Protocole industriels de sécurité

S. Natkin

Décembre 2000

Standards cryptographiques

PKCS11 (Cryptographic Token Interface Standard)

- API de cryptographie développée par RSA labs, interface C
- Définit également un modèle de parallèlime des accés
- Et un modèle de protection d’accès aux fonction

- Notion de token (ressource cryptographique) qui est une implantation partielle ou totale de l’API
- Sur une même machine plusieurs token peuvent cohabiter
- L ’accès à une ressource nécessite une authentification pour une session de sécurité:anonyme, utilisateur référencé ou officier de sécurité (SO)

Les données peuvent être

- permanentes ou transitoires (durée de vie limitée à une session),
- publiques ou privées.

Cinq types de sessions

- : Lecture seule publique (R/O P),
- Lecture/ écriture publique (R/W P),
- Lecture seule utilisateur (R/O U),
- Lecture/ écriture utilisateur (R/W U),
- Administrateur (SO)

Matrice de protection

Type des données	Type de session				
	R/O P	**R/W P**	**R/O U**	**R/W U**	**SO**
Transitoires publiques	R/W	R/W	R/W	R/W	R/W
Transitoires privées			R/W	R/W	
Permanentes publiques	R/O	R/O	R/O	R/O	R/W
Permanentes privées			R/O	R/W	

Public Key Infrastructure (PKI)

Infrastructure à clefs publiques (PKI)
Fonctionnalités

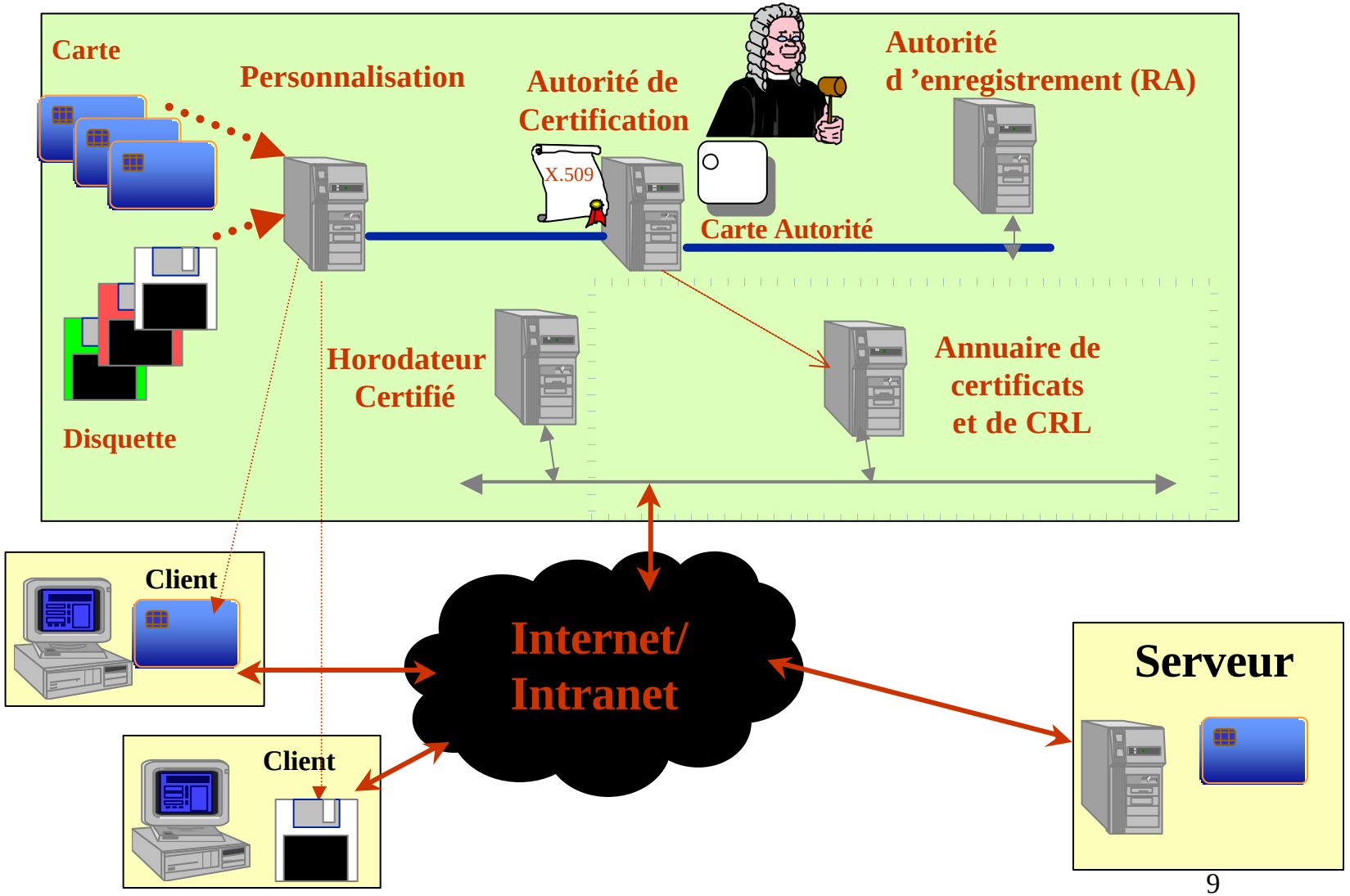
- Modules RA/LRA : Autorité d ’enregistrement locale des clients

  Elle enregistre la demande de certificat et les renseignements associés
- Module CA : Autorité de Certification

  Elle contrôle l ’identité du demandeur et génère le certificat, écrit dans l ’annuaire et la carte à puce, écrit dans la carte la clef privée
- Module DIR : Annuaire LDAPv3 de Netscape

  Sert à publier les certificats
- Module TTS : Horodateur sécurisé par carte
- Module PERS : personnalisation des dispositifs de sécurité utilisateurs : cartes à puce, disquettes

Fonctionnement des Infrastructures à clefs publiques(PKI)



MIME/SMIME

MIME : Du multimédia dans le courrier électronique

- SMTP (rfc822) : Protocole de messagerie année1982, Messages supportés : Entête puis texte en ASCII, limite de taille.
- MIME(Multipurpose Internet Mail Extensions): Définition d ’un nouveau format de message, supporte des types variés:
  - texte enrichi,
  - images,
  - sons…
  - Plusieurs parties de type différent (multipart)

MIME : Fonctionnement et exemple de message

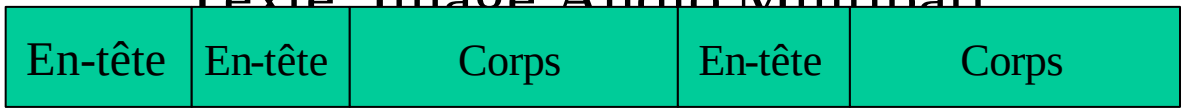
- Encodage des données 8bits:

  Quoted-printable (texte)

  Base64 (binaire)

- indication du type:

  Texte, Image, Audio, Multipart



Message mime Multipart (2 parties)

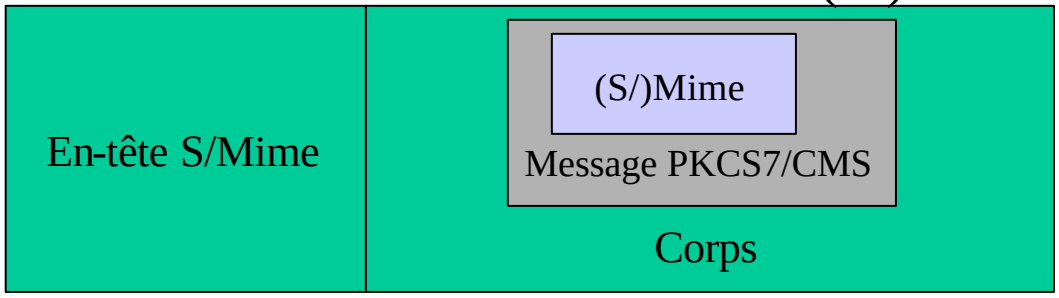
S/MIME : La sécurité dans MIME

- Introduction de nouveaux types:
  - Partie signée
  - Partie chiffrée
  - Partie composant la signature d ’un texte en clair
- La partie sécurisée est elle même une partie MIME (En tête+corps)
- Utilisation de standards imposés pour la représentation des types sécurisés
  - PKCS7 (S/Mime v2)

S/MIME : Fonctionnement et exemple de message

- Types : -application/pkcs7-mime
  -application/pkcs7-signature

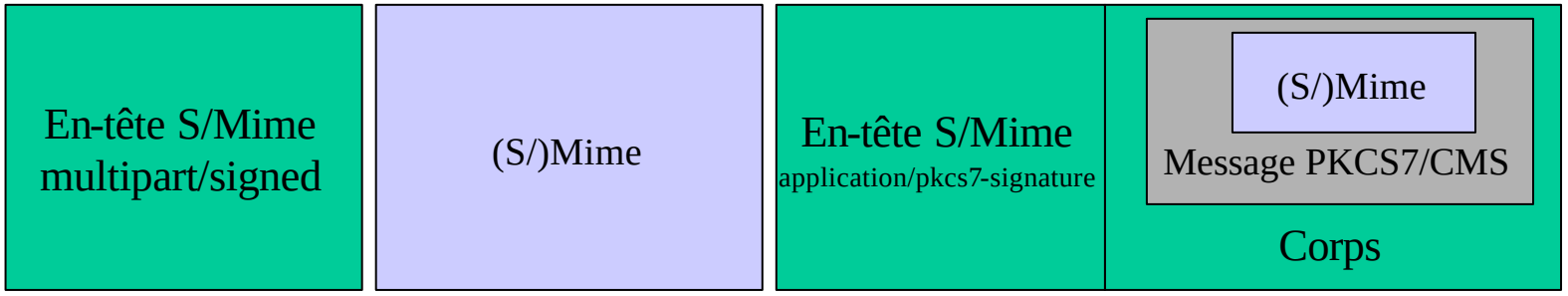
  encapsulation dans un message PKCS7/CMS de l ’entité (S/)Mime



- Processus d ’encapsulation répétable

S/MIME : Fonctionnement et exemple de message

- Types : multipart/signed
- message en 2 parties:
  1) entité (S/)Mime à signer
  2) signature de 1ere partie



- Avantage: compatibilité avec agents non S/Mime

Comparaison des 2 standards : PKCS7

- V1.5 Rfc2315 (Auteur : Rsa Labs)
- Un format indépendant : - du contenu à encapsuler - du mécanisme de transport
- Services cryptographiques
- Autres services: transport de certificat, horodatage,...

Confidentialité

EnvelopedData ::= SEQUENCE {
version **Version**,
recipientInfos **RecipientInfos**,
encryptedContentInfo **EncryptedContentInfo** }

Authentification, Intégrité, Non répudiation

SignedData ::= SEQUENCE {
version **Version**,
digestAlgorithms **DigestAlgorithmIdentifiers**,
contentInfo **ContentInfo**,
certificates [0] IMPLICIT **ExtendedCertificatesAndCertificates** OPTIONAL,
crls [1] IMPLICIT **CertificateRevocationLists** OPTIONAL,
signerInfos **SignerInfos** }

SSL/TLS

Service

- SSLV3.0 et TLS offrent des connexions asymétrique et possédant toutes les fonctionnalités des connexions TCP. Elles assurent en outre :

- Une authentification forte d'un ou des deux parties en utilisant un système de certification basé sur le RSA, Diffie Hellman ou le DSA. Le protocole ne précise rien sur la gestion des certificats proprement dite.

- Une protection contre les attaques d'interception: une fois la connexion établie l'échange est garanti se dérouler entre les parties authentifiées.

- Une protection en intégrité des messages et du flux de messages, par utilisation conjointe d'un numérotation des messages et une fonction de hachage sécurisée (basée sur le MD5 ou SHA1).

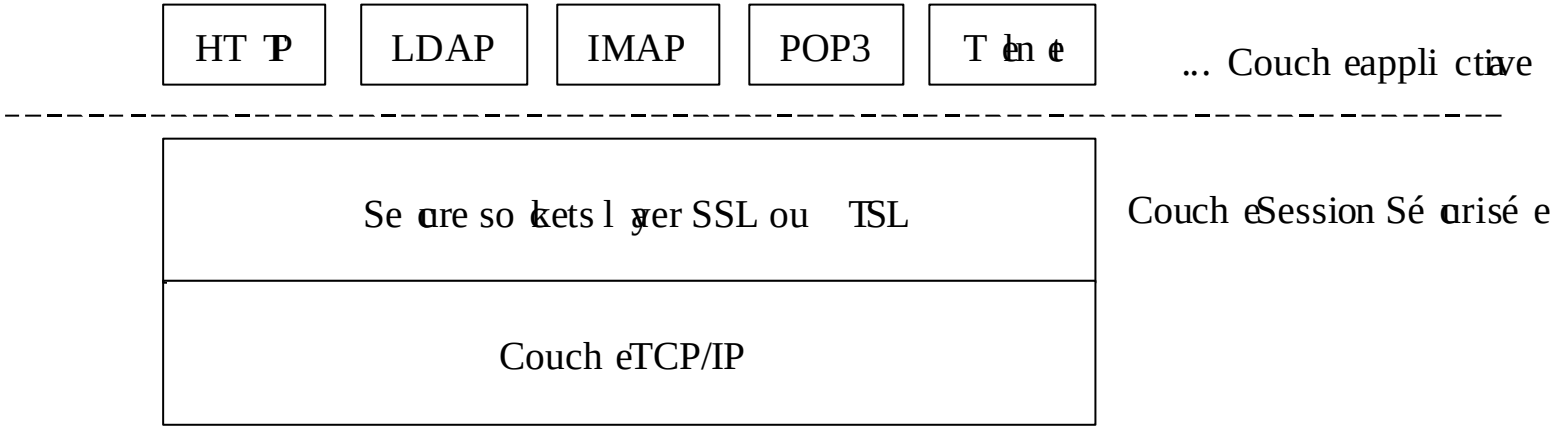
Service (2)

- Optionnellement la compression des données en utilisant tout algorithme de compression implanté de part et d'autre.

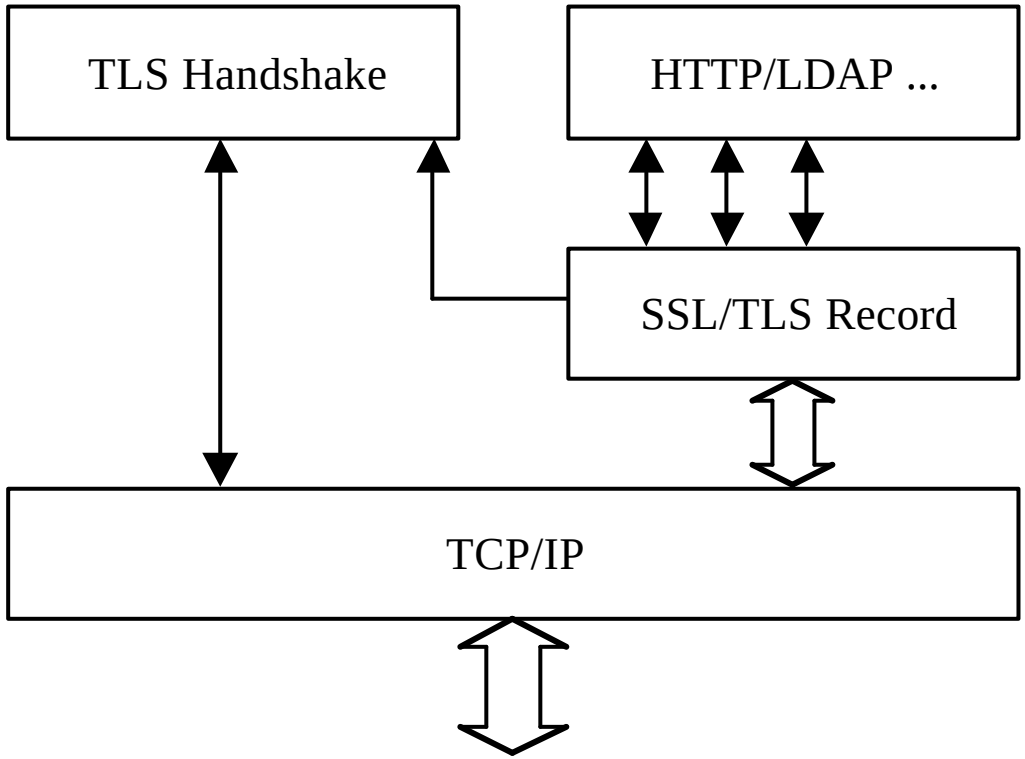
- Optionnellement une protection en confidentialité des données en utilisant tout algorithme cryptographique symétrique implanté de part et d'autre et une clef de session unique par connexion. La plus part des implantations supportent le DES, le 3DES (à clefs de 112 et 168 bits), le RC5.

- La suite cryptographique utilisée est négociée à l'ouverture de connexion.

Positionnement architectural



Architecture



TLS Handshake

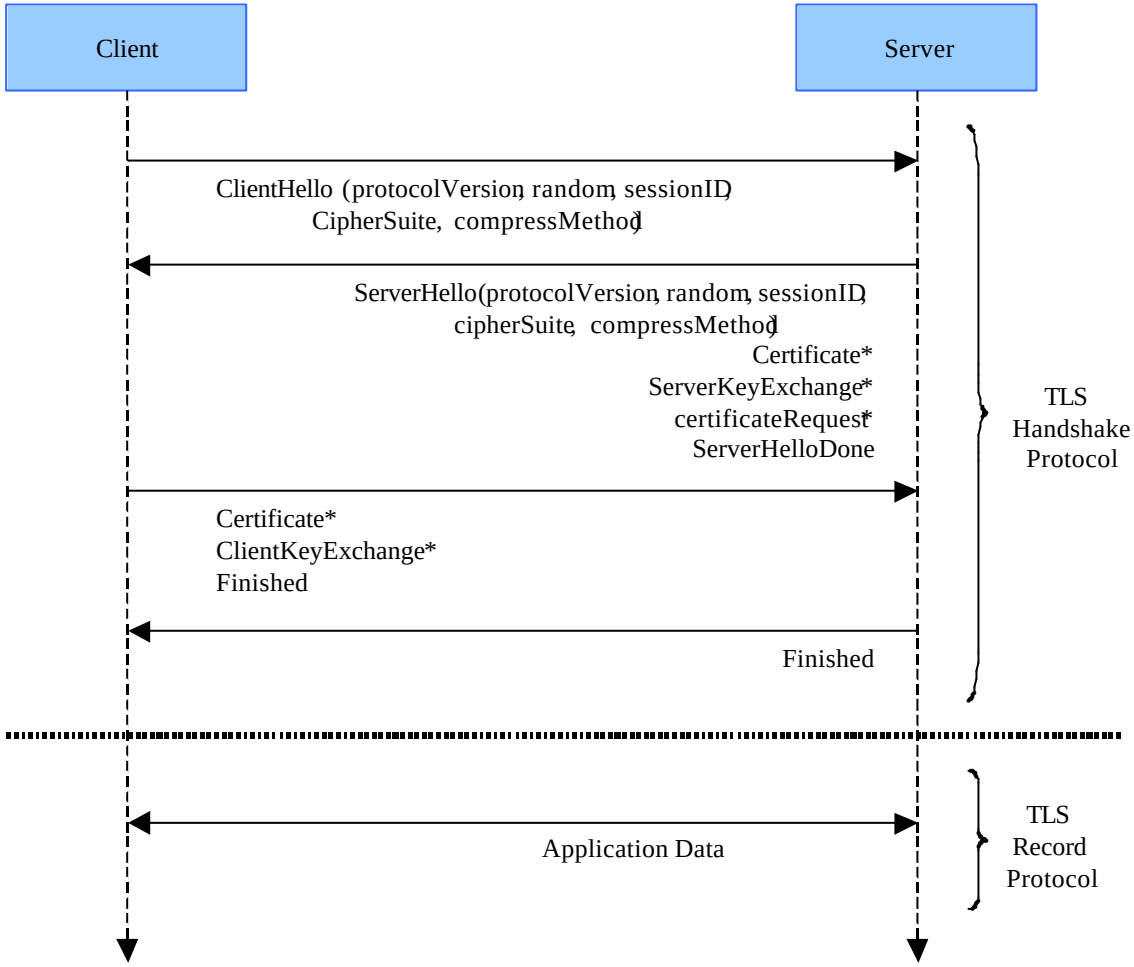
Le protocole TLS Handshake consiste en une suite de trois sous protocoles qui sont utilisées par les entités communicantes pour s'authentifier entre elles, créer un contexte de sécurité négocié utilisé ensuite par TLS Record et gérer et signaler des conditions d'erreur:

- Négociation
- Changement des paramètres de chiffrement
- Alerte

Contexte de session

- Un identifiant de session.
- Un certificat de l’entité distante. éventuellement nul.
- Une méthode de compression.
- Les spécifications du chiffrement. algorithme de chiffrement symétrique (nul, DES, etc.) algorithme de hachage (comme MD5 et SHA-1).
- La clé maître. Un secret de 48 octets partagé entre le client et le serveur.
- Un indicateur indiquant si la session peut couvrir plusieurs connexions TCP.

Exemple de MSC

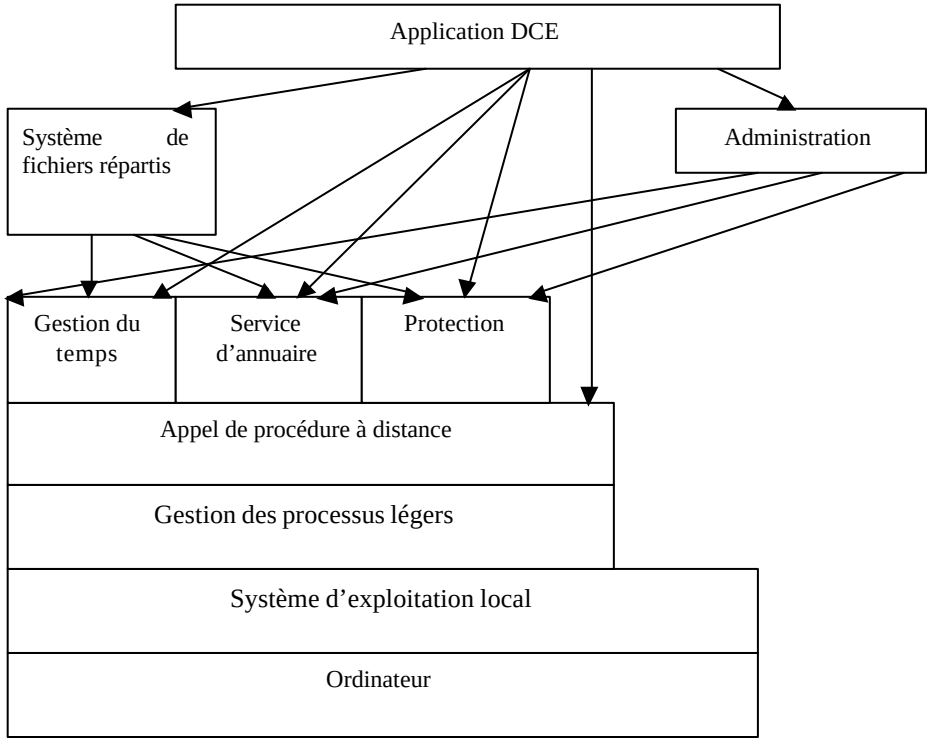


Implantation

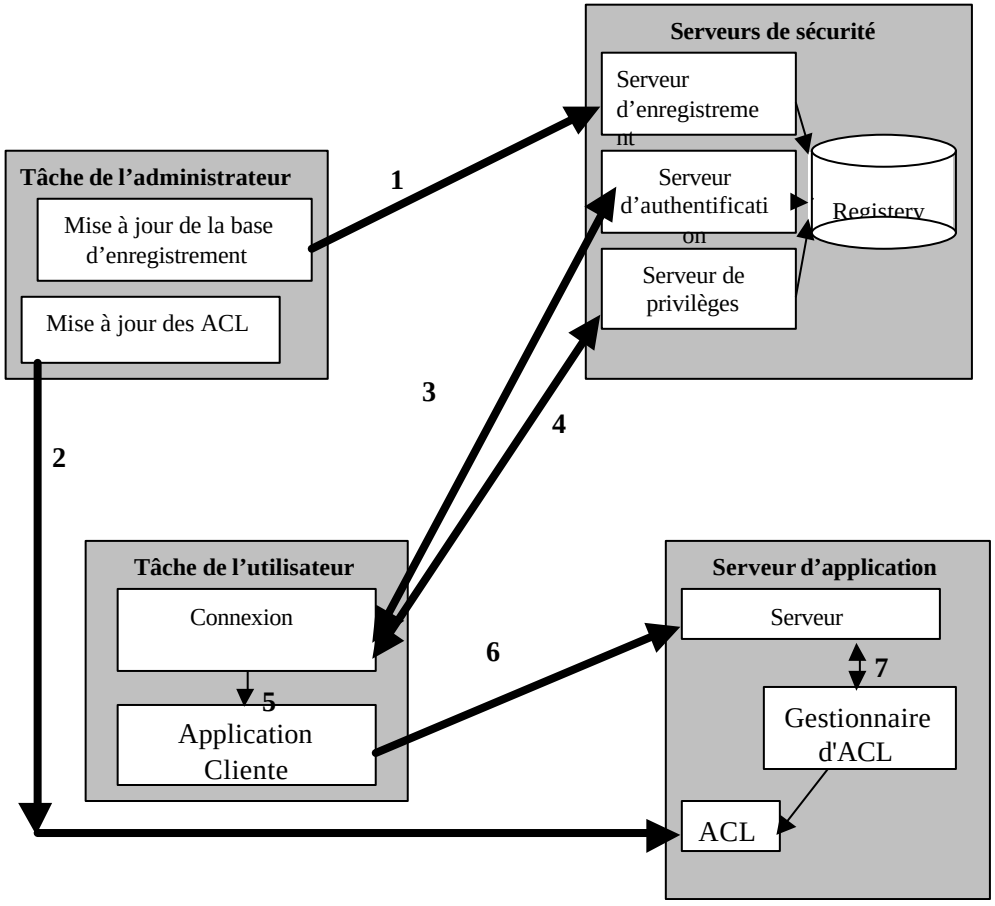
- **Mode Proxy**
- **Mode intégré**
- **Bibliothèques**

Mécanismes de protection

DCE
architecture générale



Protection dans DCE



Windows NT/2000/XP (1)

Utilisateurs: Un utilisateur est associé à compte dont les principaux attributs sont un non unique, un identifiant (SID: Security Identificator), un authentifiant qui est en standard un mot de passe avec une stratégie de gestion de cet authentifiant, les groupes auquel appartient l'utilisateur, les droits et permissions qui lui sont propre.

Droits: Un droit est l'autorisation pour un utilisateur ou un groupe d'utilisateur d'exécuter une opération donnée sur une classe de ressources particulières du système. Les droits existant dans NT sont prédéfinis.

Droits: Un droit est l'autorisation pour un utilisateur ou un groupe d'utilisateur d'exécuter une opération donnée sur une classe de ressources particulières du système. Les droits existant dans NT sont prédéfinis.

Permissions: Une permission est une règle associée à des ressources particulières (fichiers, répertoires, imprimantes) définissant quels ou quels groupes d'utilisateurs ont accès aux ressources et de quelle manière.Les droits outrepassent toujours les permissions.

Windows NT/2000/XP (2)

Listes de contrôle d'accès : Dans NT la plus grande partie des droits et permissions sont stockés dans l'environnement des ressources protégées La liste des droits associés à une ressource est une ACL.

Groupes : NT permet de créer facilement des groupes d'utilisateurs ayant certains droits, les groupes peuvent être hiérarchisés et un compte utilisateur peut appartenir à plusieurs groupes.

Trois types de groupes: les groupes locaux , les groupes globaux, les groupes spéciaux. Un groupe local est constitué à partir de comptes utilisateurs et de groupes globaux. Un groupe global n'est constitué qu'à partir de comptes utilisateurs membre du domaine de définition.

Groupes locaux prédéfinis :

- Le groupe *opérateur de compte.*
- Le groupe des *administrateurs.*
- Le groupe des *opérateurs de sauvegarde*
- Le groupe *invité.*
- Le groupe utilisateur.

Windows NT/2000/XP (3)

Domaines qualifie un ensemble de machines ayant un espace de compte centralisé commun, géré par un contrôleur de domaine.

- Pour définir un groupe global à un domaine qui a des droits donnés, on crée des groupes locaux ayant les droits donnés et on intègre le groupe global dans chaque groupe local ayant les droits choisis.
- L'authentification d'un utilisateur (et donc ses droits) n'est reconnu que dans son domaine. Un mécanisme permettant d'utiliser d'être reconnu et donc d'utiliser les relations d'approbation. Le domaine "approbateur" fera contrôler l'authentification d'un utilisateur du domaine "approuvé" par celui ci et honorera les demandes de cet utilisateur dans la limite des droits définis par des groupes globaux approuvés.

Audit: NT permet de spécifier une stratégie très subtile et complète d'audit de sécurité (et de façon plus générale d'administration).

Implantation de la protection : Très voisine de celle utilisée dans DCE

Le système n'ayant que deux niveaux de protection (utilisateur / noyau), le moniteur de référence local est exécuté en mode noyau. Il est appelé à chaque accès en ouverture à une ressource. Il contrôle que le demandeur dispose des droits suffisant en comparant un Ticket à l'ACL de la ressource.

Service de sécurité Corba

Un service d'authentification (objets représentant des utilisateurs (objets principaux) autres objets.)

Un service de propagation des droits. Ceux ci sont liés à la gestion des crédits (Credentials).

Des listes de contrôle d'accès. Les listes de contrôle d'accès peuvent porter sur une méthode, un objet, un groupe d'objet (une classe et toutes les classes dérivées, par exemple).

Un service d'audit.

Un service de non-répudiation.

Un service permettant de protéger les communications entre objets en intégrité et confidentialité.

Une notion de domaine, unité d'administration d'une politique de sécurité.

Une interface d'administration de la sécurité.

Protection dans l’internet

- Protéger dans un environnement ouvert
- Avec peu ou pas d’authentification

Règlement de sécurité Java

- Exemple:

  Une applet ne peut exécuter aucune opération du système de fichier local
- Une applet ne peut utiliser des fonction de communication réseau qu'avec l'ordinateur à partir duquel elle a été chargée. Les communications doivent s'exécuter en utilisant TCP et un port de numéro supérieur à 1024 (c'est à dire en dehors des ports réservés aux applications Internet classiques)
- Une applet ne peut accéder à toutes les fonctions de l'interface homme/machine. Toute fenêtre de dialogue créé par un applet doit donner lieu à un message prévenant l'utilisateur du caractère "non sécurisé" de l'opération.

  Une applet ne doit pas pouvoir accéder aux fonctions du système d'exploitation local qui permettent d'identifier l'utilisateur ou son compte ou les propriétés de son compte.

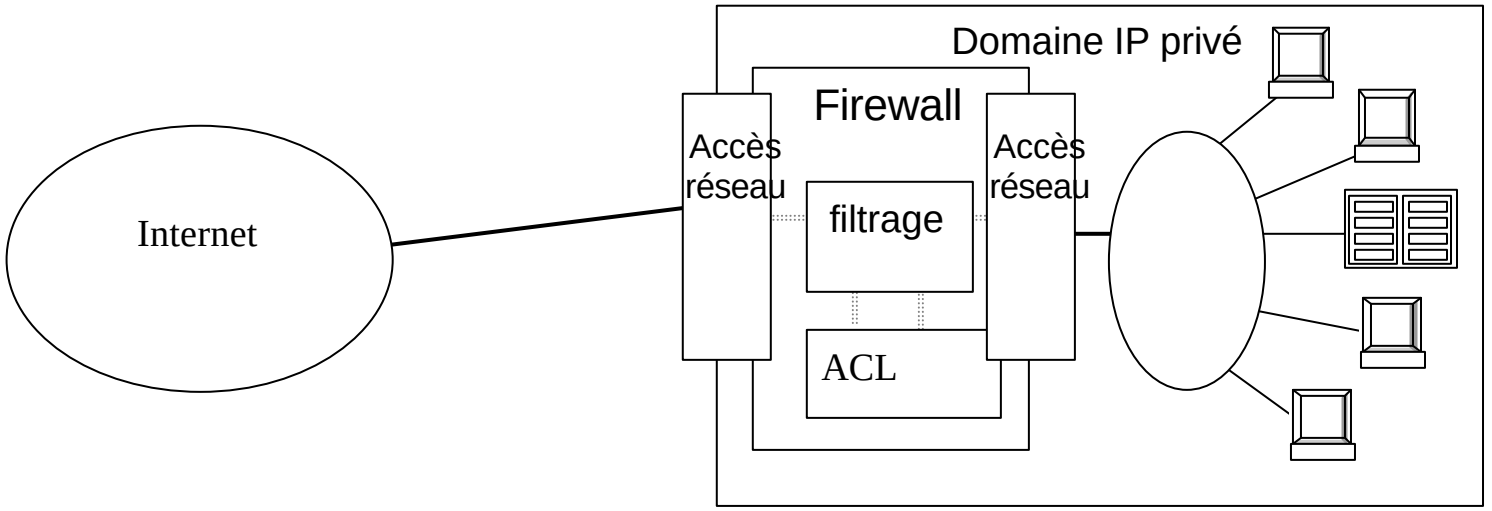
Mécanismes de protection Java

- Le contrôle statique réalisé par le JDK est destiné surtout à détecter les erreurs de programmation.
- La protection mémoire repose sur une architecture logicielle à domaines (au sens classique du terme). Lorsqu'une applet fait appel à un classe de l'API java, ceci est détecté par le chargeur de classes qui appelle le moniteur de sécurité de la JVM. En fonction des capacités du règlement de l'applet l'appel est autorisé ou interdit.
- Java peut également utiliser un mécanisme permettant de signer une applet lors de sa création ou se son installation sur le serveur. La signature, basée sur un certificat, est contrôlée lors du téléchargement.

Limites de la protection Java

- Erreur de programmation JVM et navigateurs
- Pas de protection matérielle
- Règlements de sécurités adaptés en environnement ouvert

Firewalls
(Coupe feux)



Fonctions

- Translations d’adresse
- Filtrage
- Administration

Règles de filtrage

Règles de filtrage pour le port externe

action	Source	Port sour	Dest	Port dest	Protocole Flag, option	description
Bloquer	144.19.0.0	*	*	70	tcp	Bloquer l'accès en sortie vers Gopher
Bloquer	144.19.0.0	*	*	80	Tcp	Bloquer l'accès en sortie vers le Web
Passer	144.19.0.0	*	*	*	tcp	Autoriser tous les autres accès tcp

Règles de filtrage pour le port interne

action	source	Port sour	Dest	Port dest	Protocole Flag, option	description
Passer	*	*	144.19.0.0	*	Tcp ACK=1	Accès autorisé sur connexion établie
Passer	*	*	144.19.74.200	25	Tcp	Accès e-mail autorisé
Passer	*	*	144.19.74.201	25	Tcp	Accès e-mail autorisé
Passer	*	*	144.19.74.200	119	Udp	Accès NNTP autorisé
Passer	*	*	144.19.74.201	119	Udp	Accès NNTP autorisé
Passer	*	*	144.19.74.202	53	Udp	Accès DNS autorisé