Les Infrastructures de Gestion de Clés

Établir la confiance en environnement non sécurisé

Nathanaël Cottin

contact@ncottin.net
http://www.ncottin.net

version 0.0.11 – 26 avril 2011

Besoins communs des systèmes d'information

- Identification
- Authentification
- Autorisation
- Confidentialité
- Intégrité

Besoins de sécurité complémentaires

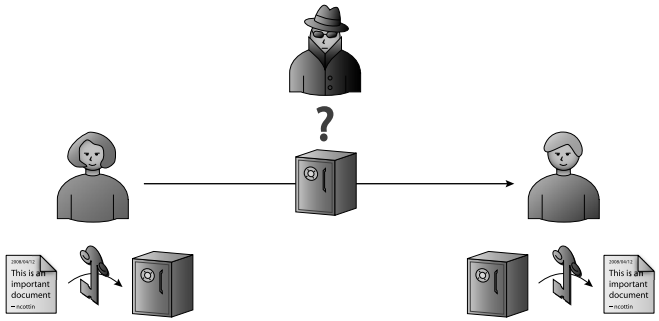
- Authentification forte
- Authenticité
- Non-répudiation de l'origine et de la destination
- Datation certaine

Question fondamentale

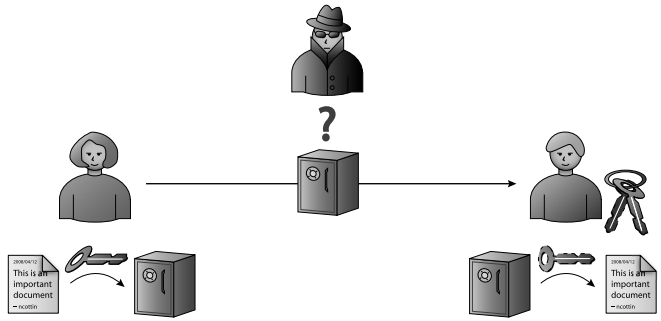
Lien clé - identité

Comment s'assurer qu'une clé publique (de chiffrement ou de vérification de signature) appartient bien à une entité donnée ?

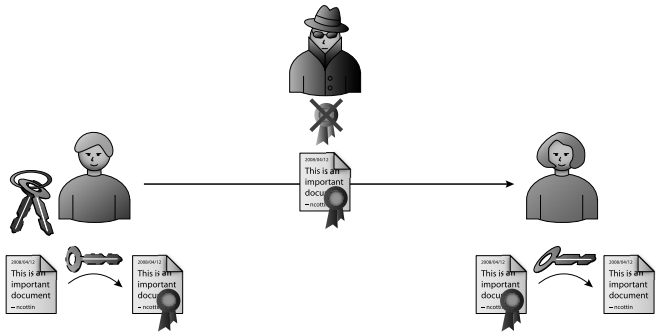
Chiffrement symétrique



Chiffrement asymétrique



Signature numérique

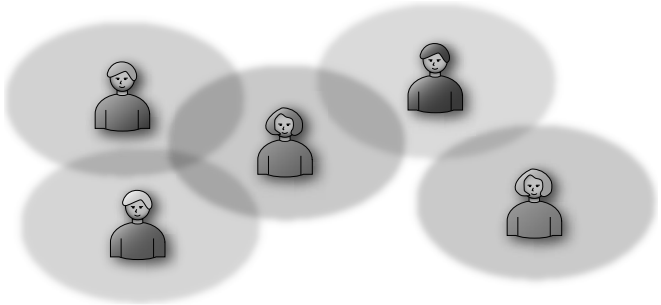


Modèles de confiance

- Confiance *partagée* : toile de confiance
- Confiance *procurée* : centre de distribution de clés
- Confiance *certifiée* : tiers certification

Toile de confiance

Décentralisé : confiance *partagée*

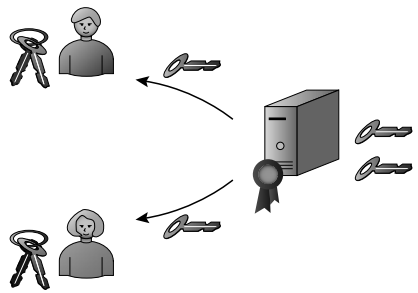


Confiance *partagée* : fonctionnement

- Listes locales de *personnes de confiance*
- Diffusion sur des serveurs publics

Centre de distribution de clés

Intermédiaire pour conservation des clés : confiance *procurée*

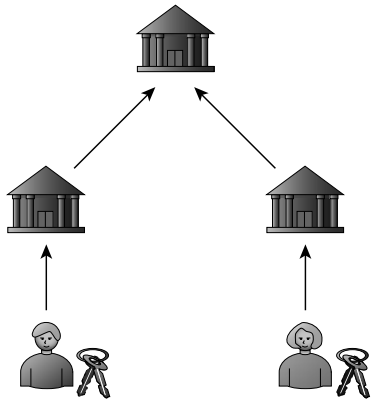


Confiance *procurée* : fonctionnement

- Enregistrement des clés et identités auprès d'un KDC
- Demande de clés au KDC
- Repose sur des protocoles sécurisés

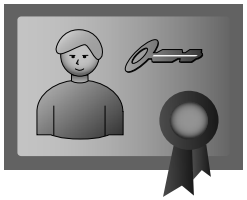
Tiers certification

Modèle pyramidal : confiance *certifiée*

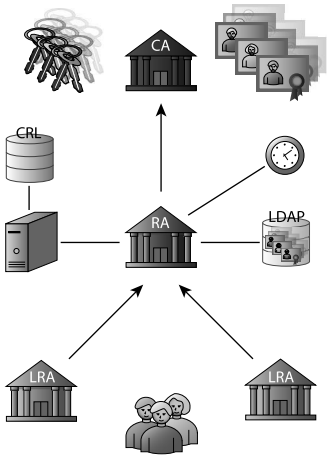


Confiance *certifiée* : fonctionnement

- Enregistrement des clés et identités auprès d'un PSCE
- Attestation du lien $\{\text{clé}, \text{identité}\}$
- Repose sur la signature numérique



Modèle général des IGC



Autorité locale d'enregistrement

Services proposés :

- Guichet ouvert aux clients
- Enregistrement des demandes
- Conservation des justificatifs
- Mise à disposition des données de sécurité
- Suivi des opérations
- Gestion des dossiers clients

Autorité principale d'enregistrement

Services proposés :

- Gestion des LRA (ajout, suppression)
- Collecte des demandes issues des LRA
- Validation (ou refus) des demandes
- Mise à disposition des données de sécurité
- Serveur web d'information
- LDAP des certificats délivrés
- Horodatage (option)

Autorité de certification

Services proposés :

- Génération des clés et certificats
- Enregistrement sur support
- Gestion des clés des RA et LRA

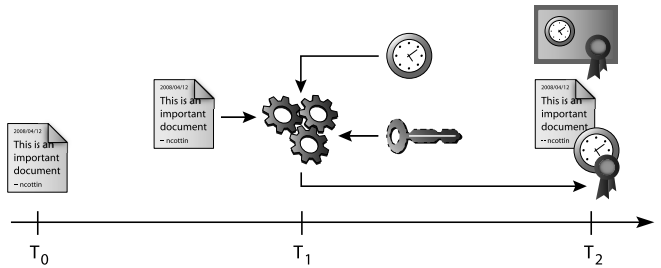
Remarque

Les IGC PKIX utilisent le format X.509

Objet de l'horodatage

- Prouver l'existence d'une information
- Établir la date d'apparition d'un évènement
- Dater des signatures électroniques
- Sceller des données numériques

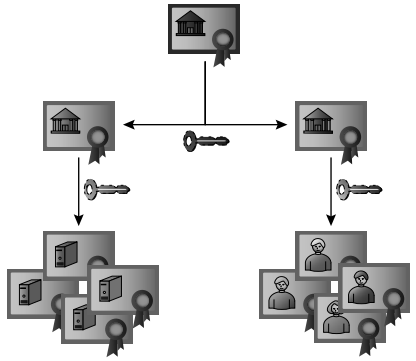
Fonctionnement de l'horodatage



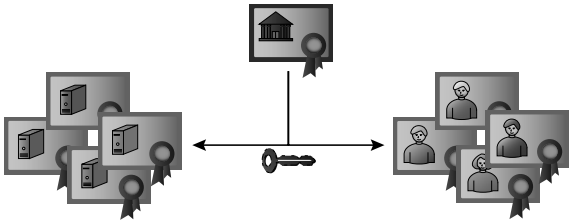
Type de modèles de certification

- Standard
- Réduit
- Différencié

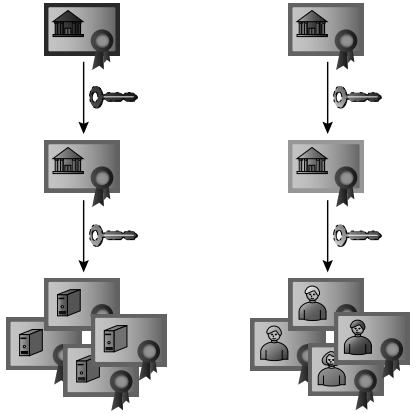
Modèle de certification standard



Modèle de certification réduit



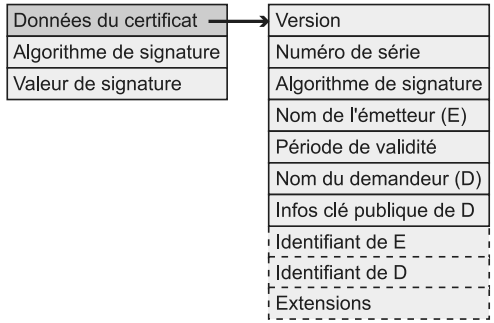
Modèle de certification différencié



Certificat de clé publique

Définition

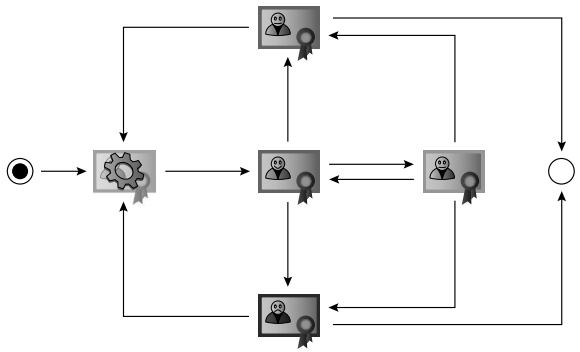
Lien identité (individu, machine) / clé publique



Rôles attribués aux certificats

- Authentification (signature)
- Confidentialité (chiffrement)
- Chiffrement de clé ou de données
- Déchiffrement
- Non-répudiation
- Accord de clé
- Signature de certificats
- Signature de CRL

Cycle de vie d'un certificat

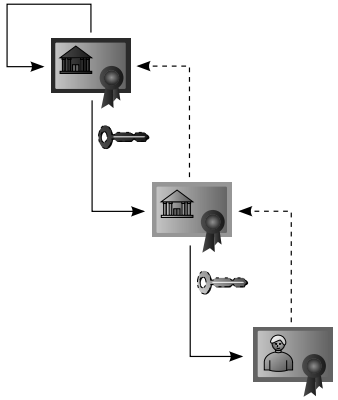


Chemin de certification

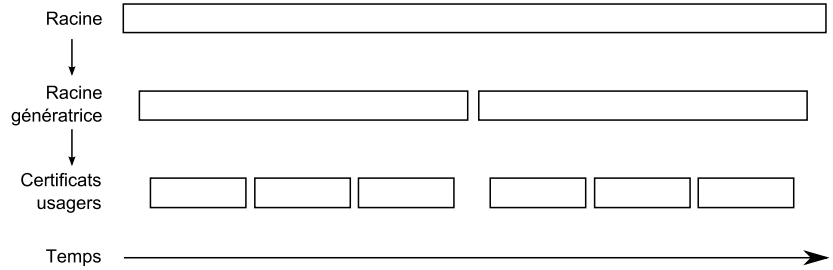
Chemin de certification

Un certificat est authentifié par un second certificat jusqu'à la racine de certification (autosignée). On parle alors de chemin ou chaîne de certification

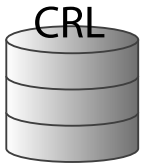
Exemple de chemin de certification standard



Dates de validité



Liste de certificats révoqués (X.509)

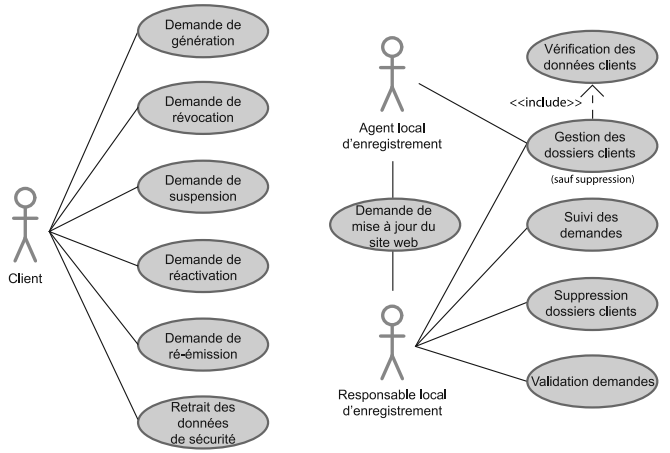


Composition :

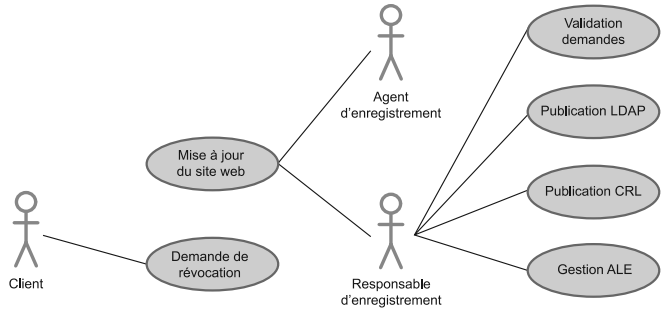
- Identifiants des certificats mis en opposition
- Dates des mises en opposition
- Motivations des oppositions (option)
- Date d'émission de la liste
- Date de prochaine mise à jour (option)

CRL et delta-CRL

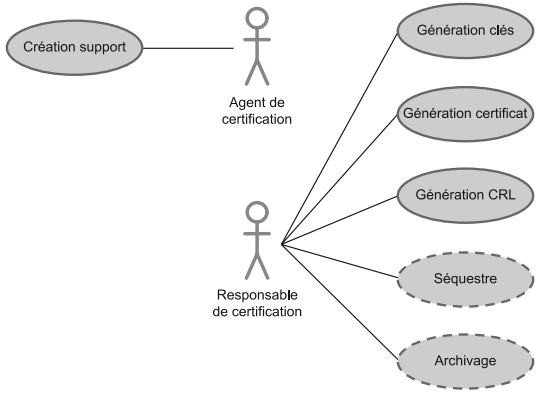
Modélisation d'une ALE



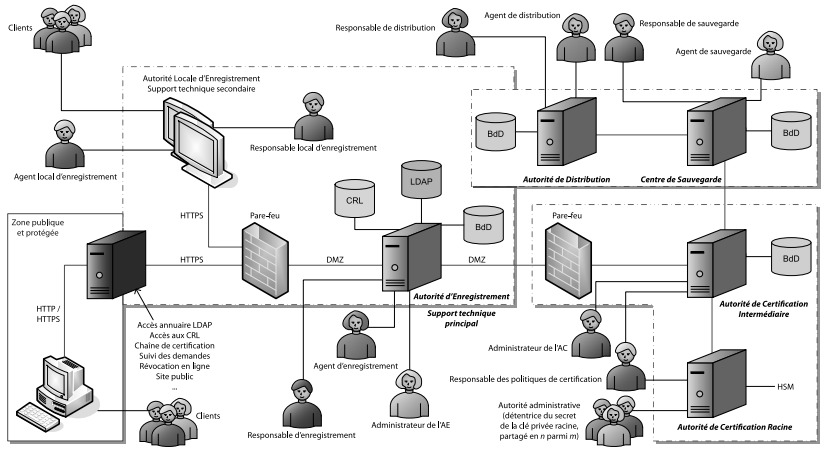
Modélisation de l'AE



Modélisation de l'AC



Exemple d'architecture de déploiement



Hardware Security Modules

Boîtes noires pour :

- Le stockage des clé privées
- Les opérations cryptographiques

FIPS PUB 140-1 : Security Requirement for Cryptographic Modules

Formats d'export

- Certificat : X.509 (v3)
- Chaîne de certification : PKCS#7
- Clé privée : PKCS#1
- Certificat et clé privée : PKCS#12

Bibliothèques

- openssl
- BouncyCastle
- J/CRYPTO de Baltimore Technologies (Java)
- CryptoAPI et CAPICOM de Microsoft (.NET)

Outils

- openssl
- keytool de Sun
- Sign & Crypt d'UTIMACO
- Aliso mySign d'Adesium

Classes de certificats

Définition

Définit le niveau de validation que l'utilisateur peut attendre d'un certificat

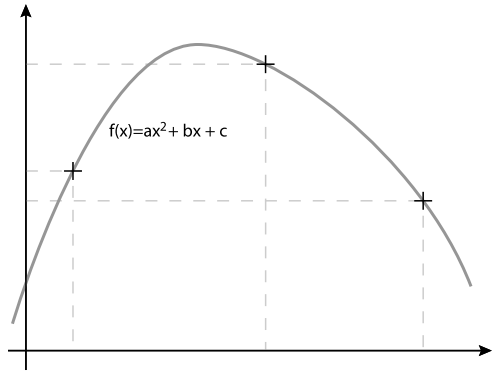
- Classe 1
- Classe 2
- Classe 3

Cérémonie de génération de la bi-clé racine

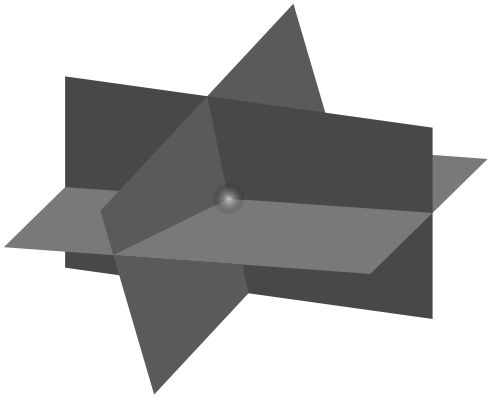
Définition

Procédure supervisée par un organisme habilité au cours de laquelle les données de sécurité racine sont générées et protégées

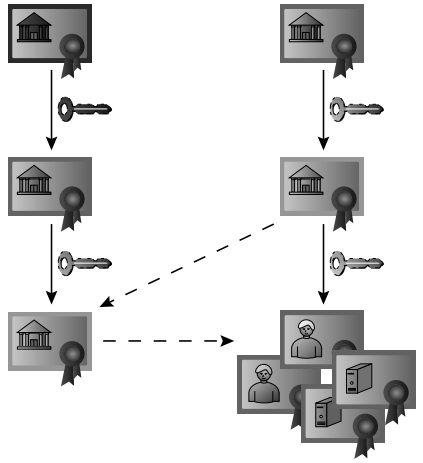
Partage de secret : schéma de Shamir



Partage de secret : schéma de Blakley



Certification croisée



Certificats qualifiés

Définition

Délivré par un PSCE à une personne physique ou morale. Il comporte de nombreuses restrictions relatives à sa génération, à sa distribution et à sa validation

Politique de certification

Définition

Ensemble de règles définissant les services d'un PSCE du point de vue du client

- Standards supportés
- Classes de certificats émis par le PSCE
- Profils des certificats et CRL
- Documents à apporter lors d'une demande

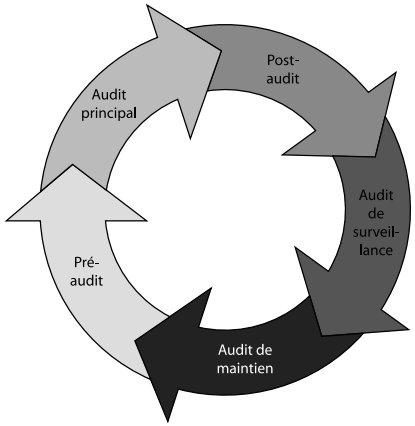
Déclaration des pratiques de certification

Définition

Décrit les modes opératoires internes du PSCE

- Types d'algorithmes utilisés
- Tailles et types de clés
- Délais d'émission des données de sécurité
- Formats et supports

Processus d'audit



Documents normatifs pour accréditation des PSCE

- BS7799 (ISO 17799)
- ANSI X9.79
- ETSI TS 101.456
- RS 784.103.1
- ISO 15489-1

Processus d'agrément

1. Demande de reconnaissance
2. Examen de la demande
3. Entente
4. Maintien

Documents normatifs pour agrément

- NF EN 45012
- ISO 10011-1/-2/-3
- CWA 14172-1
- BS7799 (ISO 17799)
- BS1500-1
- ISMS