Présentation:

- Pascal PETIT
- enseignements:
  - sécurité
  - administration système windows
- pascal.petit@shayol.org
- tel.: 01 60 87 39 XX (peu fiable)

Plan

- grands principes et gestion
  - principes de sécurité: définition des notions fondamentales
  - stratégie de sécurité
  - politique de sécurité

Plan (suite)

- éléments techniques
  - chiffrement
  - authentification
  - sécurité des réseaux : Intranet: risques
  - sécurité des réseaux : Contrôler l'accès au réseau (NAC)
  - sécurité des réseaux: pare-feu et détection d'intrusion
  - supervision de la sécurité
  - validation de la sécurité: audit et tests d'intrusion
  - réaction à une intrusion

I Principes de sécurités

- Critères fondamentaux
- domaines d'application de la sécurité
- multiples facettes de la sécurité

Critères fondamentaux

- disponibilité
- intégrité
- confidentialité
- authentification
- non répudiation

Disponibilité

- disponibilité d'une ressource: la ressource est disponible et accessible avec des temps de réponse acceptables
- s'obtient par :
  - dimensionnement approprié et redondance des éléments constitutifs;
  - gestion opérationnelle des ressources et des services
    - exemple: pour un réseau: dimensionnement correct des liens, des matériels actifs et politique de gestion et de routage satisfaisante

Disponibilité (2)

- test de montée en charge
- respect de clause d'engagement de service : indicateurs dédiés à la mesure de la continuité de service
- perte de données
  - sauvegardes
  - procédure de restauration
  - politique de sauvegarde
  - arbitrage entre coût de la sauvegarde et risque d'indisponibilité (ex.: incendie du CL)

Intégrité

- certifier que les données n'ont pas été altérées de façon intentionnelle ou accidentelle
- la modification peut avoir lieu
  - lors du transfert des données (corruption, écoute active)
  - lors du stockage des données
  - lors de leur traitement (bogues des logiciels applicatifs, des OS).
- Implications:
  - légales, plantage des applications et perte d'activité
  - perte d'image

Confidentialité

- protection des données contre une divulgation non autorisée
- 2 moyens techniques complémentaires
  - protéger l'accès aux données
  - les chiffrer
- intégrité, confidentialité : des contraintes opposées
  - intégrité : mutiplier les sauvegardes notamment hors site
  - confidentialité: limiter les lieux de stockage pour faciliter le contrôle d'accès

Identification et authentification

- **identification**: définir l'identité de l'utilisateur
- **authentification**: permet de vérifier l'identité fournie (authentification simple vs authentification forte)
  - via un élément que l'utilisateur connait (mot de passe, ...)
  - via un élément que l'utilisateur possède (carte à puce, certificat, ...)
  - via biometrie

authentification

- élément clef pour assurer :
  - la confidentialité et l'intégrité des données via un contrôle d'accès: seules les personnes identifiées, authentifiées et habilités à le faire peuvent accèder/modifier les données
  - la non-répudiation et l'imputabilité (preuve d'une transaction, ...)
- Authentification unique (SSO: Single Sign On)
  - l'utilisateur s'authentifie une fois
  - il a accès à toutes les ressources du réseau
  - cf partie technique (keberos, ...)

non répudiation

- **non répudiation** : ne pouvoir nier qu'un événement a eu lieu
- **imputabilité**: on sait qui a réalisé une action
- **traçabilité**: mémoriser des événements imputables
- **auditabilité**: pouvoir réaliser une analyse ultérieure d'un événement. Ex.: en cas d'intrusion.
- moyens: utilisation de journaux
  - de taille limitée
  - éventuellement hors site (intrusion)

Critères fondamentaux

- disponibilité
- intégrité
- confidentialité
- authentification
- non répudiation

Domaine d'application de la sécurité

- sécurité physique
- sécurité de l'exploitation
- sécurité logique
- sécurité applicative
- sécurité des télécommunications

sécurité physique

- maîtrise des systèmes et de leur environnement
- repose sur :
  - protection des sources énergétique (ex. de redbus)
  - protection de l'environnement (température, sinistre du type incendie, ...=
  - protection des accès physiques
  - sureté de fonctionnement et fiabilité des matériels
  - redondance physique
  - marquage des matériels
  - plan de maintenance préventive (test, ...) et corrective (pièce de rechanges, procédures, ...)

sécurité de l'exploitation

- tout ce qui touche au bon fonctionnement des systèmes
- points clefs
  - plan de sauvegarde,
  - plan de secours
  - plan de continuité
  - plan de test
  - inventaire régulier
  - gestion du parc
  - gestion des configurations et des mises à jour
  - gestion des incidents et suivi jusqu'à leur résolution
  - automatisation, contrôle et suivi de l'exploitation, supervision
  - analyse des journaux
  - gestion de la maintenance
  - environnement de test et de production séparés

sécurité logique

- mécanisme de contrôle d'accès aux données
- identification/authentification/autorisation
- cryptographie/mots de passe/authentification
- classifier les données pour qualifier leur sensibilité (publique, confidentielle, ...) et les droits d'accès correspondant

sécurité applicative

- fiabilité des logiciels pour assurer la continuité de service et l'absence de corruption des données
- repose sur :
  - méthodologie de développement
  - robustesse des applications
  - contrôles programmés, jeux de tests, procédures de recettes
  - sécurité des progiciels
  - élaboration des contrats (clause d'engagement de responsabilité)
  - validation et audit des programmes
  - qualité et pertinence des données
  - plan d'assurance sécurité (souvent une section du plan d'assurance qualité)
  - indépendance des fournisseurs (logiciel libre, travail en régie, développement local, ...)

sécurité des télécommunications

- offrir une connectivité fiable de bout en bout
- infrastructure réseau sécurisée au niveau:
  - des accès
  - des protocoles de communication
  - des systèmes d'exploitation
  - des équipements (redondance, boucles, ...)
- ex. de pb classiques:
  - la pelleteuse
  - bug sur un matériel actif
  - problème d'interopérabilité entre matériel actifs, logiciels, ...

Exercice (énoncé)

- dans une petite entreprise, l'ingénieur système a organisé les sauvegardes de la façon suivante :
  - les données sont sur les postes utilisateurs;
  - chaque poste utilisateur est muni d'un graveur de DVD qui contient un DVD RW
  - pour effectuer une sauvegardes, les utilisateurs
    - effacent le DVD-RW
    - créent un fichier .zip
    - le sauvent sur le DVD
- Que pensez-vous de cette procédure ?

Exercice (éléments suggérés par la salle)

- à saisir en direct sur la suggestion des étudiants

Exercice (éléments de correction)

- procédure non automatisée, intégralement manuelle reposant sur les utilisateurs
- quid d'un crash pendant la sauvegarde ?
- exhaustivité de la sauvegarde ? , évaluation des risques ?
- quid des tests ?
- quid de la procédure de restauration ?
- surveillance des sauvegardes (journaux)
- sauvegarde hors site ?
- confidentialité des sauvegardes en cas de vol ?
- quid du sav du matériel, procédure en cas de crash ?

facettes de la sécurité

- diriger la sécurité:
  - politique de sécurité
  - un ensemble de mesure techniques éparses ne doit pas se substituer à une gestion cohérente comprenant une évaluation des risques
- aspects juridiques:
  - responsabilité des autres vis à vis de nous (contrat, lois,
  - responsabilité lié au droit des nouvelles technologie (conservation des données, gestion des données personnelles, surveillance, propriété intellectuelle, délit de manquement à la sécurité, ...)

facettes de la sécurité (2)

- éthique et formation:
  - charte reconnue par tous
  - les signataires doivent avoir les moyens de l'appliquer
  - actions d'information et de formation
- architecture de la sécurité:
  - dimension techniques et opérationnelles
  - dimension humaine
  - dimension juridique et réglementaire
  - dimension organisationnelle et économique

II La stratégie de la sécurité

- évaluer les risques
- démarche sécuritaire
- stratégie de sécurité
- rapport coûts/bénéfices

Evaluer les risques

- but: garantir la pérennité de l'entreprise
- Comment: via une stratégie de sécurité :
  - en se protégeant
  - en organisation la défense
  - en élaborant des plans de réactions aux sinistres

Risque:

- danger plus ou moins prévisible
  - mesurer sa probabilité
  - mesurer les dommages consécutifs
- réagir en
  - réduisant sa probabilité à un niveau acceptable (?)
  - prévoir les mesures à prendre s'il se produit

Démarche sécuritaire

- étape 1 : mise en place d'une politique de sécurité
  - identifier les valeurs
  - identifier les risques qu'elles courrent
  - identifier les moyens et mesures de sécurité à mettre en oeuvre
- étape 2: mise en oeuvre des outils et des procédures
- étape 3: évaluer périodiquement l'adéquation et la cohérence des mesures de sécurité

stratégie de sécurité

- garantir les fondamentaux (intégrité, ...) à l'aide d'outil (coupe-feu, ... et de procédures de gestion)
- démarche globale de l'entreprise (buts, vocabulaire commun, cohérence des outils et procédures déployées, ...)
- portée par la direction de l'entreprise
- compromis entre coût/niveau de sécurité/impact sur le fonctionnement de l'entreprise

rapport coût/bénéfice

- perte de productivité
- perte de parts de marché
- pénalité de retard
- perte d'image vis à vis des clients/fournisseurs/...
- coût de gestion des sinistres (assurance, experts, investigation ...)
- frais de justice
- coût de la remise en état

III Politique de sécurité

IV partie technique

- préliminaire: chiffrement
  - chiffrement symétrique/asymétrique
  - PKI: infrastructure de clefs publiques
  - hachage
- Authentification
- sécurité des infrastructures de communication
- contrôle d'accès réseau
- supervision
- audit et tests d'intrusion
- réaction en cas d'intrusion

Chiffrement: robustesse

- cryptanalyse: analyser une information chiffrée pour la déchiffrer(dont méthodes en force brute, ...)
- algo public
- la sécurité repose sur :
  - la non divulgation de la clef
  - la robustesse de l'algorithme
  - la taille de la clef (gare aux comparaisons entre algo différents)
  - l'utilisation de clefs différentes pour chiffrer des messages différents limite la quantité d'information à la disposition de l'attaquant

chiffrement: taille des clefs

- attaques en force brute: tenter une partie importante de l'espace des clefs
- temps dépend du nombre de clefs possibles et donc de la taille de la clef:
  - 10 bits : 1024 clefs possibles
  - 56 bits: 2^56=7 10^16
  - dépendance exponentielle en fonction de la taille de la clef: 1 bit de plus = 2 fois plus de temps
- la taille critique dépend de l'algo (et de sa vitesse, de ses faiblesses, ...)

algorithme de chiffrement

- chiffrement symétrique/asymétrique
  - symétrique:
    - les algo classiques sont rapides
    - **la même clef sert au chiffrement et au déchiffrement**
    - souvent utilisé via une clef de session
      - clef de session: transmise via algo asymétrique (on parle d'enveloppe digitale)
      - session: chiffrée par un algo symétrique et la clef transmise

algorithme de chiffrement

- chiffrement symétrique/asymétrique
  - asymétrique:
    - les algo classiques sont lents
    - **couple de clef publique/clef privée**
      - clef publique: peut être connue de tous
      - clef privée: tenue cachées
      - ce qui est chiffré avec l'une ne peut être déchiffré qu'avec l'autre

algorithmes classiques

- symétriques:
  - DES (1976): standard américain (1977), clef de 56 bits sur des blocs de 64 bits. dépassé de nos jours.
  - triple DES (1978): variante, triple application de DES, clefs entre 128 et 192 bits sur des blocs de 64 bits.
  - RC2, RC4, RC5 (1994) et RC6:
  - IDEA (1992): clef 128 bits sur des blocs de 64 bits
  - blowfish: clef 32 à 448 bits sur des blocs de 64 bits. Algo très analysé,considéré comme solide. utilisation libre.
  - AES (1998): clefs 128, 192 ou 256 bits sur blocs de 128 bits. standard américain. utilisation libre.

algorithmes classiques

- asymétriques:
  - RSA s'appuyant sur la factorisation de nombres premiers
  - Diffie-Hellman et El Gamal s'appuyant sur le calcul des logarithmiques discrets
  - des algorithmes nouveaux s'appuyant sur les courbes elliptiques

durée de vie des clefs

- dépend de sa taille
- dépend de son taux d'utilisation
- dépend du contexte d'utilisation
- hiérarchie de clef (clef maîtresse, clef de session par ex.)
- révocation de clef
- une utilisation intensive du chiffrement nécessite la mise en place d'une IGC (infrastructure de gestion de clef ou PKI – Public Key Infrastructure en anglais)

hachage/ empreinte

- principe:
  - une fonction non réversible H:
    - connaissant H(x), il est très difficile de trouver y tel que H(y)=H(x)
  - telle que deux empreintes différentes correspondent forcément à deux textes différents
  - la probabilité d'avoir deux empreintes identique est très faible

hachage: applications

- authentification des utilisateurs:
  - on stocke la version hachée du mot de passe
  - un grain de sel permet d'éviter que deux personnes qui ont le même mot de passe aient la même empreinte
- copie optimisée de fichiers
- vérification de l'intégrité de fichiers

Hachage: algo classiques

- MD4 (mdp windows NT & Co)
- MD5 (mdp unix): empreinte de 128 bits, considéré comme faible (collisions)
- sha-1: empreintes de 160 bits (solidité mise en doute actuellement)
- sha-2: empr. de 256, 384 ou 512 bits au choix
- utilisation d'un algo de chiffrement: le mot de passe est transformé en clef pour chiffré un texte connu. ex. connu: DES modifié itéré 25 fois pour les mots de passe unix.

signature d'un message

- On considère l'algorithme de signature suivant :
  - chiffrer avec sa clef privée un message m contenant le texte « je m'appelle toto »
  - joindre le courrier en clair à ce message chiffrée et l'envoyer au destinataire
  - le destinataire peut lire le courrier et déchiffer la signature avec la clef publique de toto.
- citez les failles de cet algorithme
- proposez des solutions pour les combler

One Time passwd: une application amusante des algo d'empreintes

- Exercice.

services offerts par le chiffrement:

- confidentialité
- intégrité: chiffrer une empreinte du message
- signature numérique
- authentification (ex.: ssh qui authentifie les machines)
- kerberos: authentification centralisée unique
- non répudiation: prouver qui a créé un message: utilisation de tiers de confiance, chiffrement à clef publique

PKI: Public Key Infrastructure (IGC: Infrastructure de Gestion de Clefs)

- Problème:
  - comment être sur qu'une clef publique est valide et est bien la clef publique d'une personne donnée ?
- Solutions:
  - PGP: confiance transitive : WeB Of Trust
  - Certification par un tiers de confiance : IGC

IGC: définition

- IGC: ensemble de moyens matériels, de logiciels, de composants cryptographiques mis en oeuvre par des personnes, combinés par des politiques, des pratiques, des procédures requises qui permettent de :
  - créer
  - gérer
  - conserver
  - distribuer
  - révoquer

  des certificats basés sur la cryptographie asymétrique

éléments obligatoires d'une IGC

- 3 éléments obligatoires :
  - autorité de certification
  - autorité d'enregistrement
  - service de publication

•autorité de certification (CA ou Certification Authority en anglais)

- autorité de confiance reconnue par une communauté d'utilisateurs
- délivre et gère des certificats de clefs publiques
- maintient une liste des certificats révoqués (LCR en français, CRL en anglais)
- les certificats sont conformes à la norme X.509
- génère les certificats à clef publique et garantit l'intégrité et la véracité des informations qu'ils contiennent en les signant avec sa clef privée

•Autorité d'enregistrement (RA: Registry Authority)

- intermédiaire entre l'utilisateur et l'autorité de certification.
- l'utilisateur s'adresse à elle
- en application de la politique de certification, elle vérifie les données de l'utilisateur :
  - identité
  - correspondance clef privée/publique
  - ...
- transmet les informations validées à l'AC

•Service de publication

- met à la disposition de la communauté les certificats générés par l'AC
- publie aussi la liste des certificats révoqués

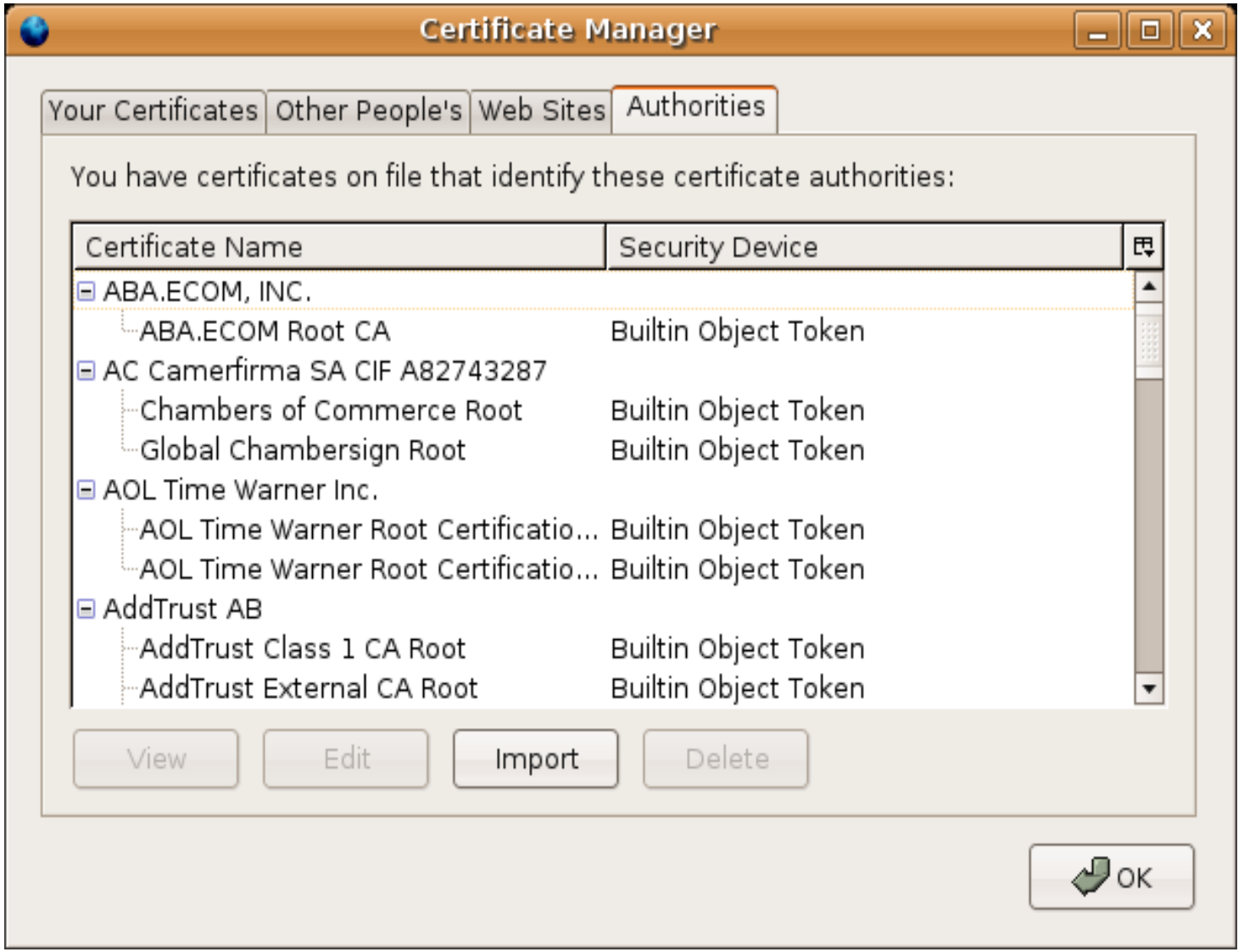
•Composants optionnels de l'IGC

- autorité d'horodatage (AH ou Timestamping Authority)
  - date des données qui lui sont transmises
  - Le Protocole D'horodatage (ou Time-Stamp Protocol) : rfc 3161
- service de séquestre:
  - stocke de façon sûre des clefs privées
  - pour permettre le déchiffrage des données en cas de perte
  - ne doit pas concerner les clefs de signature

•Certificat

- contient entre autre
  - l'identité de son propriétaire (personne, machine, ...)
  - sa clef publique signé par une AC
  - période de validité
  - type d'utilisation de la clef (champ optionnel)
  - ...

•Exemple: navigateur WeB

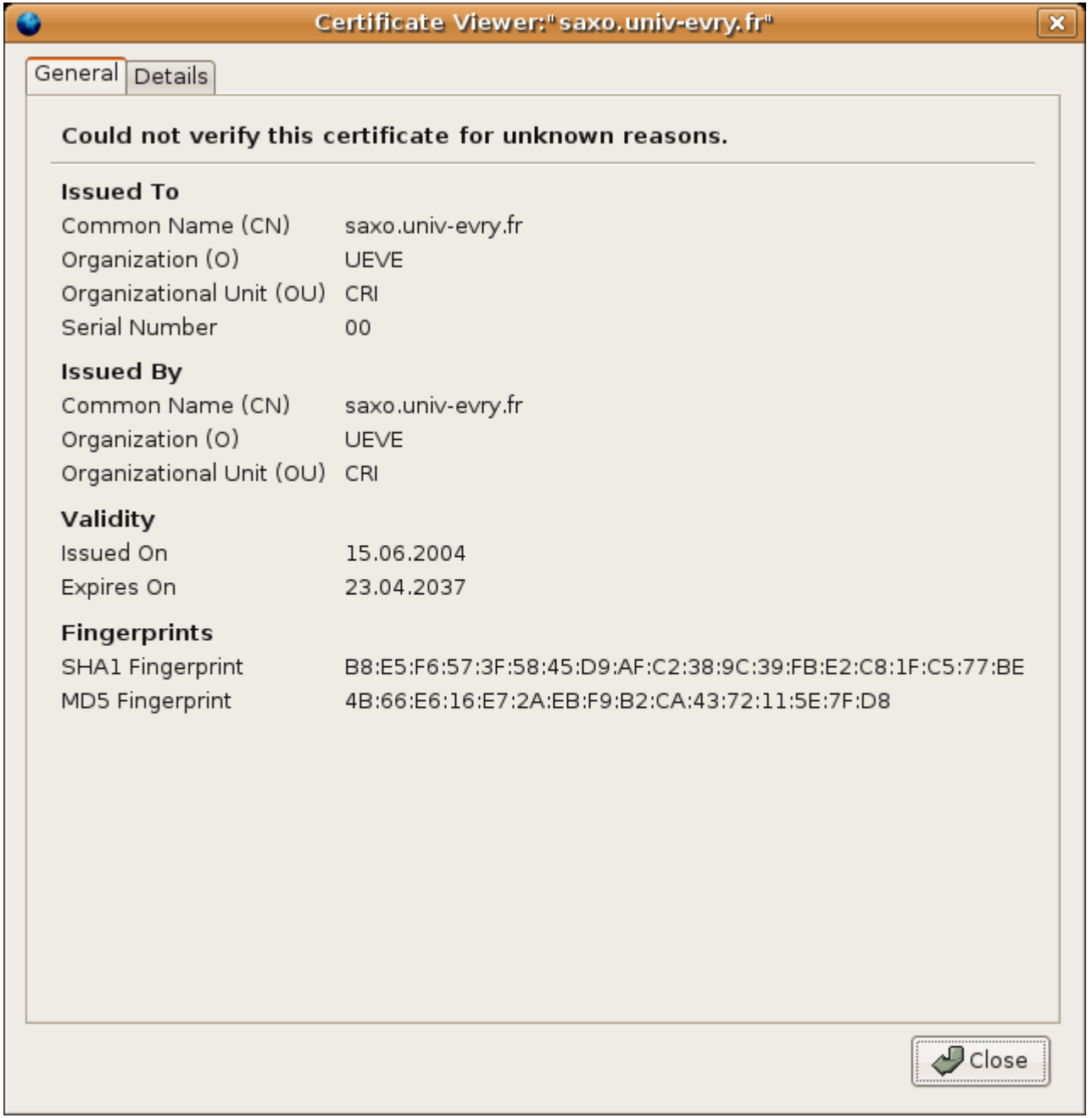


•Exemple: navigateur WeB:

- un client se connecte sur le site WeB de l'entreprise
- il obtient les références de l'AC et le certificat
- il vérifie le certificat
- il génère une clef de session qu'il transmet chiffrée au serveur de l'entreprise
- la session est maintenant chiffrée

•Exemple: Pb certification

•Exemple: certificat



Bibliographie:

- « méthodes de cassage des mots de passe » par D. Ducamp, 2005-2006, http://www.ossir.org/resist/supports/cr/20060530/mdp-RESIST-2006-05.pdf
- MISC No 13, mai-juin 2004: « PKI »
- « Sécurité informatique et réseaux » de S. Ghernaouti-Hélie, Dunod 2006