilisateur / système doit interroger manuellement la CRL de l'AC concernée avant de valider un certificat
  - l'emplacement de la CRL devrait être indiqué dans le certificat (CRL-DP)

- Mécanisme complexe et consommateur de ressources
  - bande passante (dans le cas d'utilisation intensive des certificats)
  - que faire si un utilisateur/système n'a pas accès à la CRL ou que celle-ci est expirée ?

OCSP : une alternative

1. Un utilisateur souhaite connaître le statut d'un ou plusieurs certificats

2. L'utilisateur contacte l'AV de l'AC du certificat et génère une requête OCSP contenant le N° de série du certificat

3. L'AC interroge sa propre CRL pour connaître le statut du certificat

4. L'AV retourne la réponse OCSP signée à l'utilisateur

Problèmes & Solutions

- https://scotthelme.co.uk/revocation-is-broken/
- Gestion des CRL par les navigateurs modernes ?
  - ☹
- Gestion d'OCSP par les navigateurs modernes ?
  - ☹
- OCSP Stapling + extension « must staple »
  - ☺
- Certificate Transparancy (CT)
  - ☺

partie 1 : Introduction

partie 2 : Rappels de Cryptologie

partie 3 : Certificats numériques

partie 4 : PKI / IGC

partie 5 : Bonnes pratiques IGC

partie 6 : Retours d'expériences

Qui délivre les certificats X509 ?

Important rappel : une IGC doit effectuer des contrôles sur l'identité des demandeurs et la légitimité de leurs demandes

IGC, une question de confiance

le niveau de confiance des certificats est identique à celui de la PKI qui les a émis :

- confiance dans la chaine de certification ;
- confiance dans la manipulation des certificats ;
- confiance dans le processus de délivrance / révocation des certificats ;
- confiance dans les porteurs de certificats (utilisateurs) ;
- confiance dans la protection des secrets ;
- confiance dans la sécurité de l'infrastructure de la PKI.

Importance des Processus et Procédures

- Une IGC est globalement composée de :
  - **20**% d'opérations techniques
  - **80**% d'opérations organisationnelles

- Seule la maitrise des processus et procédures d'une IGC permet de contrôler la sécurité et la **confiance** associées aux certificats générés

- Les procédures permettent de définir les **objectifs** de confiance
  - Etablir des prérequis afin de gérer, protéger et distribuer des données sensibles.
  - Contribuer à mettre en œuvre la politique de sécurité dans l'infrastructure.

Importance des Processus et Procédures

- Les procédures permettent de :
  - **Définir** « qui doit faire quoi et comment ? » pour tous les cas d'usages
  - **Savoir** « qui a fait quoi, comment et quand ? »

- Elles introduisent une infrastructure **gérable** et en accord avec la politique de sécurité de l'organisation.

- Les procédures doivent être **renforcés** dans l'autorité d'enregistrement et par l'action des opérateurs.

Définition des procédures

- Procédures liées au cycle de vie des AC
  - Cérémonie des clés
    - Procédure de génération des bi-clés d'AC
  - Cérémonie d'Initialisation
    - Procédure d'insertion des bi-clés dans l'IGC
  - Procédure en cas de compromission
    - Quelles sont les actions à mener en cas de compromission des bi-clés d'AC ?
  - Gestion et protection des secrets
    - Quels sont les éléments secrets de l'IGC et qui en est responsable ?

Définition des procédures

- Procédures liées à la gestion des certificats utilisateurs
  - Demande de certificat
    - Éléments nécessaires en entrée, interlocuteurs et validateurs
  - Révocation de certificat
    - Éléments nécessaires en entrée, interlocuteurs et validateurs
  - Renouvellement de certificat
    - Éléments nécessaires en entrée, interlocuteurs et validateurs
  - Génération des bi-clés
    - Génération des clés et moyens cryptographiques associés

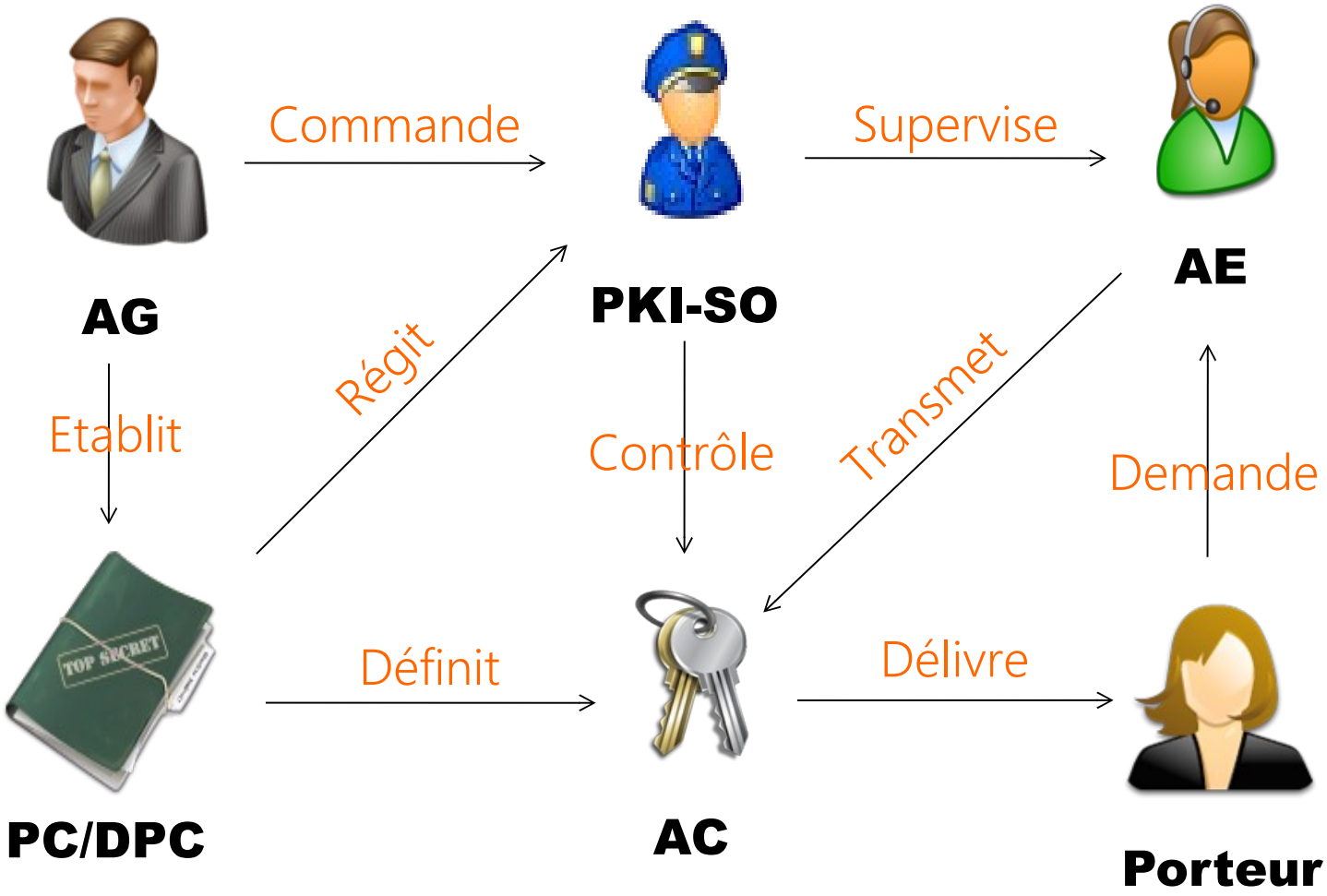
Définition des procédures

- Procédures liées à l'exploitation de l'IGC
  - Mise à jour de l'IGC
    - Processus de mise à jour, correctifs de sécurité
  - Sauvegarde / restauration
    - Comment et avec quel niveau de sécurité est sauvegardé l'IGC ?
  - Plan de continuité d'activité
    - Comment revenir en conditions opérationnelles après un sinistre ?
  - Audits et contrôles
    - Quels sont les éléments essentiels à contrôler, comment et avec quelle fréquence effectuer ces contrôles ?

Définition des rôles

- Une IGC nécessite la définition et l'attribution (droits & devoirs) de ces rôles :
  - Porteur de secret (DS)
  - Opérateur de certification (OC)
  - PKI Security Officer (PKI-SO)
  - Opérateur d'AE (OAE)
  - Administrateur / Exploitant
  - Opérateur du support
  - Auditeur / contrôleur
  - Autorité de Gouvernance (AG)
  - Détenteurs de certificats & demandeurs

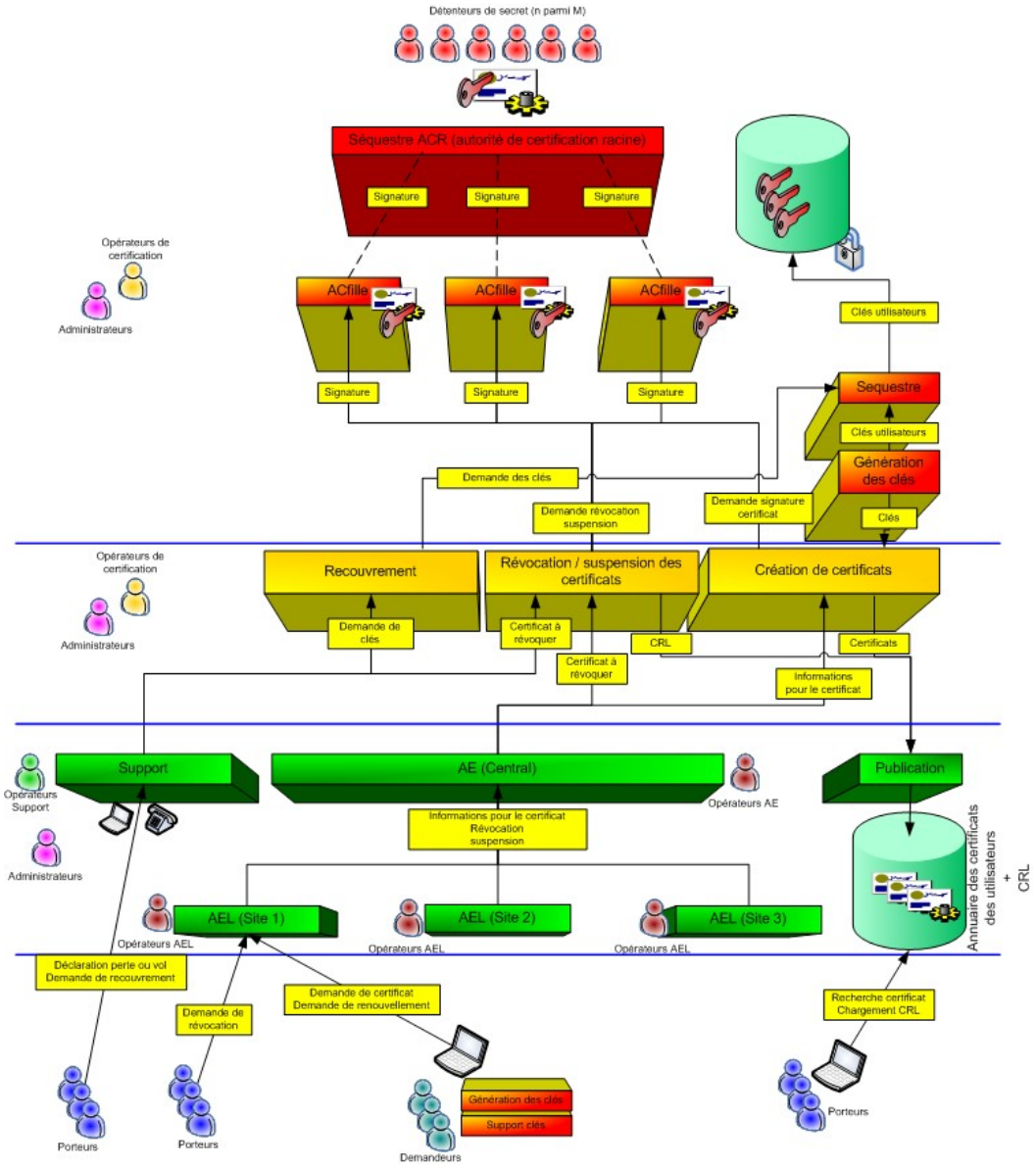
Définition des rôles



Cloisonnement des rôles

- Il est primordial de bien **séparer** les rôles des différents acteurs de l'IGC afin qu'une personne n'ait pas un contrôle total sur l'infrastructure
- Il est préférable de **partager** les secrets de l'IGC entre plusieurs parties (notamment les clés d'AC) pour éviter les compromissions
- Il est nécessaire que les rôles critiques à l'IGC soient des compétences **internes** à l'organisation

Cloisonnement des rôles



Politiques de certification

- Les procédures de l'IGC et les obligations sont documentées dans :
  - La Politique de Certification (PC)
  - La Déclaration des Pratiques de Certification (DPC)
  - Les Conditions Générales d'Utilisation (CGU)

- Ces documents décrivent les mécanismes (juridiques, organisationnels et techniques) établis pour assurer la sécurité et le niveau de **confiance** de l'IGC.
  - RFC 3647 : Certificate Policy and Certification Practices Framework
  - En Europe : ETSI 102 042
  - En France : RGS

Politiques de certification

- La PC :
  - Décrit les exigences qui définissent la génération, la délivrance et l'utilisation des certificats
  - Liaison entre l'IGC et les utilisateurs, elle permet d'établir la confiance
  - Document publique accessible à tous

- La DPC
  - Décrit les pratiques et procédures implémentées pour respecter les règles de la PC
  - Définit les noms des acteurs et leur fonction, les procédures et les mesures techniques mises en œuvre
  - Document confidentiel accessible aux auditeurs

Politiques de certification

- Les exigences décrites dans les PC couvrent de nombreux aspects, notamment :
  - Processus de gestion des certificats (délivrance, révocation, renouvellement) ;
  - Niveau de sécurité physique et logique des infrastructures techniques ;
  - Niveau d'engagement juridique de l'Autorité de Certification vis à vis des porteurs, de tiers ;
  - Traçabilité des opérations effectuées par tous les participants au sein de la chaine de confiance ;
  - Continuité du service, et plan de reprise en cas d'incident ;
  - Niveau de disponibilité des infrastructures ;
  - Gestion des habilitations des personnels faisant partie de la chaîne de confiance ;
  - Archivage de toutes les pièces permettant de reconstituer le cycle de vie des certificats émis (formulaires d'enregistrement, validations internes, certificats, CRL…) ;
  - Engagements en matière de qualité de service (sur tous les aspects liés à la gestion des certificats, et pas seulement sur le niveau de disponibilité des serveurs).

partie 1 : Introduction

partie 2 : Rappels de Cryptologie

partie 3 : Certificats numériques

partie 4 : PKI / IGC

partie 5 : Bonnes pratiques IGC

partie 6 : Retours d'expériences

Les étapes de mise en place d'un projet IGC : Think

Etape 1 : Etude du contexte

Analyse du besoin :
- pourquoi mettre en œuvre une PKI ?
- quels services seront offerts par la PKI (chiffrement , etc.) ?
- quelles populations sont concernées ?

Expression de besoins

Etape 2 : Analyse de risques

Identifier les menaces :
- prendre en compte le contexte (analyse fonctionnelle & technique)
- définir les besoins de sécurité
- définir les risques encourus
- mettre en regard les moyens nécessaires à la maitrise des risques

Objectifs et exigences de sécurité

Etape 3 : analyse des objectifs de sécurité

Définition des exigences :
- définir les catégories de certificats en fonctions des usages et risques associés
- détermination des exigences de sécurité associées à chaque catégorie (stockage, activation, sensibilité)
- définition des prérequis associés à chaque catégories (demande, validation, délivrance, etc.)

Profils de certificats + Ebauches de PC

Etape 4 : Etudes amont

Etudes du choix de PKI :
- PKI interne ou externalisée ?
- quels sont les acteurs impliqués dans le cycle de vie de la PKI ?
- quelles sont les procédures au cycle de vie des certificats et de la PKI ?
- quels outils / protocoles doivent être utilisés ?

Chartes des acteurs + Ebauches de procédures

Etape 5 : Rédaction du cahier des charges

Cahier des charges :
- définir le support d'évaluation des solutions PKI
- définir les exigences contractuelles, de maintenance, de support, etc.

Cahier des charges de la PKI

Les étapes de mise en place d'un projet IGC : Build

Etape 1 : PC

Politiques de Certification :
- rédaction des exigences techniques, organisationnelles et de sécurité de la PKI sous forme de Politique de certification (RFC 3647)
- une politique de certification par usage (AC racine, authentification, etc.)

Politiques de Certification

Etape 2 : Préparation KC

Préparation de la KC :
- préparation de la cérémonie des clés (Key Ceremony) en vue de créer des procédures de génération d'AC de confiance en liaison avec le HSM sélectionné et les acteurs de la PKI

Scripts de cérémonie ces clés

Etape 3 : Intégration

Intégration de la PKI :
- rédaction des dossiers de spécification et d'architecture
- intégration et/ou développement de la solution PKI
- paramétrage des outils et de la solution
- rédaction des dossiers d'installation, exploitation et administration de l'infrastructure

Dossiers d'installation, d'exploitation et d'administration

Etape 4 : DPC

Déclarations des pratiques de certification:
- rédaction des procédures de gestion de l'IGC et du cycle de vie des certificats
- Rédaction des déclarations des pratiques de certification en liaison avec les PC et les documents de la PKI (procédures, scripts de KC, DAT, MI, MEX, etc.)

Déclarations des Pratiques de Certification

Etape 5 : Validation

Cahier des charges :
- mise en œuvre de l'infrastructure et de l'organisation associée sur une plateforme de pré-production
- mise en œuvre des outils nécessaires à la réalisation des tâches des différents acteurs de l'IGC
- tests et validation de la solution et des procédures
- formation des acteurs

Cahiers de tests Supports de formation

Les étapes de mise en place d'un projet IGC : Run

Etape 1 : KC

Cérémonie des clés :
- initialisation du HSM et des secrets associés
- génération des bi-clés de l'AC racine et auto-certification de celle-ci
- génération de ou des AC fille(s)
- génération de l'ARL

Secrets & certificats AC + ARL

Etape 2 : Mise en Production

Mise en production :
- déploiement de la solution sur la plateforme de production
- cérémonie d'initialisation en vue d'insérer les clés dans le HSM
- mise en place d'une phase pilote avec un groupe de test
  - revue des procédures

Procédures de gestion de l'IGC

Etape 3 : Déploiement

Déploiement à grande échelle :
- accompagnement des futurs porteurs
- accompagnement du support (help-desk)
- planification du déploiement
- migration (si besoin) d'une ancienne PKI

Supports de Formation / accompagnement
Dossier de migration

Etape 4 : Exploitation

Exploitation de la PKI :
- exploitation et administration de l'infrastructure
- correction ou amélioration de défauts techniques ou organisationnels
- maintien en condition opérationnelle et en condition de sécurité

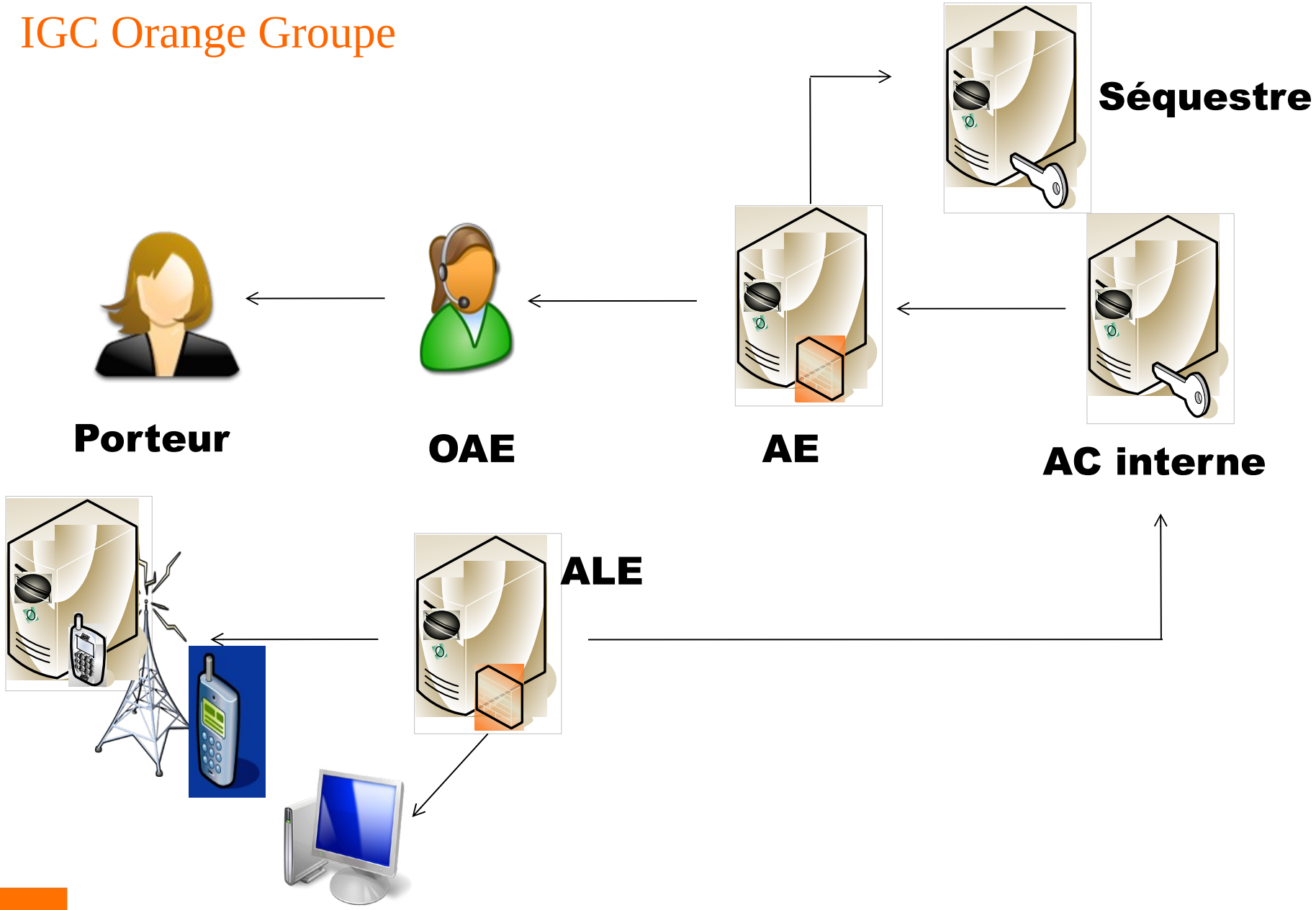
Dossiers de MCO/MCS

Etape 5 : Audits

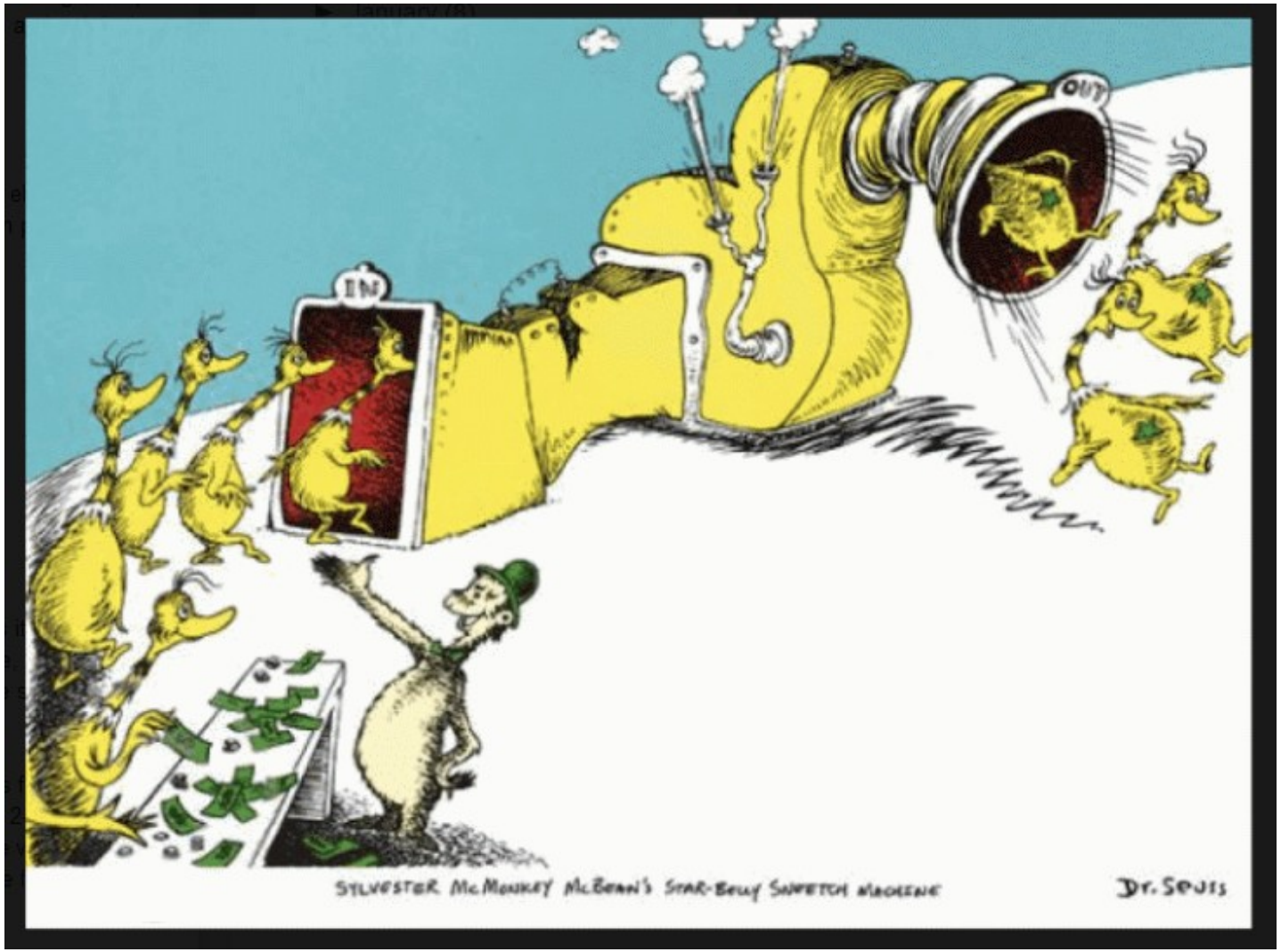
Audits de la PKI :
- Mise en place de contrôles internes afin de s'assurer de la bonne mise en œuvre des procédures
- Mise en place de contrôles externes afin de s'assurer de la conformité de la PKI avec les bonnes pratiques
- amélioration des procédures et pratiques

Rapports de contrôle et cahier de suivi

IGC Orange Groupe



OpenSSL


IN
OUT
SYLVESTER McMONKEY McBEAN'S STAR-BELLY SNEETCH MACHINE
DR. SEUSS

Questions

Merci