Sécurité des RO

Partie 4

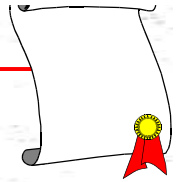
PKI
IGC

Anas ABOU EL KALAM
anas.abouelkalam@enseeiht.fr

PKI

IGC

Certificats : pourquoi ?



- **chiffrement & signatures supposent l'authenticité des clés publiques, disponibles sur un annuaire ou un serveur web**
  - signature garantit que le message provient bien du détenteur de la clé privée … mais …
    - A qui appartient clé privée/publique ?
  - Chiffrement garantit que le message ne pourra être déchiffré que par le détenteur de la clé privée (associée à la clé publique utilisée lors du chiffrement) … mais
    - A qui appartient cette clé publique ?
- ***Est-on sûr qu'il ne s'agit pas d'un usurpateur ?***

Certificats : pourquoi ?

- *Scénario* :
  - Alice et Marie veulent s'envoyer des messages
  - Bob = pirate

Bob
- modifie l'annuaire ou le serveur web qui héberge les clés publiques
- remplace clé publique d'Alice par la sienne.

- Bob peut mnt lire les courriers destinés à Alice et signer des message en se faisant passer pour Alice !!

- si Marie envoie message « M » chiffré à Alice,
  - Marie va chiffrer M avec clé publique de Bob (*croyant que c'est la clé d'Alice*).

- Bob pourra
  - déchiffrer les messages destinés à Alice avec sa clé privée,
  - lire ainsi le courrier confidentiel d'Alice.

Les signatures et les MACs ne résolvent pas entièrement le problème de l'authenticité.

On introduit alors la notion de **certificat** !

Certificats : quoi ?

- **permet d'établir un environnement de confiance entre deux entités distantes ayant besoin de communiquer entre elles et de s'échanger des informations :**
  - non-répudiables (nécessité de signature) ou
  - confidentielles (application de chiffrement).

- **certificat : vise à effectuer un lien entre une personne et une bi-clé (privé/publique)**
  - Il est délivré par une autorité de certification (AC)
  - Il est nominatif
  - Il est destiné à un usage unique (signature OU chiffrement)
  - Il a une durée de validité donnée
  - Il est certifié par l'AC
  - Il est révocable

- **X.509-v3 : norme proposée par l'ISO (et la plus répandue)**

Utilisation des certificats

- Services fondamentaux de sécurité
- Utilisés par de nombreuses applications et protocoles
  - SSLv3/TLSv1 (https, ldaps, IMAPS, POPS ...)
  - VPN IPSec avec IKE
  - Authentification de niveau 2 : EAP-TLS (802.1X)
  - Chiffrement de volume
  - Signature électronique

Formats

Il n'existe pas d'usages canoniques pour les extensions de fichiers contenant des certificats. Ils peuvent varier suivant les produits et les éditeurs !!

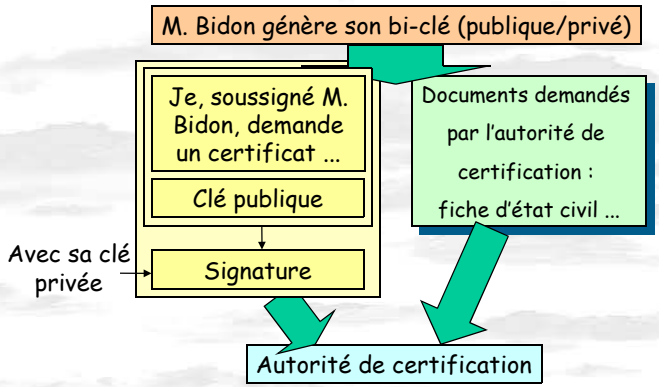
- **DER (Distinguished Encoding Rules) [6]**
  - ASN.1 (Abstract Syntaxe Notation One)
  - Représentation de données sous un format binaire
  - autres: BER (Basic Encoding Rules) CER (Canonical E.R)
  - exnsions usuelles : .der, .cer, .crt, .cert
- **PEM (Privacy Enhanced Mail)**
  - format par défaut de openssl
  - Peut contenir clés privées, clés publiques et certificats X509.
  - C'est du DER encodé en base64 auquel sont ajoutées en-têtes en ASCII
  - Extensions usuelles : .pem, .cer, .crt, .cert
- **PKCS#12 (Personnal Information Exchange Syntax Standard)**
  - fait partie des spés (Public-Key Cryptography Standards) de sté RSA
  - format (binaire) d'exportation d'un certificat et/ou d'une clef privée
  - standard pour stocker des clés privées, des clés publiques et des certificats en les protégeant en confidentialité et en intégrité (e.g., mdp)
  - utilisé par Mozilla et IE/Outlook pour importer/exporter certificat avec sa clé privée associée.

Formats

	I/E/ Outlook	Mozilla / Netscape 7 Netscape 4.7x	
Exportation cert	PEM / DER		
Importation cert	PEM / DER	PEM / DER	
Exportation cert avec Kp	PKCS#12	PKCS#12	PKCS#12
Importation cer avec Kp	PKCS#12	PKCS#12	PKCS#12

Demande de certificat (3)

- **Processus de certification :**



Certificats X 509

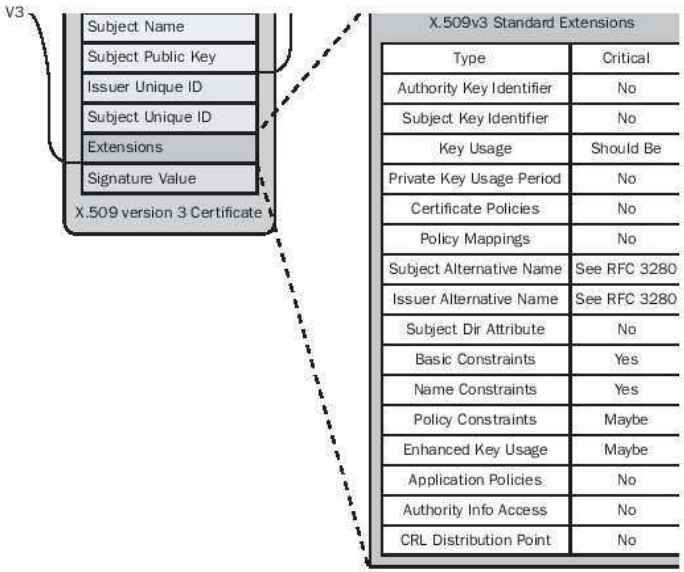
- **Objectif : Certifier qu'une clef publique appartient à une entité identifiée**
  - + durée de validité
  - + rôles et contraintes
- **Ensemble d'informations sur l'utilisateur (qq Ko) signé**
  - structure ASN.1 public signée
  - protégée en intégrité
  - encodage DER
- **Typiquement :**
  - Clef publique
  - Propriétaire de la clef : utilisateur, machine, serveur, équipement réseau...
    - qui possède la clef privée
  - Durée de validité
  - Information sur la signature (signataire/émetteur, algorithme de signature)
  - la signature elle-même

Certificats : exemple

- **Structure du certificat X.509v3 (1996)**

Version du certificat
Numéro de série du certificat
Algo.de signature de l'AC
Nom de l'AC ayant délivré le certificat
Période de validité
Nom du propriétaire du certificat
Clé publique
Algo. à utiliser avec la clé publique
Identification de l'AC (opt)
Identification du propriétaire (opt)
Extensions (opt)
Signature de l'AC

Certificats : exemple



Certificats : exemple

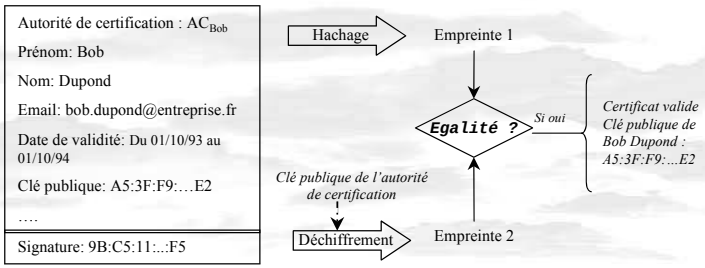
```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=FR, ST=IdF, L=Paris, O=Test, OU=IT, CN=ca/emailAddress=ca@test.fr
    Validity
      Not Before: Dec  7 19:47:52 2004 GMT
      Not After : Dec  7 19:47:52 2005 GMT
    Subject: C=FR, ST=IdF, O=Test, OU=IT, CN=pierre/emailAddress=pierre@test.fr
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:aa:90:7b:cb:dc:66:3c:8c:19:6e:01:29:95:f6:
          ...
          84:2b:b5:05:c9:ae:c5:3e:15
        Exponent: 65537 (0x10001)
```


Certificats : exemple

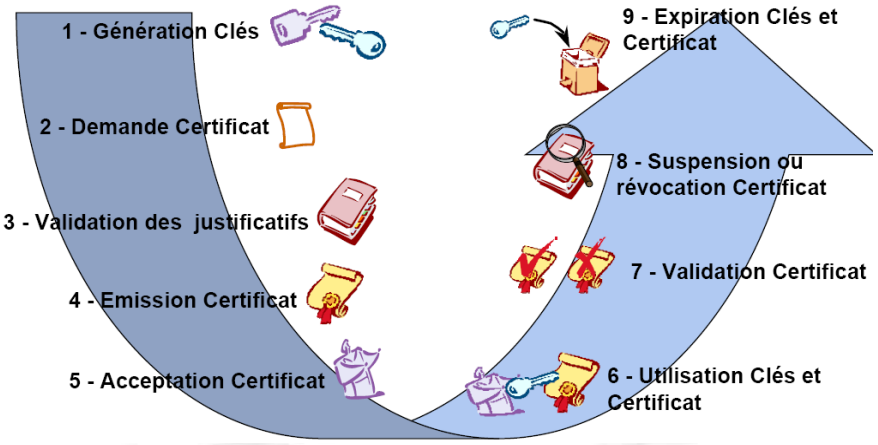
```
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment
      Netscape Comment:
        OpenSSL Generated Certificate
      X509v3 Subject Key Identifier:
        09:67:DD:9A:41:42:54:64:94:E7:78:99:03:7D:B5:3C:0F:6C:A8:31
      X509v3 Authority Key Identifier:
        keyid:AC:7D:85:4A:06:1F:65:1D:CF:C2:9B:31:73:DA:28:71:06:52:51:A0
        DirName:/C=FR/ST=IdF/L=Paris/O=Test/OU=IT/CN=ca/emailAddress=ca@test.fr
        serial:87:D0:28:56:B2:27:C5:B8

      X509v3 Subject Alternative Name:
        othername:<unsupported>
Signature Algorithm: md5WithRSAEncryption
  02:b3:2e:39:fd:61:41:7e:34:62:a5:f8:16:52:e7:1c:03:03:
```


Certificats : vérification

- **Vérification certificat**



Cycle de vie

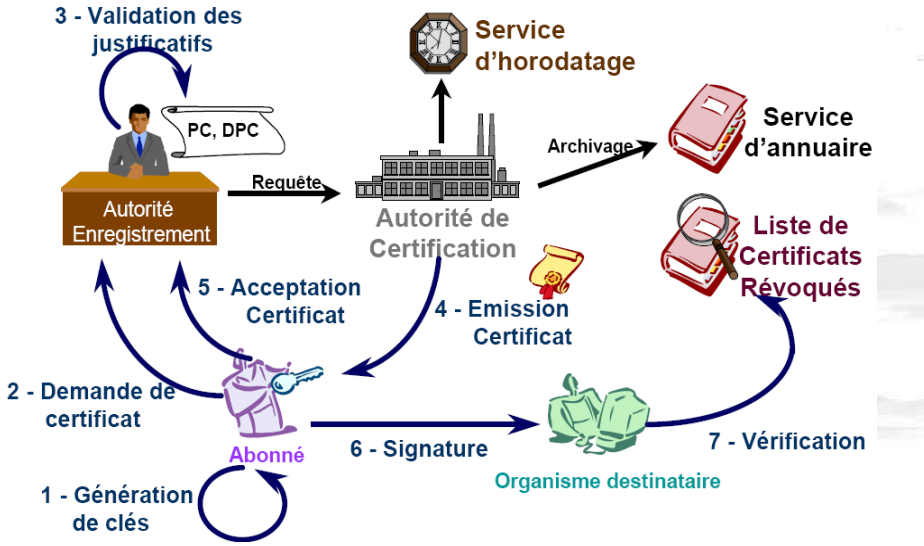


Infrastructure de gestion de clés

- **IGC ou PKI (*Public Key Infrastructure*) recouvre les services mis en œuvre pour assurer la gestion des clés publiques**
  - enregistrement des utilisateurs
  - vérification des attributs,
  - génération de certificats,
  - publication des certificats valides et révoqués,
  - identification et authentification des utilisateurs,
  - archivage des certificats, etc.

- **Composants fondamentaux d'une IGC**
  - Autorité de certification ;
  - Autorité d'enregistrement,
  - Service de publication ou autorité de validation ;
  - Annuaire qui contient les clés publiques, les certificats distribués, ainsi que les listes de certificats révoqués.

Etapes



Les acteurs de la certification

- **Le porteur**
  - Il est référencé par le certificat
  - Il est le seul à posséder la clé privée associée
- **L'utilisateur**
  - Il utilise le certificat
    - Il vérifie que l'identité indiquée par le certificat est bien son interlocuteur
    - Il vérifie que le certificat n'est pas révoqué (en consultant des listes de certificats révoqués - CRL)
    - Il vérifie que l'utilisation qu'il veut faire du certificat est conforme à son usage (chiffrement, signature, …)
    - authentifie et vérifie l'intégrité du certificat à l'aide de la clé publique de l'AC

- L'autorité de certification (AC)
  - Elle émet le certificat
  - Elle a la confiance des utilisateur
  - diffuse la valeur de sa clé publique auprès des structures qu'elle connaît et des annuaires (e.g., LDAP « Light Directory Access Protocol ») ;
  - Elle peut optionnellement créer des clés

Les acteurs de la certification

- L'autorité d'enregistrement (AE)
  - Elle dépend de l'AC
  - Elle s'occupe des aspects administratifs :
    - réception utilisateurs
    - Vérification de l'identité du demandeur
    - Vérification que le demandeur est habilité à recevoir les droits indiqués dans le certificat
    - s'assure que celui-ci possède bien un couple de clés privée-publique,
    - Obtention la clé publique
    - Transmission de la demande à l'AC
    - Traitement les demandes de révocation, suspension ou activitation d 'un certificat
  - L'AE est le point faible du système (affaire Microsoft/Verisign)

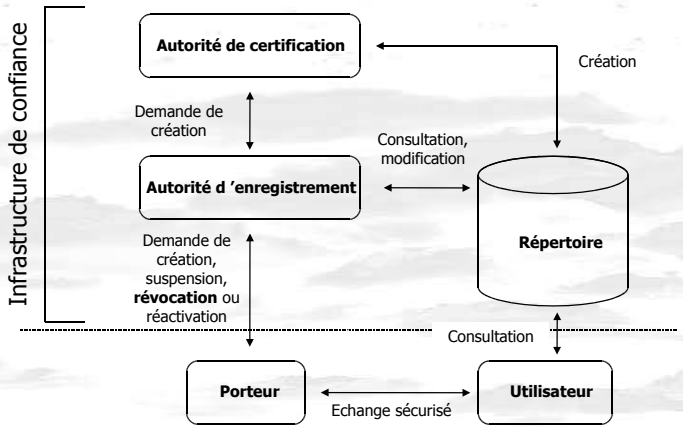
Les acteurs de la certification

- **En janvier 2001, Verisign a délivré deux certificats à la société Microsoft ... mais le porteur du certificat n'était pas affilié à Microsoft http://www.amug.org/~glguerin/opinion/revocation.html**
- **Verisign, suite à un audit de sécurité (6 semaines après), annonce que les deux certificats sont révoqués**
- **Microsoft publie un patch pour ne plus accepter ces certificats**

Les acteurs de la certification

- **Le service de publication**
  - **Publie**
    - les certificats
    - les CRL
  - **Disponible à tous ceux qui font confiance à l'AC**
  - **Contraintes sur ce service:**
    - à jour
    - disponible
    - intègre
  - **Protocole privilégié : LDAP**
  - **Protocoles spécifiques en cours de définitions**
    - Online Certificate status Protocol – OCSP
    - Simple Certificate Validation Protocol

Les acteurs de la certification



Autres composants

- **Autorité d'horodatage (TA Timestamping Authority) – RFC 3161**
  - Fournit un service de datation certifiée
  - Empêche les signatures antidatées
    - Même pour un certificat révoqué, une signature antérieure à la révocation reste valide
- **Service de séquestre**
  - Conservation des clefs privées de chiffrement
  - Sécurisé!!
- **Générateur de bi-clef (KGS, Key Generator System)**
  - contraintes cryptographique et de performance
  - Centralisé vs décentralisé
- ***L'autorité d'approbation des politiques***
  - spécifie règles selon lesquelles l'AC est autorisée à délivrer des certs
- ***Autorité d'attributs***
  - délivre des « sous-certificats » temporaires (comme par exemple des délégation de signature)

Les étapes de la certification

- **L'utilisation du certificat**
  - L'étape la plus importante dans l'utilisation du certificat est sa validation
    - Vérification de l'intégrité du certificat
      - Chaque certificat est signé par l'AC
      - Chaque AC possède donc un certificat appelé certificat racine et qui est « bien connu »
        - » Il faut vérifier le certificat racine également (peut impliquer *n* étapes si le certificat racine appartient à une AC fililale)
    - Vérification de la validité du certificat
      - certificat n'a pas expiré
      - certificat n'a pas été révoqué
      - On peut faire appel à une service de validation pour simplifier le travail
    - Vérification de l'adéquation d'usage du certificat
  - Note : tous les logiciels ne mettent pas en œuvre l'entièreté de ces étapes !!!

Les étapes de la certification

- **La révocation du certificat**
  - Un certificat est révoqué car :
    - Il a expiré
    - Les clés secrètes ont été perdues ou compromises
    - Le porteur à fait un usage illégal du certificat
    - Il est non valide
  - Chaque AC publie *périodiquement* une liste des certificats révoqués (CRL)
  - Cette liste pouvant être volumineuse, on procède
    - En publiant des delta (modifications incrémentales)
    - En découpant la CRL en partition. Chaque certificat contient un pointeur vers la partition où il devrait se trouver

Les étapes de la certification

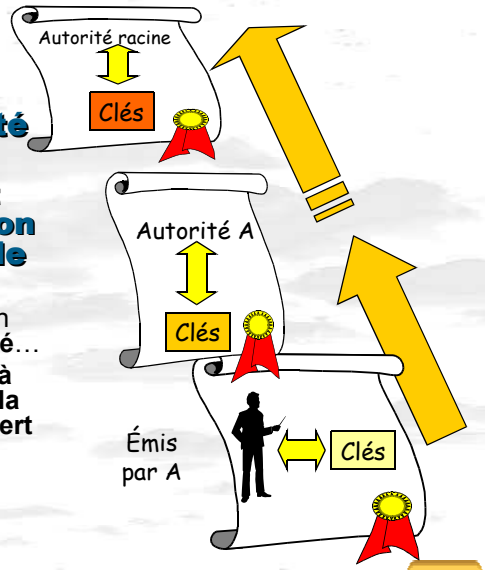
- **La révocation du certificat**
  - La CRL peut être obtenue,
    - A partir d'un URL accessible publiquement (et bien connue)
      Ex : http://crl.verisign.com/Class3SoftwarePublishers.crl
    - Manuellement (en téléchargeant une liste des certificats révoqués)
    - A partir d'une URL contenue dans le certificat racine (celui de l'AC)
    - A partir d'une URL contenue dans le certificat
  - La polémique de l'affaire Microsoft/Verisign porte sur l'absence d'une infrastructure de révocation

Organisation des PKI

- **le certificat ne peut garantir seul la validité d'une transaction, le sérieux de la PKI ayant délivré le certificat est important également**
- **Etant donné qu'il n'existe pas qu'une seule PKI, il arrive un moment ou une relation de confiance doit être établie entre les intervenants dépendant de plusieurs PKI**

Chaîne de certification (5)

- **La confiance est déplacée vers l'autorité de certification**
- **Des autorités peuvent en certifier d'autres : on aboutit à une chaîne de certification**
  - à la racine, on a forcément un certificat "*racine*" **auto-certifié**…
  - **si on ne fait pas confiance à cette autorité racine, toute la chaîne de certification ne sert à rien**
  - généralement, il s'agit d'une organisation très réputée

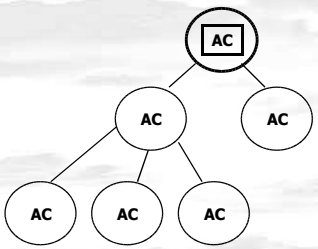


Organisation des PKI

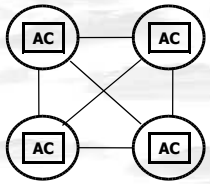
- **En fonction du nombre et de la nature des intervenants, on parle de modèle de confiance à 1,2,3,4 ou 5 coins**
- **Modèle à un coin**
  - Une entreprise émet des certificats pour ses employés.
    - modèle à un coin : employés et E/se sont considérés comme une même entité juridique
- **Modèle à deux coins**
  - Une entreprise (ex: une banque) émet des certificats pour ses clients et fournit un logiciel sécurisé par lequel passent toutes les transactions
- **Modèle à trois coins**
  - Une entreprise émet des certificats pour ses clients, mais n'est pas l'intermédiaire de toutes les transactions
- **Modèle à quatre coins**
  - Deux clients effectuent des transactions ensemble et chacun dispose de sa PKI.
    - Il existe relation confiance entre les PKI impliquées
- **Modèle à cinq coins**
  - Deux clients effectuent des transactions ensemble et chacun dispose de sa PKI. Les deux PKI appartiennent à un réseau fédérateur de PKI

Organisation des PKI

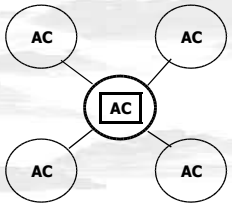
- **les AC peuvent être organisées de manière hiérarchique. Plusieurs organisations sont possibles :**
  - Organisation arborescente
  - Organisation en maillage
  - Organisation en étoile (avec point focal)



Arborescente



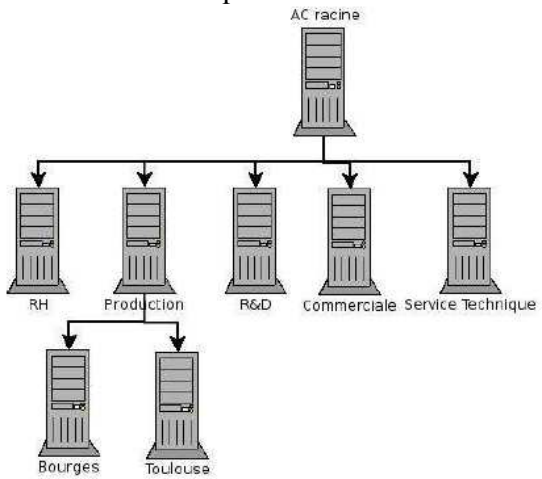
Maillage



En étoile

Organisation des PKI

Exemple : IGC hierarchique



Politique de certification

- ensemble de règles identifié par un nom, qui fournit un renseignement sur la possibilité d'utiliser un certificat pour une communauté particulière ou des applications ayant des besoins de sécurité communs
  - Spécifie les conditions de délivrance d'un certificat
  - Les limitations appliquées en fonction
    - de son usage
    - de sa validité
    - de son renouvellement
  - La PC doit être connue et acceptée par tous les utilisateurs
    - Un certificat doit contenir un identificateur de sa PC
    - Peut être déposée auprès d'un organisme international
- Ex : Procédures et Politiques de Certification de Clés . DCSSI
- X.509 Certificate Policy for the US Department of Defense (class 2 à 5 ...)

Politique de certification

- qu'est ce qui peut être sécurisé par ces certificats
- Niveau de protection des clefs privées
- Types de mesures prises pour valider l'identité d'une personne demandant un certificat
- Responsabilités du propriétaire en cas de compromission de la clef privée
- RFC 2196 - Site Security Handbook
- ISO/IEC 17799:2000 Code of practice for information security management

Sécurité physique, organisationnelle, du personnel, contre les sinistres, contrôle d'accès, ...

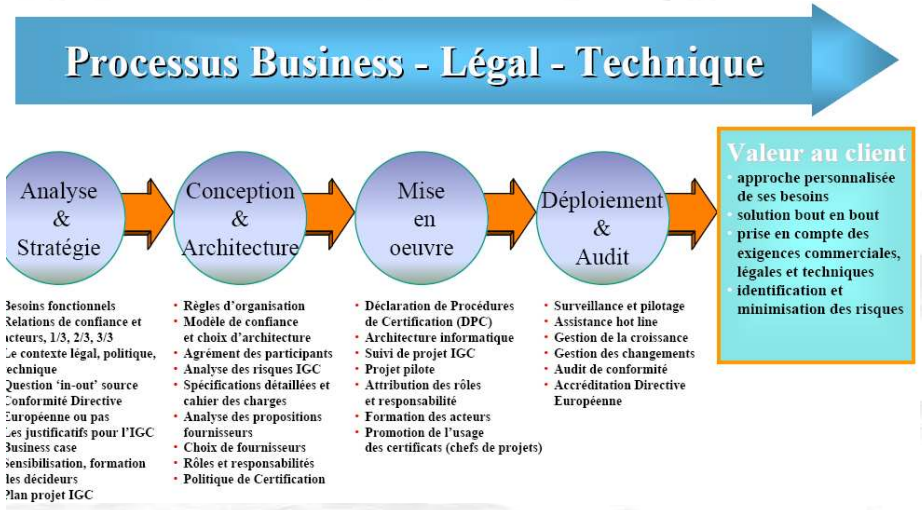
Declaration pratiques de certification

- **Énoncé des pratiques de certification effectivement mises en oeuvre par une** autorité de certification pour émettre et gérer des certificats.
- **Détaille les moyens mise en oeuvre pour atteindre le niveau de sécurité décrit dans le PC**
  - comment est validée l'identité des demandeurs de certificat
  - les utilisations prévues et définies dans les certificats
  - montant maximum des transactions protégées par ces certificats
  - coût des certificats
  - procédure d'audit
  - juridiction / lois applicables
- **Des DPC différentes peuvent répondre à une même PC**
- **Une même DPC peut être utilisée pour deux PC différentes**
  - conforme à la PC la plus exigeante

Declaration pratiques de certification

- **RFC 2527 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**
- propose un plan pour les DPC
  - Introduction
  - General provisions
  - Identification and authentication
  - Physical, Procedural and Personel Security controls
  - Technical Security controls
  - Certificate and Certificate Revocation List Profiles
  - Specification Administration
- **Ces documents sont nécessaires pour déterminer si l'autorité de certification d'une organisation peut être jugée de confiance**

Plan de déploiement d'une PKI



Analyse & stratégie

- Analyser des besoins métier en coordination avec le plan stratégique de l'organisation
  - Analyse de l'existant
  - Processus business
  - Cartographie des applications concernées
  - Topologie réseau et localisation
  - Architecture sécurité existante
- Définir les besoins spécifiques
  - Web, messagerie, VPN, e-Commerce, etc..
- Définir les modèles de confiance
  - Modèles de 1 à 4 coins

Analyse & stratégie

- Analyse et décision de dvpmt interne ou d'externalisation
  - Intégration des facteurs réglementaires ou politiques
  - Intégration des impacts opérationnels d'une exploitation interne
  - Choix produits sur étagère ou développement open source
  - Étude de coût et de risques
- Spécifications fonctionnelles et techniques de haut niveau de l'IGC
  - Localisation de l'AC (Racine ou intermédiaire)
  - Organisation des AE
  - Relations possibles avec d'autres domaines de confiance
  - Supports de clés de l'utilisateur final
- Établir la valeur de l'information et analyser les risques associés
- Plan d'affaires et décision de lancement du projet
  - Retour sur investissement direct ou indirect
  - Planification du projet

Conception & architecture

- Définition des rôles et responsabilités
  - Comité d'approbation des politiques
  - Agents des AE
  - Équipe opérationnelle de l'AC et autres composantes
  - Responsables sécurité (RS) /auditeurs
- Spécifications fonctionnelles et techniques détaillées
  - Obtention d'informations des fournisseurs IGC
  - Détail des exigences en vue de la rédaction d'un cahier des charges (crypto, délais, supports, etc.)
- Définition/rédaction de la Politique de Certification
- Formalisation des facteurs de changements internes
  - À court terme : organisation
  - À moyen et long terme : impact sur les applications

Conception & architecture

- Rédaction / émission du cahier des charges
  - Fournisseur des composants IGC: AE, AC, horodatage, service de publication, etc..
  - Fournisseur de solution poste client: outil de signature, validation de signature, chiffrement
  - Fournisseur d'un support des secrets: carte à puce, token USB
  - Fournisseur d'un système de validation des applications
- Sélection des fournisseurs
  - Définition des critères d'évaluation des fournisseurs
  - besoins exprimés / caractéristiques produits
  - Évaluation des propositions par rapport aux besoins
  - Établissement d'une liste réduite / Négociation contractuelle
  - Choix du (des) fournisseur(s)
  - Processus administratifs de contrat et notification

Mise en oeuvre

- Plan de développement
  - Mise en place de l'équipe projet
    - Maîtrise d'ouvrage: Directeur de projet, chef de projet, juristes, ...
    - responsable des TI (exploitation), marketing, etc..
    - Maîtrise d'oeuvre: unique ou multiple
  - Suivi de projet
    - Planification : tâches, Gantt, délais, ressources, budgets, etc..
    - Suivi opérationnel: comités/réunions d'avancement, tableaux de bord
    - Livraison des produits (services): recettes unitaires
    - Travaux d'infrastructure physique (si interne)
    - Formation (opérateurs et utilisateurs finals)
    - Contrôle qualité
- Déclaration des pratiques de certification
- Contractualisation
  - Contrats avec les abonnés et autres acteurs
  - Contrats d'assurance / couverture du risque
  - Contrat de services si externalisation
- Plan de recette

Mise en oeuvre

- Mise en place d'un pilote
  - Choix des acteurs impliqués
  - Mise en place d'un support téléphonique (centre d'appel, web)
  - Suivi de mise en oeuvre : retour d'expériences sur le pilote et adaptation
- Actions marketing de promotion des services
  - En externe: vers les utilisateurs finals
  - En interne: vers les chefs de projets pour promouvoir l'utilisation des certificats dans les nouvelles applications

Deploiement & Audit

- Déploiement
  - Gestion de la croissance: montée en charge
  - Maintenance
  - Retour d'expérience sur le déploiement et adaptations
- Surveillance et pilotage
  - Procédures d'alertes
  - Gestion des incidents
  - Plan de secours / recouvrement
- Gestion des changements
  - Du système technique: nouvelles versions du système
  - Des documents de politique: PC, OID des certificats, etc.
  - Évolution de l'architecture
    - Ajout d'AC filles
    - Croisements avec d'autres IGC

Audit

- Audit de type conformité / qualité
  - Conformité de la DPC aux exigences de la PC
- Qualification au titre de l'article 7 de la loi du 30 mars 2001
  - relatif à la signature électronique,
  - procédure d'accréditation des organismes et la procédure d'évaluation et de qualification des prestataires de services de certification électronique.
- Contrôle DCSSI au titre de l'article 9 de de la loi du 30 mars 01
- « labellisation » au titre d'autres référentiels
  - FNTC (Fédération Nationale des Tiers de Confiance)
  - WebTrust pour autorités de certification
  - ISO 17799 (norme internationale concernant la sécurité, 12/00)

Critiques

- **Après une période d'euphorie (commerciale)**
- **les IGC ont essuyé beaucoup de critiques au début des années 2000**
- **Compilation of Resources Regarding Difficulty With PKI:**
  - « What you are not being told about PKI », B. Schneier, G. Ellisson
  - « The fundamental inadequacies of conventional PKI », R. Clarke
  - « Only mostly dead : PKI, Why a security plateform never took off », S. Berinato

PKI is dead. Mercifully. PKI arrived as a gimpy pony in the first place, and by now we are pretty tired of beating a dead horse.

- « 2002 will be the year that PKI dies », G. Schultz
- « Les IGC : Faut-il tempérer les enthousiasmes? » S. Aumont

Critiques

- **Critères de validité d'un certificat**
  - Propriétés d'un certificat valide :
    - Certificat émis par une AC à qui on fait confiance
    - Avec un usage du certificat défini et adapté à l'application
    - Possédant des dates d'utilisation valides
    - Et n'étant pas révoqué
- **Nombre de vérifications sont de la responsabilité du client**
- Problème d'implémentation:
  - Tout certificat émis par une AC à laquelle ont fait confiance est pris en compte par le client
  - Tout certificat émis par une sous-AC d'une AC à laquelle ont fait confiance est pris en compte par le client si les options de certificat sont correctes
  - Tous les usages définis dans le certificat sont considérés comme valables même s'ils sont incohérents

Critiques

- **Problème de confiance: Une IGC implique la confiance dans des AC**
  - Certains clients arrivent avec une liste de AC prédéfinie
    - Mais que faut il comprendre lorsqu'une CA est dite « digne de confiance »?
    - Qui a accordé à une CA le pouvoir d'attribuer de telles preuves d'identité ?
  - L'utilisateur doit valider le certificat :
    - Certains critères sont délicats à appréhender
      - Extensions X.509, PC, DPC...
    - les certificats nous protègent uniquement contre les partenaires avec lesquels le client refuse de travailler.
    - Vu leur nombre, ces AC ont forcement des PC différentes
      - Différence non prise en compte dans les clients : aucune pondération
    - Installation d'AC par inadvertance est possible
    - Attaque du stockage de ces AC
  - Exercice : Essayez de supprimer une AC dans mozilla

Critiques

- **Problème de confiance: la révocation de certificat**
  - service essentiel ... rarement utilisé !
- **Le principe d'une CRL**
  - Principe de fonctionnement : Dés que l'on sait sa clef compromise (volée, perdue physiquement, ...) on la met sur une CRL
  - Approche : tant qu'on est pas sûr qu'un certificat est compromis ... on peut s'en servir
- **Diminution de la fenêtre de vulnérabilité**
  - Dépend de 3 facteurs
    - La capacité à détecter la compromission d'une clef
    - La réactivité de l'IGC
    - La diffusion de la révocation et sa prise en compte par les applications
      - Mises à jour « régulières » de CRL

Critiques

- **Problème de confiance: le secret de la clef secrète**
  - la sécurité des clefs logicielles dépend de la sécurité des machines qui les stockent
  - Elles sont chiffrées! Oui mais
    - le mot de passe lui-même peut être volé
    - Des attaques par dictionnaire
      - La plupart des logiciels n'imposent pas de règle de constitution
  - En général, non chiffrée pour les clefs associées à un service
  - Utilisation de cartes cryptographiques
    - carte à puce ou token USB pour les utilisateurs
    - HSM (Hardware Security Module) pour les serveurs
    - Les clefs peuvent être générées par la carte
      - à aucun moment la clef privée ne sort de la carte
      - seuls la clef publique et les résultats des calculs cryptographiques sont fournis par la carte

Critiques

- **Difficultés d'exploitation d'une IGC**
  - En général, engagement à (très) long terme
  - Conformité à la PC
    - application de la DPC
      - Notamment des règles organisationnelles
      - Recouvrement de clef collaboratif
  - la difficulté de changement du certificat d'un AC racine
    - validité très longue
      - ex : RSA Security Inc : 2001-> 2026
    - Choisir une longueur de clef suffisante
    - Faire évoluer la PC et la DPC

Vulnérabilités

- **La façon dont Konqueror manipule les certificats électroniques permet à un attaquant distant de mener une attaque de type "Man in the Middle".**
  - Konqueror est un outil développé pour l'environnement graphique KDE, qui fait à la fois office de navigateur web et de gestionnaire de fichiers.
  - Konqueror possède sa propre implémentation de SSL.
    - SSL utilise des certificats.
    - pour authentifier un correspondant, Konqueror se base sur l'@ IP fournie par le certificat et non pas sur le nom de la machine.
    - Un attaquant peut donc se placer entre deux personnes désirant communiquer et intercepter de façon transparente les données échangées.

Biblio

1. Cryptographie Appliquée, Bruce Schneier (Wiley), 1996, ISBN 0-471-59756-2 (ISBN 2-84180-036-9 en VF)
2. MISC 15, septembre/octobre 2004, dossier « Authentification »
3. ITU-T Recommendation X.208, « Specification of Abstract Syntax Notation One»
4. http://asn1.elibel.tm.fr/fr/utilisations/rfc.htm
5. http://sourceforge.net/projects/asn1c/
6. ITU-T Recommendation X.690, « ASN.1 : Encoding Rules »
7. MISC 13, mai/juin 2004, dossier « PKI »
8. http://www.securityfocus.com/infocus/1810
9. RFC 3280 – Internet X.509 PKI Certificate and Certificate Revocation List profile
10. RFC 3161 - Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP)
11. RFC 3647 - Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework
12. PC2 – Procédures et Politiques de Certification de Clés . DCSSI

Conclusion

	Intégrité	Authenticité	Non répudiation
Empreinte digitale			
MAC		Voir note 1	
Signature digitale		Voir note 2	
Signature digitale + certificat			Voir note 3

A retenir

Note 1. Impossible d'identifier précisément l'émetteur si la clé secrète est partagée entre plusieurs personnes.

Note 2. On garantit que l'émetteur possède la clé privée, mais pas l'identité effective de l'émetteur.

Note 3. Ne pas oublier de vérifier la validité (date, répudiation…) du certificat.

Références (authentification)

- **Généralités sur l'authentification**
  - Site de MSI S.A. http://shl.msi-sa.fr
  - FAQ R.S.A http://www.rsasecurity.com/rsalabs/faq/
  - FAQ des news sci.crypt
- **Signatures digitales, certificats**
  - Site de Verisign http://digitalid.verisign.com/client/help/technical.htm
  - Site de Thawte http://www.thawte.com
- **Algorithmes**
  - "*The MD5 Message Digest Algorithm*" de R. Rivest - RFC 1321
  - "*Secure Hashing Standard*" - FIPS 180-1
  - "*Handbook of applied cryptography*" de A. Menezes, P. van Oorschot et S. Vanstone

Résumé: Utilités la sécurité à tous les niveaux