

Sécurité

**Sécurité des Systèmes d'Information
Concepts, Organisation, Outils et Tendance**

J. Saraydaryan

CPE - Lyon



Contrôle d'Accès

Sécurité des Systèmes d'information
Concepts, Organisation, outils et Tendance

J. Saraydaryan

CPE - Lyon



I Introduction et définitions

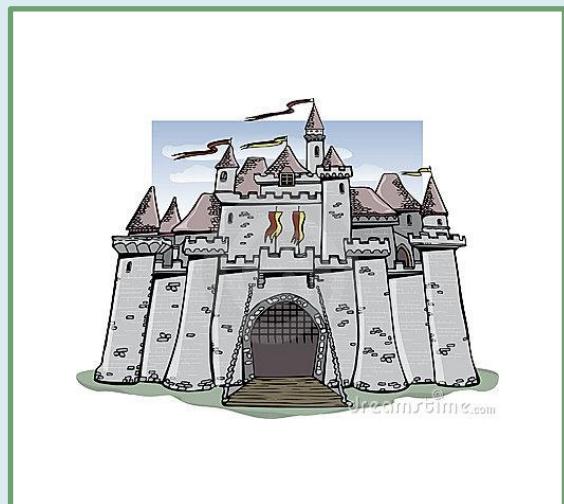
II Identification et authentification

III Autorisation

IV Modèle de contrôle d'accès

V Gestion des contrôles d'accès

VI Conclusion



Introduction et définitions

• Contrôle d'accès

Définition

Le contrôle d'accès est l'ensemble des outils de sécurité qui contrôlent comment les utilisateurs et systèmes interagissent avec le SI (systèmes et ressources)



Les concepts clés

- Accès

L'accès est le flux d'information entre un sujet et un objet

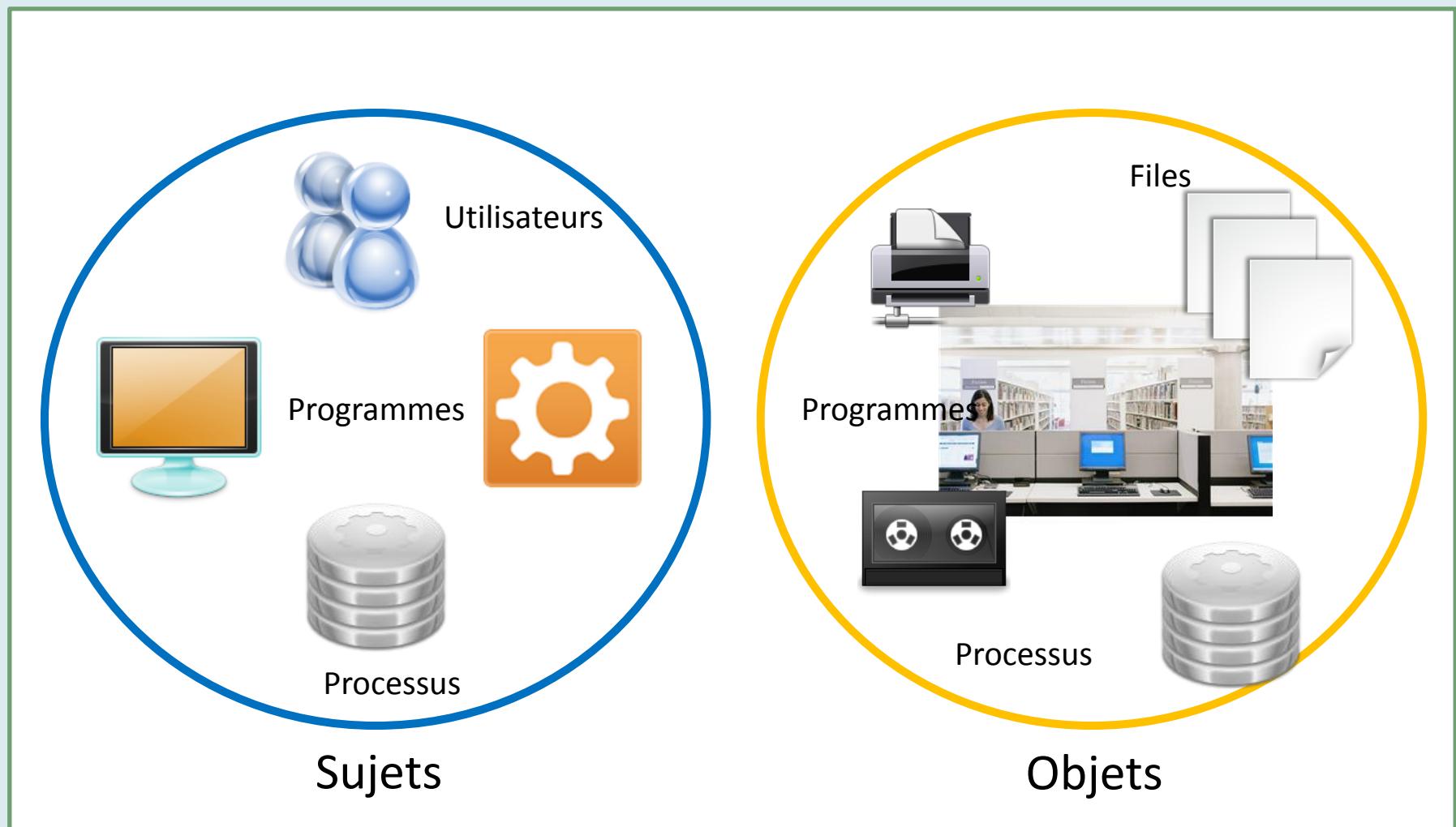
- Sujet

Utilisateur, programme, processus qui accède à un objet afin d'accomplir une tâche

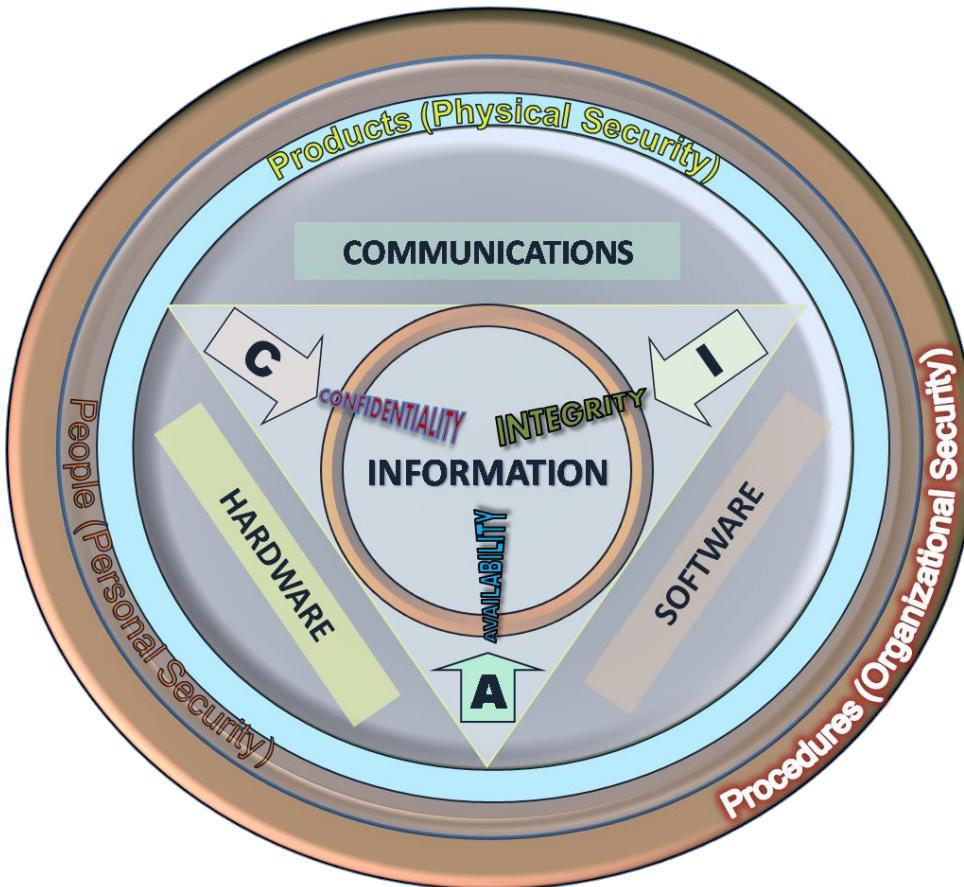
- Objet

Entité passive contenant de l'information.

- Contrôle d'accès



- Contrôle d'accès: Objectif



Contrôle d'accès : Identification, Authentication, Authorization, Accountability (AAA)

Identification

Méthodes permettant d'assurer qu'un sujet est bien celui qui prétend être,

Authentification

Afin d'être correctement authentifié, le sujet doit fournir une seconde pièce comme justificatif



Autorisation

Si le système détermine que le sujet peut accéder à une ressource alors il autorise le sujet à accéder à cette ressource

Accountability

Capacité à enregistrer les actions d'un sujet afin de le rendre responsable de ces actes

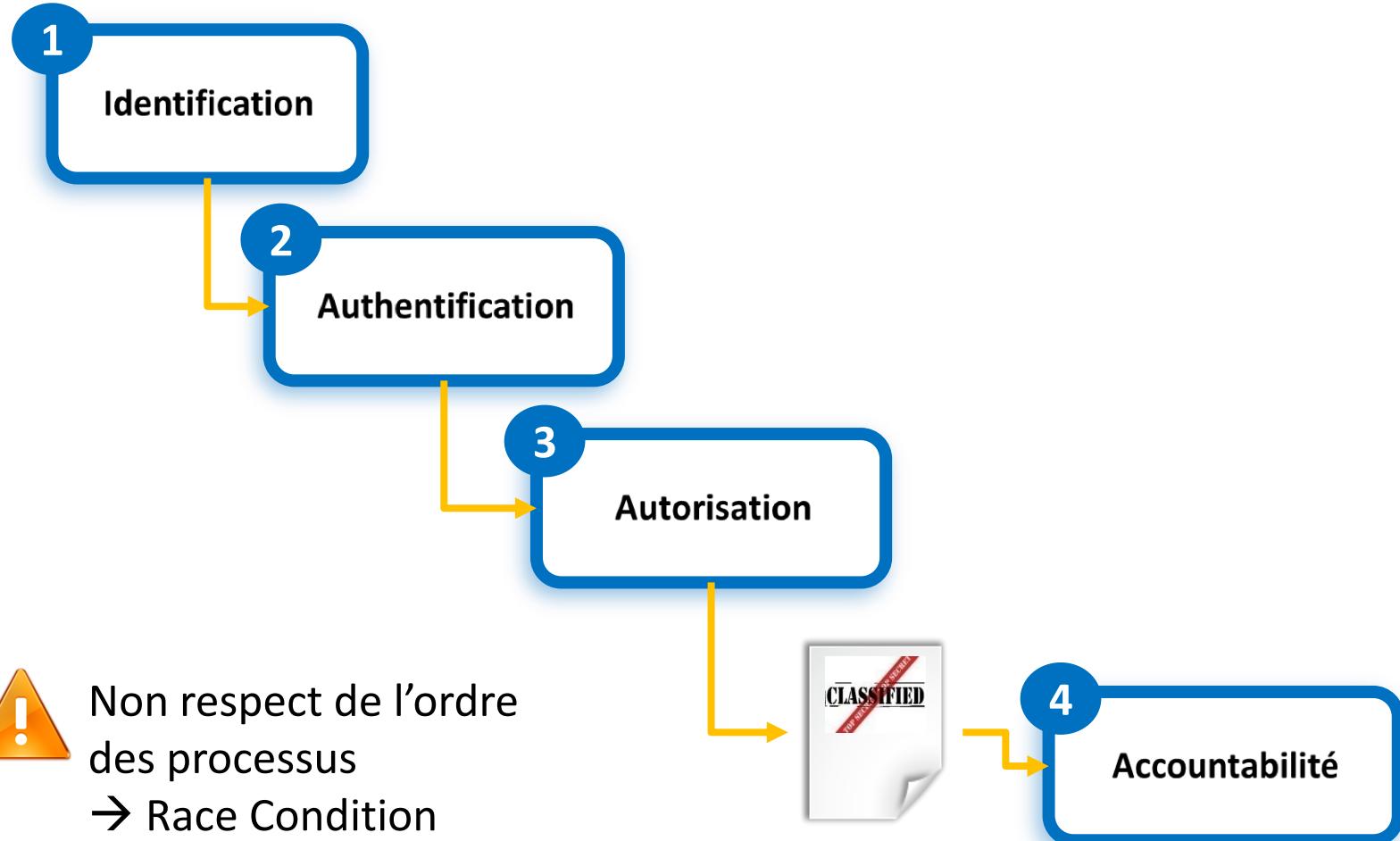
Contrôle d'accès : Identification, Authentication, Authorization, Accountability (AAA)

□ Concepts standardisés par l'IETF, e.g.:

- Generic AAA architecture (RFC2903)
- AAA Authorization Application Examples (RFC2905)
- AAA Authorization Framework (RFC2904)



- Contrôle d'accès: Objectif



Identification et Authentification

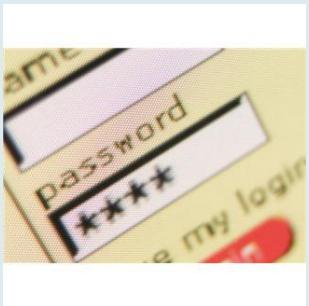
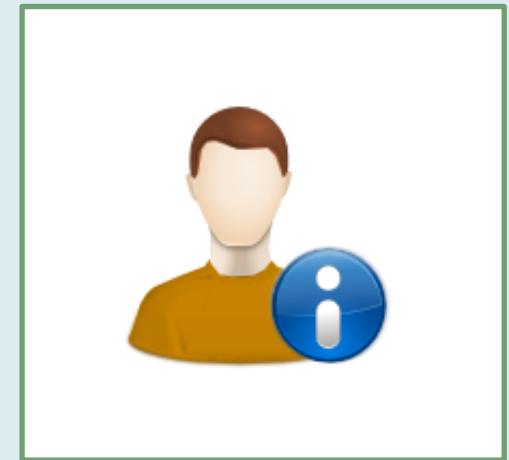
-
- Introduction
 - Management des identités
 - Biométrie
 - Gestion des mots de passe

- Contrôle d'accès: Identification et Authentification

- Comment un sujet peut-il être authentifié?

- 3 facteurs:

- Quelque chose que le sujet connaît
 - Quelque chose que le sujet possède
 - Quelque chose qui définit le sujet (ce qu'il est)



- Contrôle d'accès: Objectif

Vérification 1:1

VS

Vérification 1:N

Suis la personne que je prétend être ?

Quelle est cette personne?

Identification et Authentification

-
- Introduction
 - Management des identités
 - Biométrie
 - Gestion des mots de passe

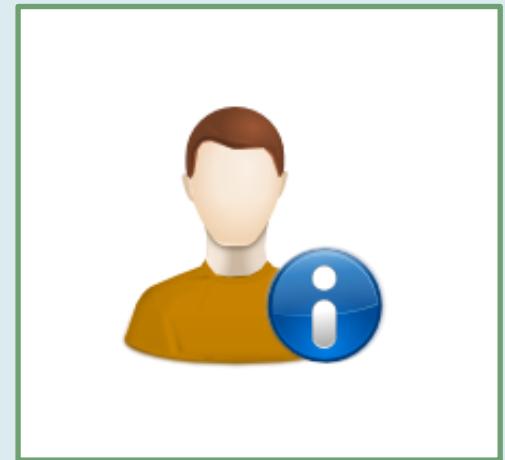
- **Contrôle d'accès: Identification et Authentification**

- **Management des identités**

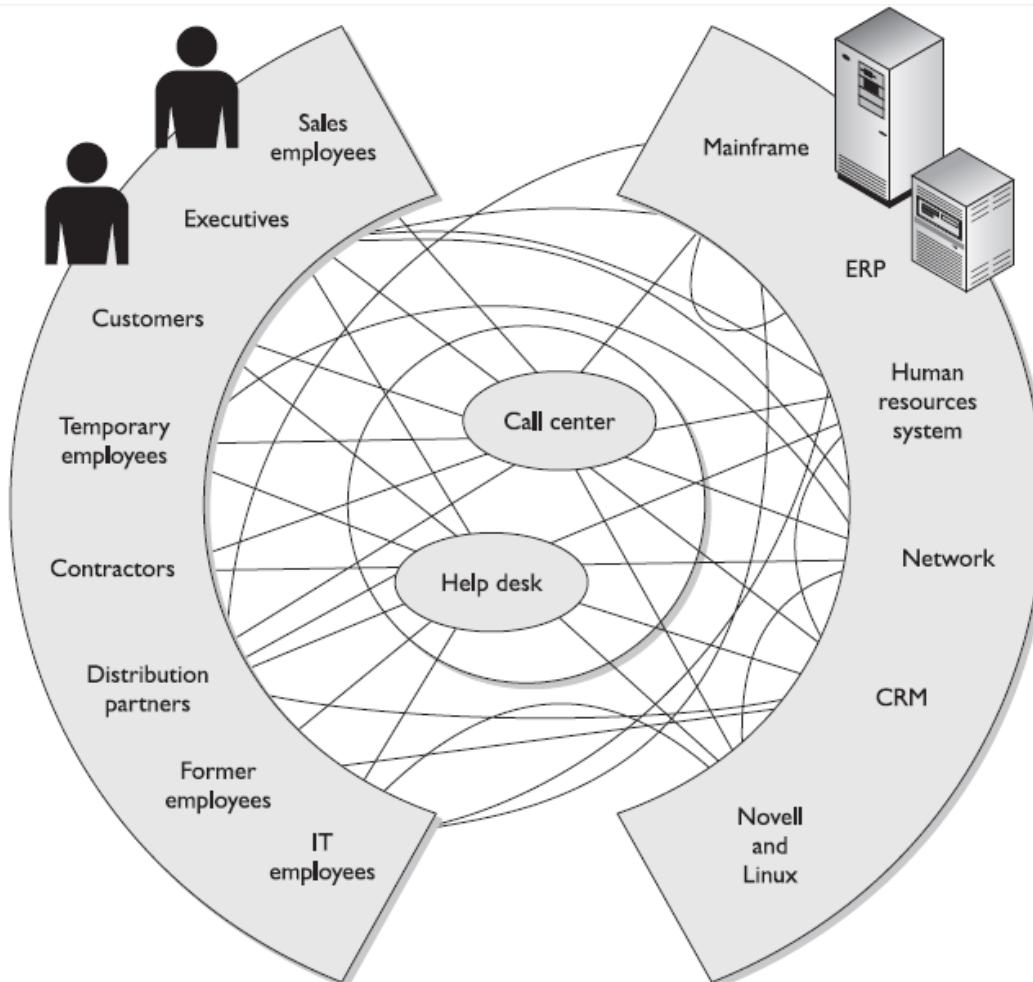
- Multiplication des outils → multiplication des authentifications

- **Objectif:**

- Homogénéiser la gestion des identités et des authentifications
 - Réduire la complexité d'utilisation



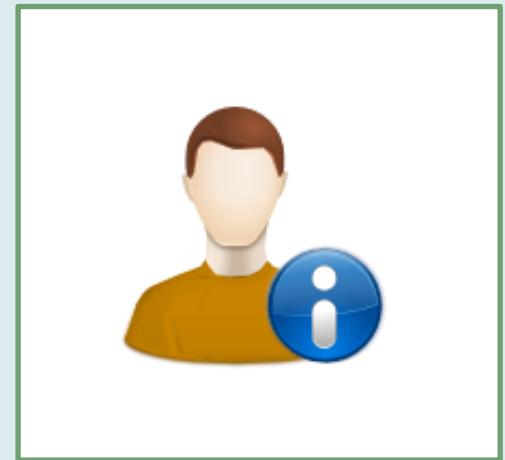
- Contrôle d'accès: Objectif



• Contrôle d'accès: Identification et Authentification

Management des identités

- Plusieurs outils spécialisés existent
- Types de technologies utilisées
 - Annuaires
 - Le management des accès web
 - Les mots de passe
 - Identification unique (Legacy single sign-on)
 - Management des comptes / mise à jour des profiles



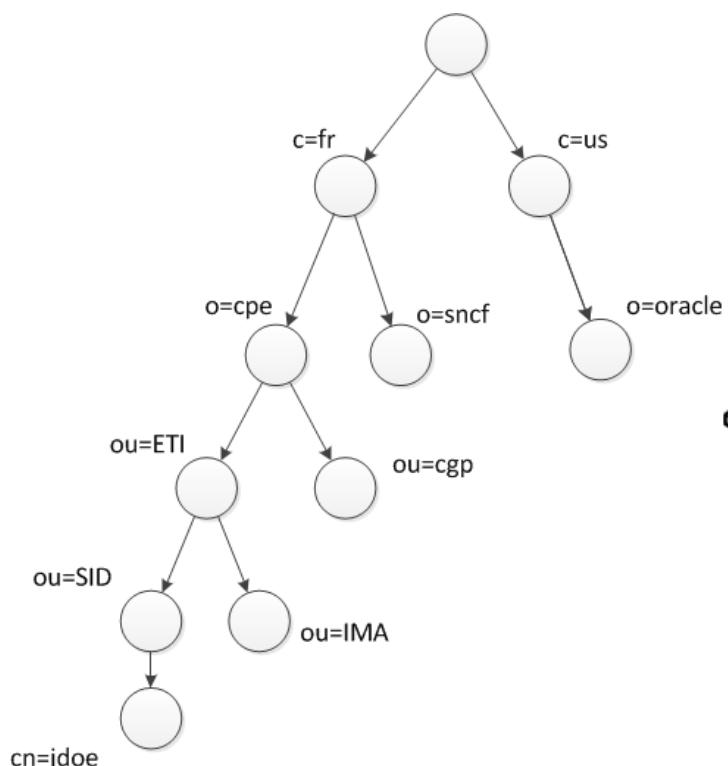
- **Identification et Authentification : Annuaires**

- **Base de données hiérarchiques**

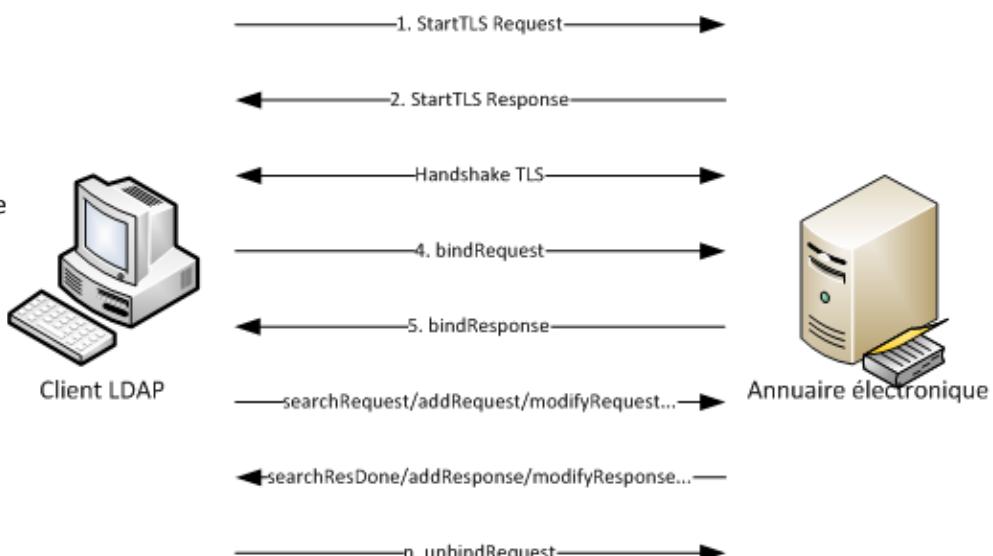
- Format de stockage: e.g. X.500
 - Protocole de communication: e.g LDAP
 - Les objets au sein de l'annuaire sont labélisés et identifiés avec un espace de nommage
 - Les services d'annuaires (directory services) administration de l'annuaire



- Identification et Authentification : Annuaires



Format de
données X500



Protocole LDAP

- **Identification et Authentification : Annuaires**

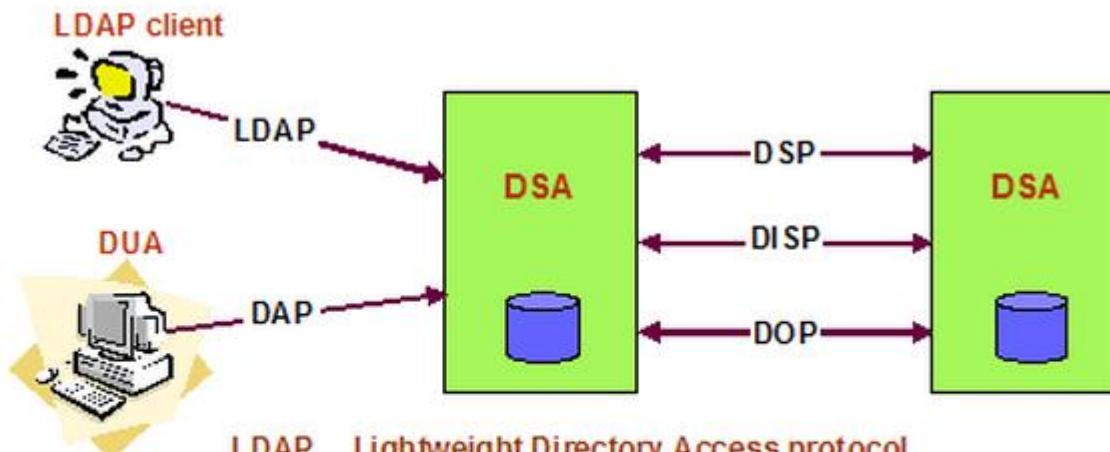
- **X500**

- Service d'annuaire global
 - Structure de modèle
 - Protocoles de communication
 - Procédures de distribution
 - X.500 UIT-T, ISO/CEI 9594-1 (1990)
 - X500 directory: stocker des informations d'organisation (personnes, liste, groupe...)



- Identification et Authentification : Annuaires X500

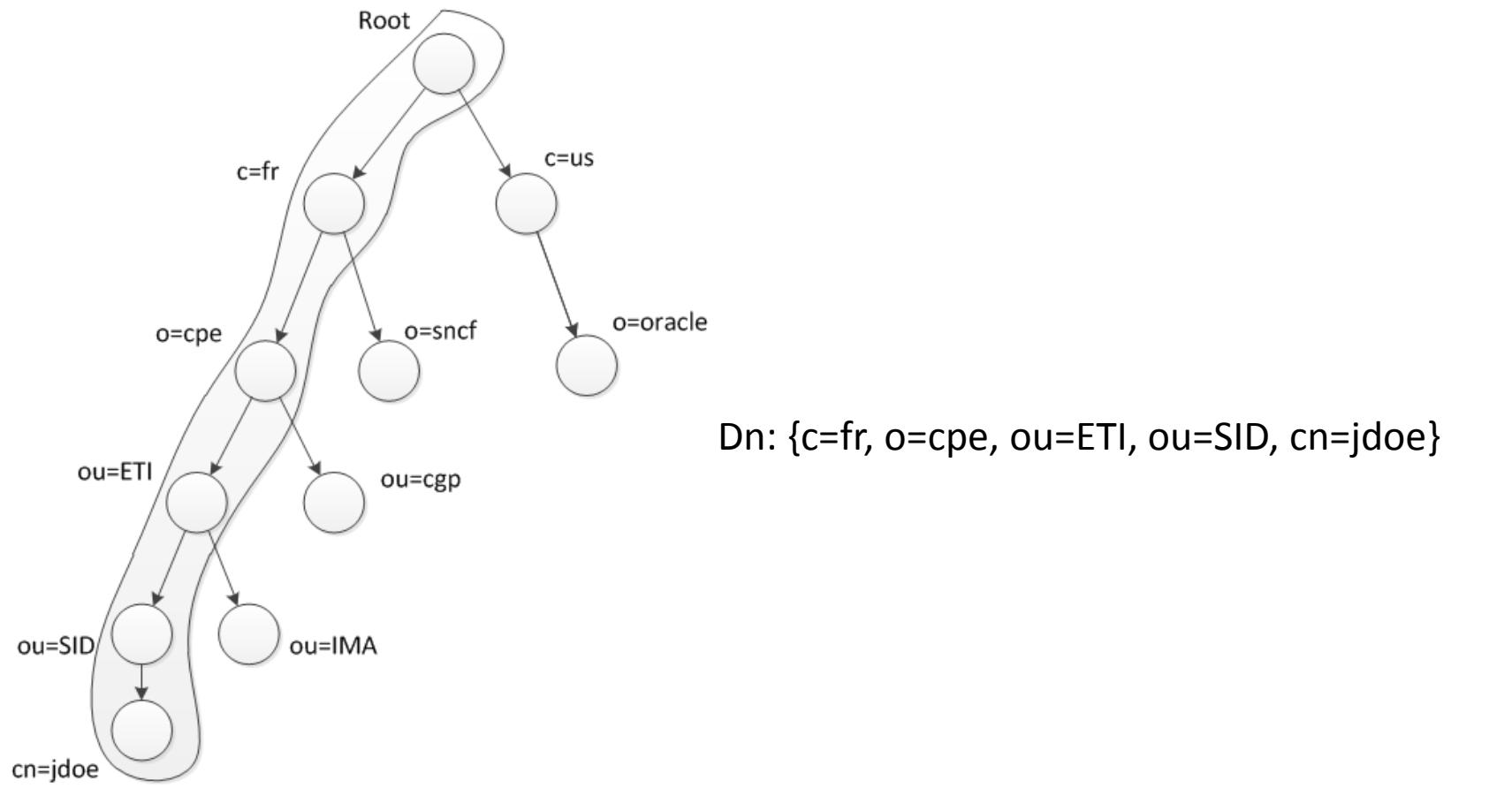
X.500 COMPONENTS AND PROTOCOLS



LDAP	Lightweight Directory Access protocol
DAP	Directory Access Protocol
DSP	Directory System Protocol
DISP	Directory Information Shadowing Protocol
DOP	Directory Operational Binding Management Protocol
DUA	Directory User Agent
DSA	Directory System Agent

- Identification et Authentification : Annuaires

- X500 espace de nommage



- **Identification et Authentification : Annuaires**

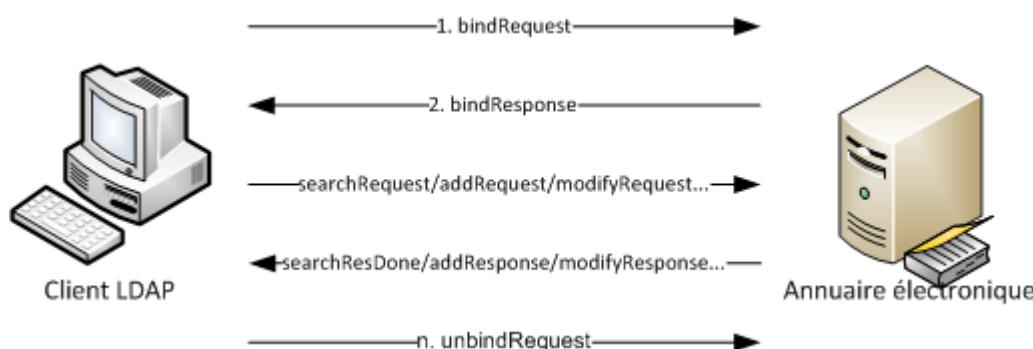
- **LDAP (Lightweight Directory Access Protocol)**

- Protocole applicatif (sur TCP/IP)
 - Mode connecté
 - Port 389, 636 (ldap et ldap over TSL/SSL)
 - Modèle de communication request-response



- Identification et Authentification : Annuaires LDAP

Message	Signification
bindRequest	Demande la connexion (authentifiée ou anonyme) à un annuaire
bindResponse	Réponse à la demande d'authentification
unbindRequest	Demande de déconnexion/fin de session
searchRequest	Demande à effectuer une recherche en fonction d'un filtre donné
searchResEntry	Réponse à une recherche, contenant une entrée LDAP
searchResDone	Dernier message indiquant la fin des réponses à une recherche
StartTLS Request	Demande de création d'une connexion chiffrée par une couche TLS émanant du client.
StartTLS Response	Réponse de la demande de création d'une connexion par couche TLS, continue par un handshake
TLS closure alert	Message envoyé pour demander/acquitter la fin d'une session protégée par une couche TLS
addRequest	Demande d'ajout d'une entrée dans l'annuaire
modifyRequest	Demande de modification d'une entrée de l'annuaire
modifyDNRequest	Demande la modification d'un <i>Distinguished Name</i> de l'annuaire (cf. section modèles de données)



- **Identification et Authentification : Annuaires LDAP**

Exemple d'URL LDAP:

ldap[s]://<hostname>:<port>/<base_dn>?<attributes>?<scope>?<filter>?<extensions>
ldap://ldap.mit.edu/ou=employees,dc=mit,dc=edu
ldap://ldap.example.com/dc=example,dc=com?postalAddress
ldap://ldap.example.com/cn=David%20Brent,dc=example,dc=com?cn,mail
ldap://ldap.example.com/dc=example,dc=com??sub?(sn=Jensen)

Exemple de requête

Exemple 3.1. Toutes les personnes ayant leur numéro de téléphone renseigné dans la base :
(&(objectclass=person)(telephoneNumber=*))

Exemple 3.2. Toutes les personnes dont le nom commence par 'A' et n'habitent pas Paris :
(&(objectclass=person)(cn=A*)(!(l=Paris)))

Exemple 3.3. Toutes les personnes dont le nom ressemble à Febvre (Faivre, Fèvre, Lefebvre, ...):
(&(objectclass=person)(cn~=fevbre))
(&(objectclass=person)(cn=*&f*&vre))

<http://ldapbook.labs.libre-entreprise.org/book/html/ch03s02.html>

- **Identification et Authentification : Annuaires LDAP**

Exemple d'URL LDAP:

ldap[s]://<hostname>:<port>/<base_dn>?<attributes>?<scope>?<filter>?<extensions>
ldap://ldap.mit.edu/ou=employees,dc=mit,dc=edu

Exemple de requête

Exemple 3.5. Lecture de toutes les personnes du service vente

ldap://ldap.netscape.com/ou=Sales,o=Netscape,c=US?cn,tel,mail?scope=sub?(objectclass=person)

Exemple 3.6. Lecture des objets personnes d'un annuaire

ldap://localhost:389/?sub?objectclass=person

Exemple 3.7. Recherche de Valery Febvre

ldap://ldap.easter-eggs.fr/cn=Valery%20Febvre,ou=Moyens%20Informatiques,dc=easter-eggs,dc=fr

Exemple 3.8. Recherche approximative d'une personne

ldap://ldap.easter-eggs.fr/o=easter-eggs,dc=fr?mail,uid,sub?(sn=Febvre)

• Identification et Authentification : Management des accès Web

❑ Objectif

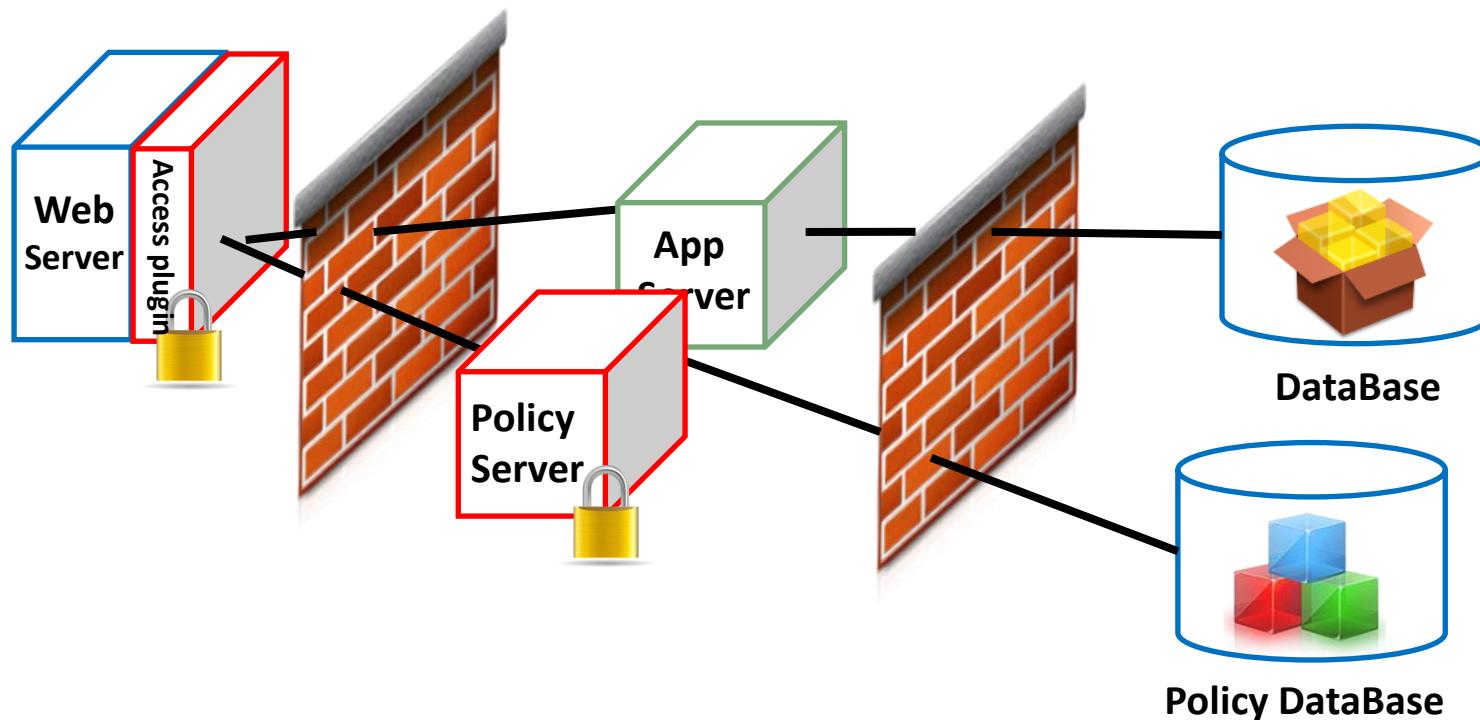
Contrôler à quoi les utilisateurs ont accès quand il utilisent un navigateur web pour interagir avec les « assets » web de l'entreprise.



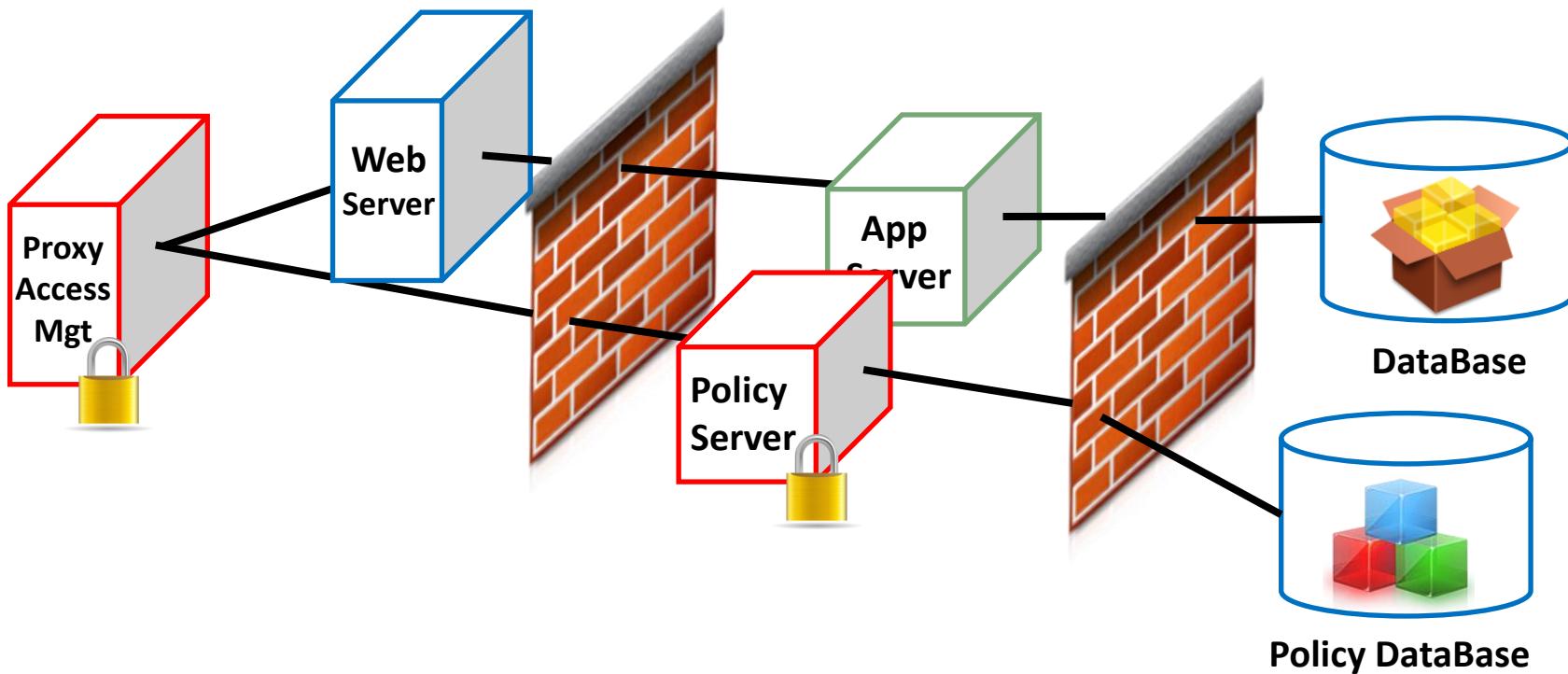
❑ Propriétés:

- Possibilité d'identification unique (http -> https)
- 2 Architectures possibles:
 - Plug-in des serveurs web (CA SiteMinder)
 - Proxy de redirection (maxsecurity)
- Utilisation des ressources locales utilisateurs (cookies->anti-hijacking)

- Identification et Authentification : Management des accès Web



- Identification et Authentification : Management des accès Web



• Identification et Authentification : Mots de passe

□ Problématique

- Gestions multiples de mot de passe
 - Administration complexe
 - Chaque mot de passe doit fournir une complexité minimum
- Accessibilité vs Sécurité



□ Solutions

- Synchronisation des mots de passe
- Reset des mots de passe en self service
- Reset des mots de passe assisté

- **Identification et Authentification : Mots de passe**

- **Synchronisation des mots de passe**

- 1 mot de passe pour tous les accès
 - Le mot de passe devient une ressource critique
 - Mot de passe = complexité élevée



- **Reset des mots de passe en self service**

- À la création de compte: fournir des questions personnelles
 - Mot de passe perdu= autre authentification (smart card, token) + questions

- **Reset des mots de passe assisté**

- Autoriser l'utilisateur de reseter son mot de passe après s'être authentifié

- **Identification et Authentification : Identification unique** (Legacy single sign-on)

- **Objectif**

*Permettre aux utilisateurs de s'authentifier 1 seule fois
et d'accéder à l'ensemble des ressources du système.*

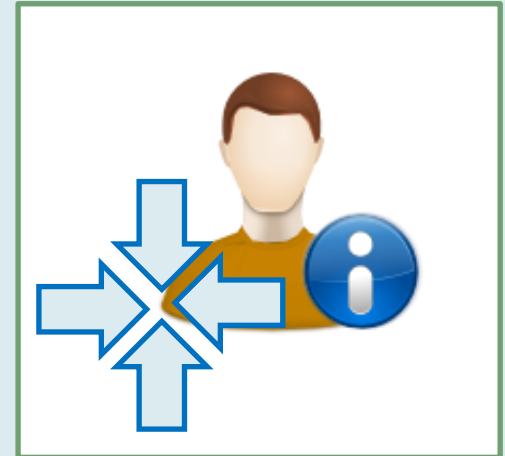
- Différent de la synchronisation des mots de passe
 - Un seul système d'authentification fournit les autorisations aux ressources
 - Attention au point d'engorgement
 - Point de stockage des informations authentification unique.



- **Identification et Authentification Management des comptes**

- **Objectif**

Outil permettant de gérer les comptes d'accès, de faciliter le changement des profiles et de droits, de s'assurer que les comptes inutiles ou expirés ne sont plus actifs



Identification et Authentification

-
- Introduction
 - Management des identités
 - Biométrie
 - Gestion des mots de passe

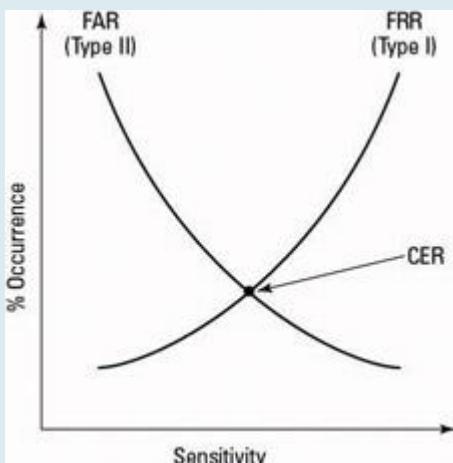
- Identification et Authentification

- La biométrie

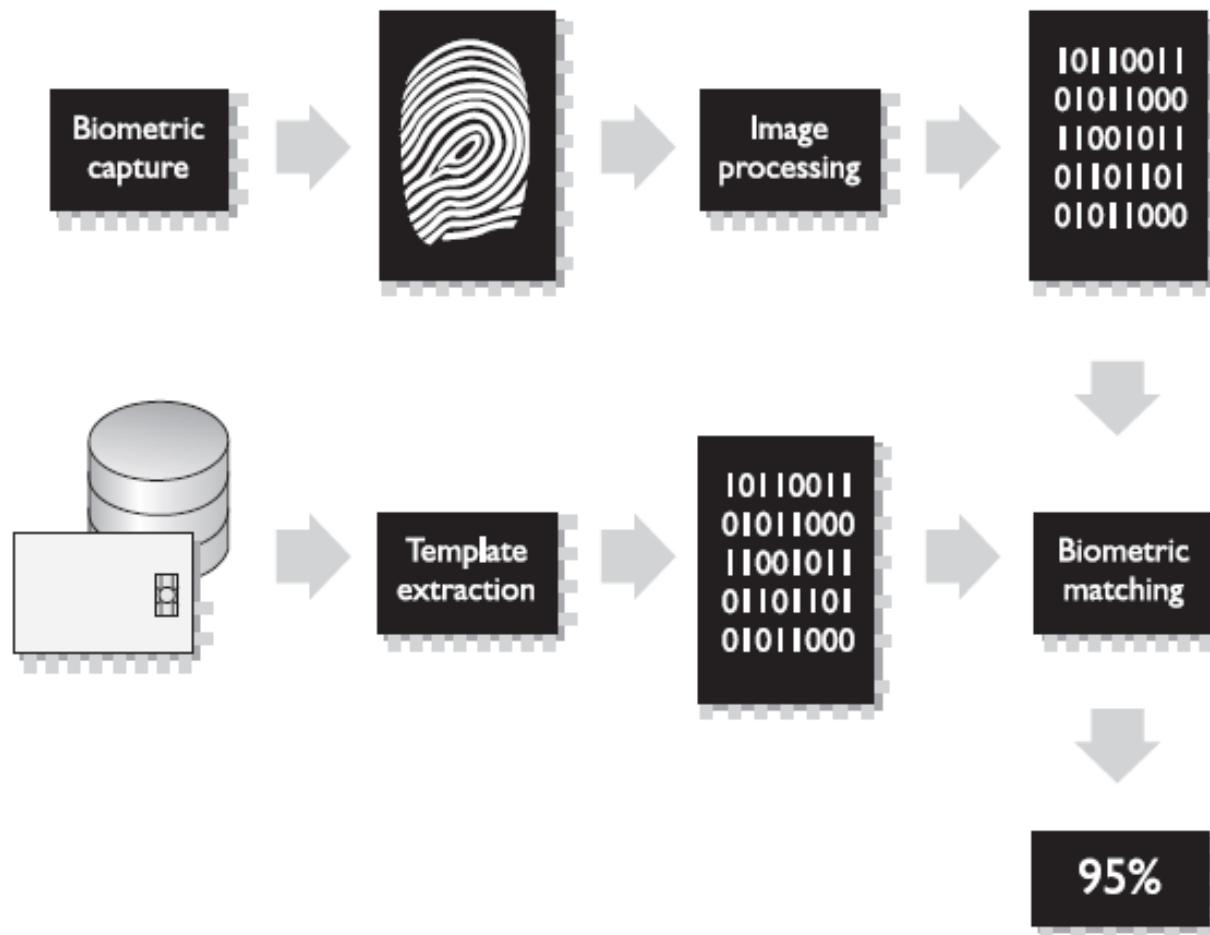
Vérifier l'identité d'un individu en analysant un attribut ou un comportement unique.

- Notion de Crossover error rate (CER)

Seuil représentant le point où le nombre de mauvais rejets est égal au nombre de mauvaises autorisations

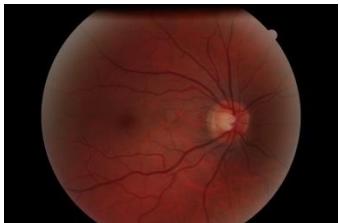


- Identification et Authentification: la biométrie

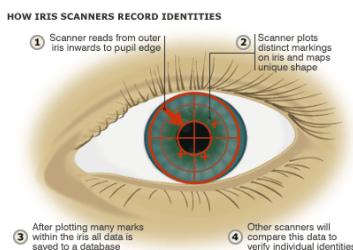


• Identification et Authentification: la biométrie

Rétine



Iris



Empreinte



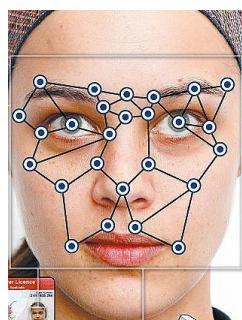
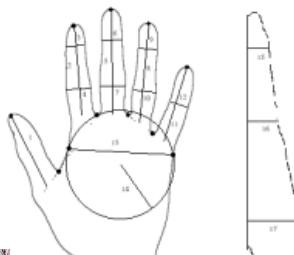
Empreinte vocale



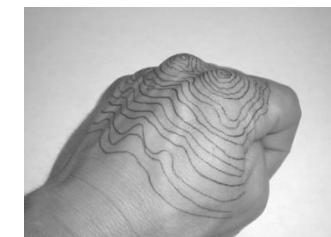
Signature (mouvement)

Clavier (mouvement)

Géométrie des mains



Visage



Topographie de la main

Identification et Authentification

-
- Introduction
 - Management des identités
 - Biométrie
 - Gestion des mots de passe

- **Identification et Authentification**

- **Gestion des mots de passe**

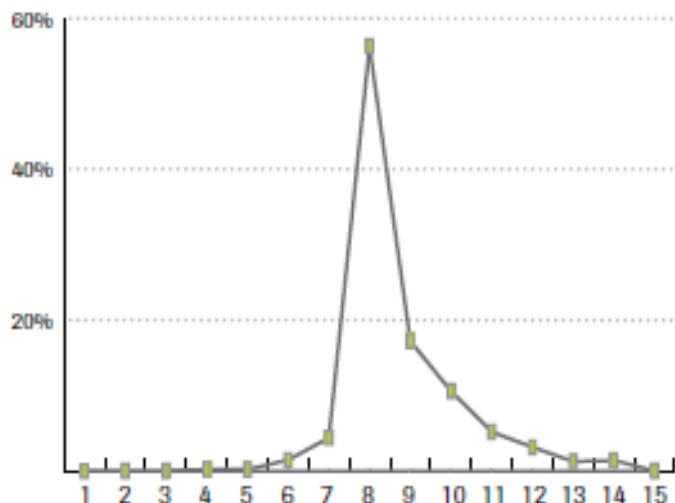
- Les plus utilisés pour l'authentification
- Complexité et taille importante nécessaire pour être sûr
- Cible d'attaques:
 - Sniffing
 - Accès aux fichiers contenant le mot de passe (serveur d'authentification)
 - Brute force
 - Attaque par dictionnaire
 - Social Engineering
 - Rainbow tables (hash format)



- Identification et Authentification: Gestion des mots de passe



- Identification et Authentification: Gestion des mots de passe



Password Length

Password Possibilities	
10	5.98737×10^{19}
9	6.30249×10^{17}
8	6.6342×10^{15}
7	69,833,729,609,375
6	735,091,890,625
5	7,737,809,375
4	81,450,625
3	857,375
2	9025
1	95

• Identification et Authentification: Gestion des mots de passe

Sécurisé les mots de passe

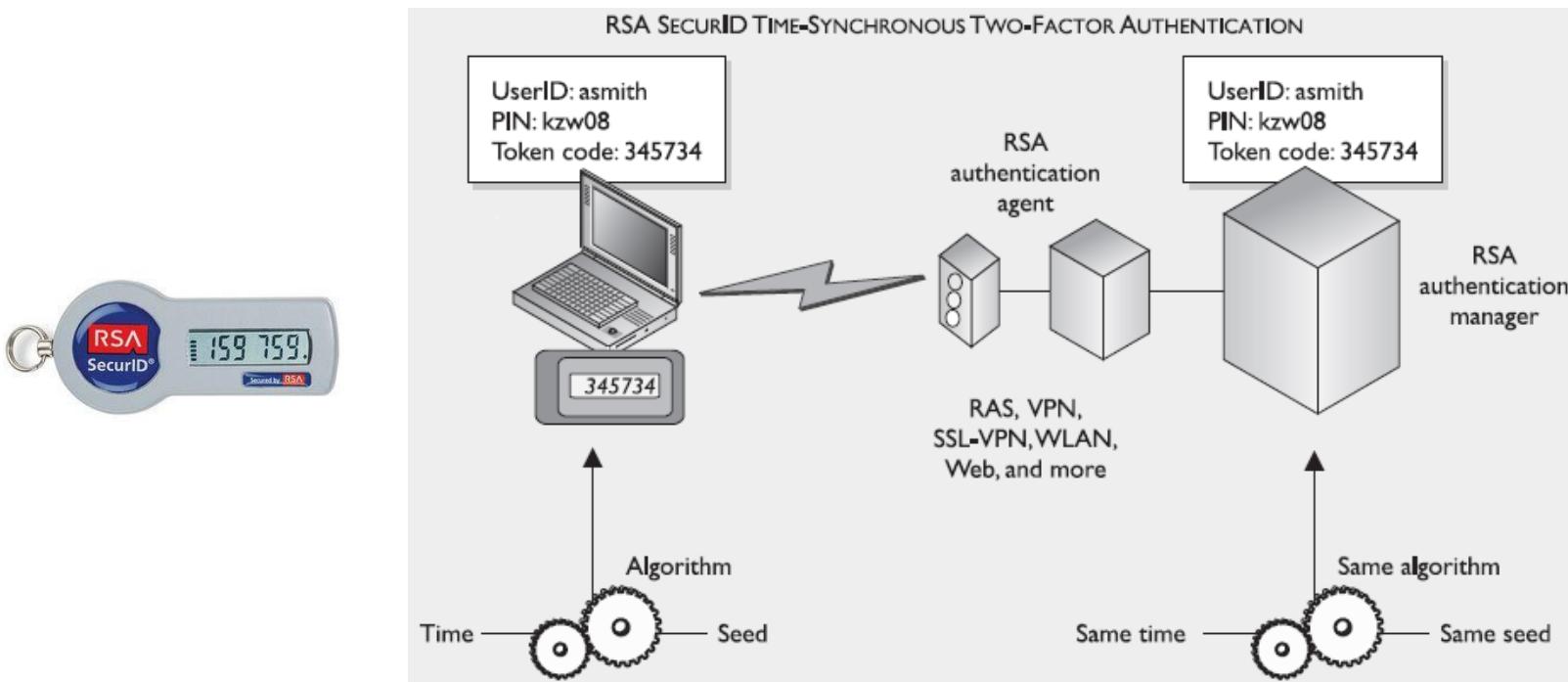
- Complexité (exemple : au moins 1 majuscule, 1 caractère spécial, taille min 8)
- Stockage: chiffrement ou Hash (MD4,MD5)
- Nombre de tentatives limité
- Durée de vie

Autres types de mots de passe

- Mot de passe cognitif (série de questions)
- Mot de passe à usage unique
 - Token synchrones
 - Token asynchrones (challenge/response)



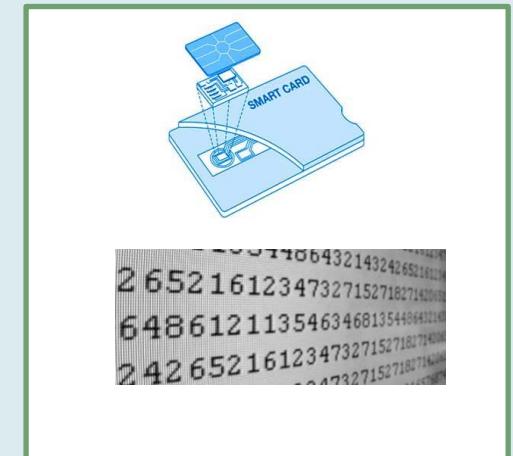
- Identification et Authentification: Gestion des mots de passe



RSA Security

• Identification et Authentification: Autres méthodes

- Clé cryptographique (signature numérique)
 - Memory card
 - Smart card



Autorisation

-
- Définition
 - Les Outils

• Contrôle d'accès: autorisation

Objectif

Déterminer si un sujet possède les droits suffisants permettant d'accéder à un objet et évaluer les actions permises sur cet objet

Concepts Clés

- **Role** : Utilisation de rôles pour déterminer le niveau d'autorisation. Le rôle est basé sur la fonction (job) du sujet dans l'organisation
- **Groupe**: Rassembler les sujets possédant les mêmes types d'accès à un objet au sein d'un groupe, facilite le management de l'autorisation
- **Paramètres de restriction**
 - Localisation physique ou logique:
 - Isolation temporelle
 - Type de transaction



- Autorisation: Règles de base



par défaut AUCUN ACCES



Seulement ce que le sujet à
besoin de connaître

ACCES AC CONNAIR

- **Autorisation: Domaine de sécurité**

- **Objectif**

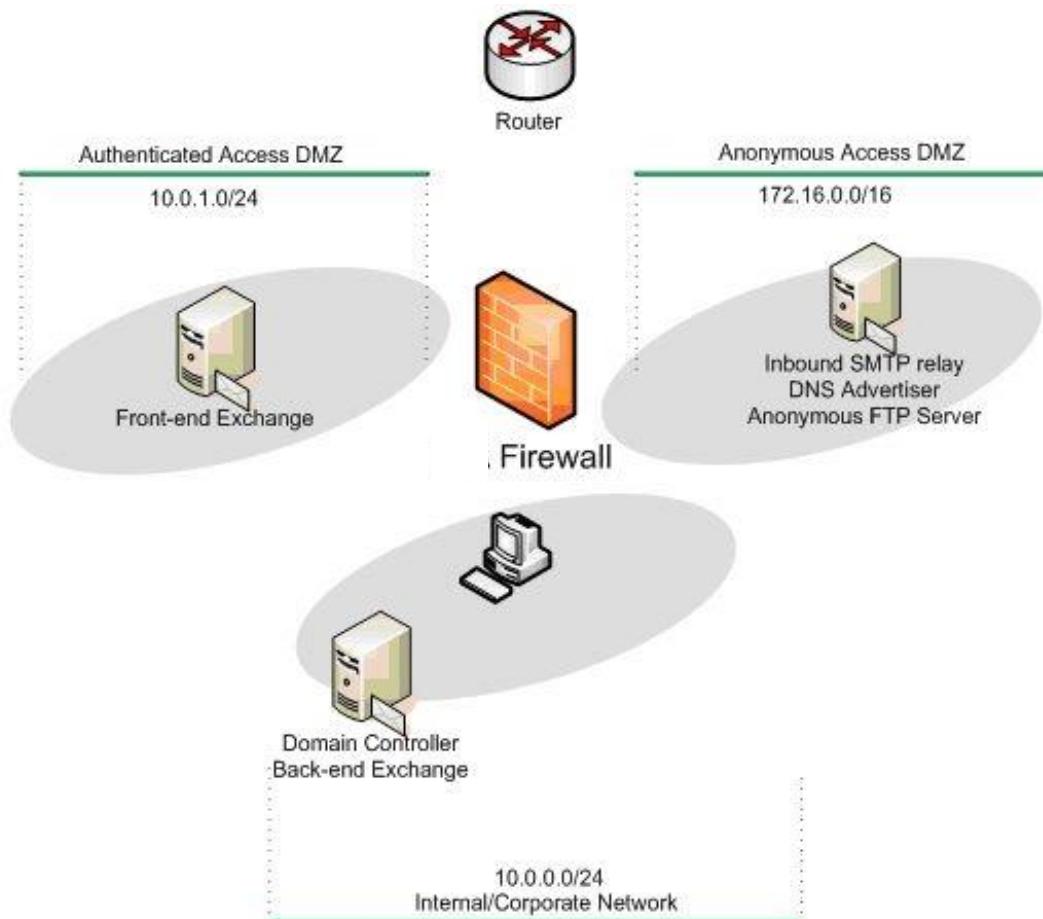
Ensemble de ressources d'une même structure logique (domaine) partageant les mêmes politiques de sécurité et administrées par le même groupe.

- **Exemple**

- Séparation de zones logiques réseaux par des firewalls
 - Stockage de documents classés d'un même niveau dans une même zone logique



- Autorisation: Domaine de sécurité



<http://www.isaserver.org/tutorials/Creating-Multiple-Security-Perimeters-Multihomed-ISA-Firewall-Part2.html>

Autorisation

-
- Définition
 - Les Outils

• Autorisation : KERBEROS

définition

Protocole d'authentification délivrant des autorisations par le biais de « tickets ».

Propriétés

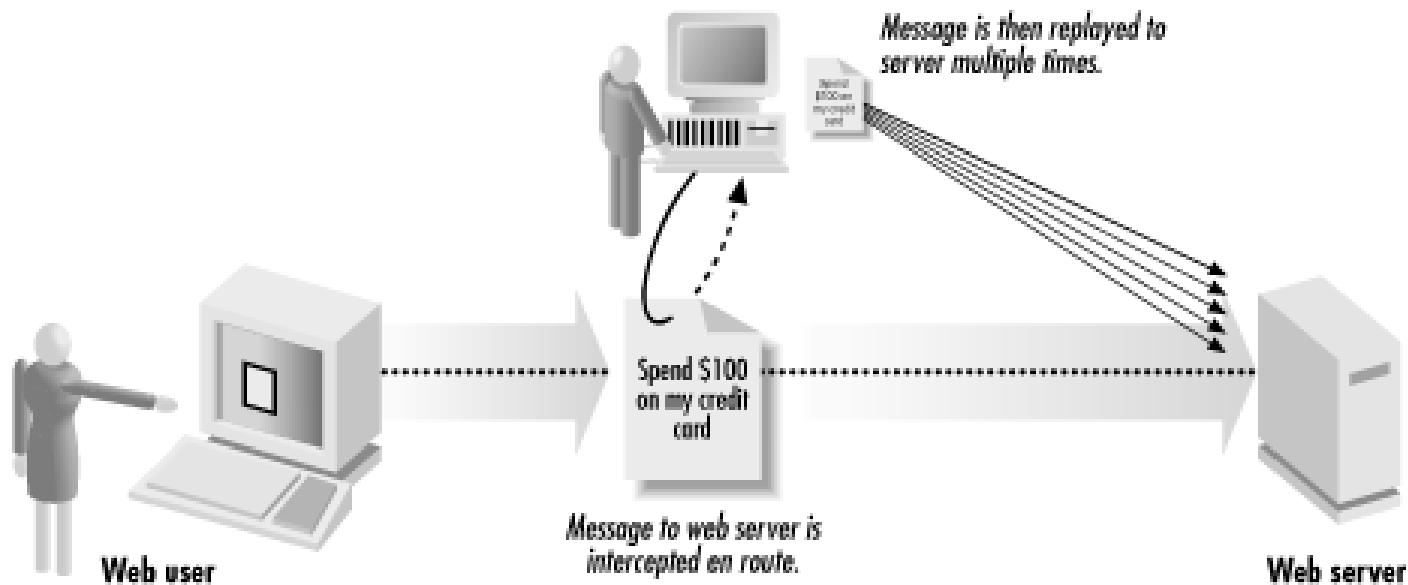
- Client serveur
- Authentifications et autorisations sécurisées sur réseaux non-sécurisés
- Authentification mutuelle sujet↔objet
- Protège contre les écoutes clandestines (eavesdropping) et les replay attack
- Utilise le chiffrement symétrique (asymétrique en option)

- MIT v5 RFC 4121



- **Autorisation: Kerberos**

Replay attack



• Autorisation : KERBEROS

Concepts

AS: *Authentication serveur*

Assure que le client est bien celui qu'il prétend être

KDC: *Key distribution Center*

Fournit les autorisations aux services demandés

TGS: *Ticket Granting Service*

Fournit des tickets d'utilisation relatif au service demandé

SS: *Service Serveur*

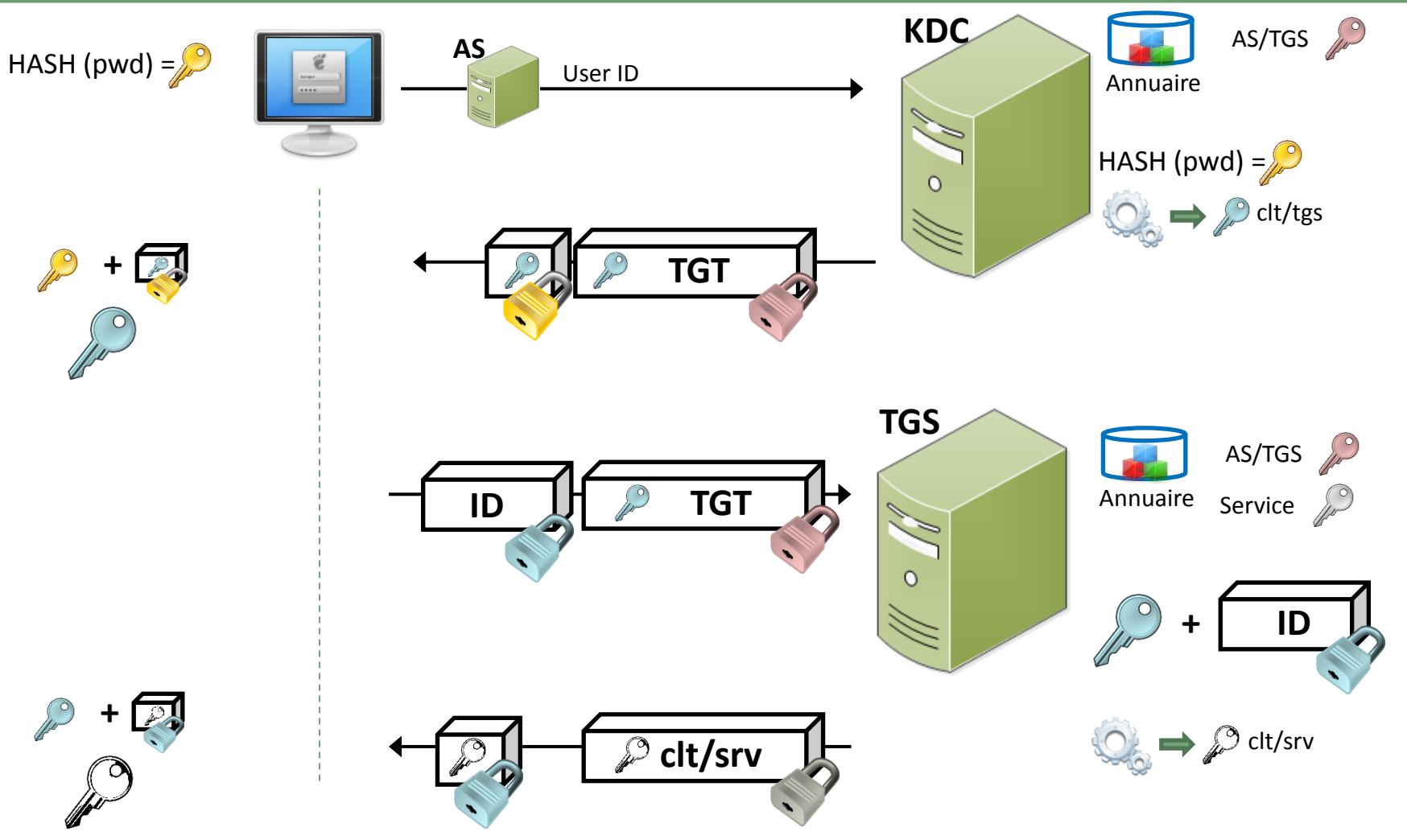
Fournit le service si les informations d'autorisation lui sont correctement transmises

TGT: *Ticket Granting Ticket*

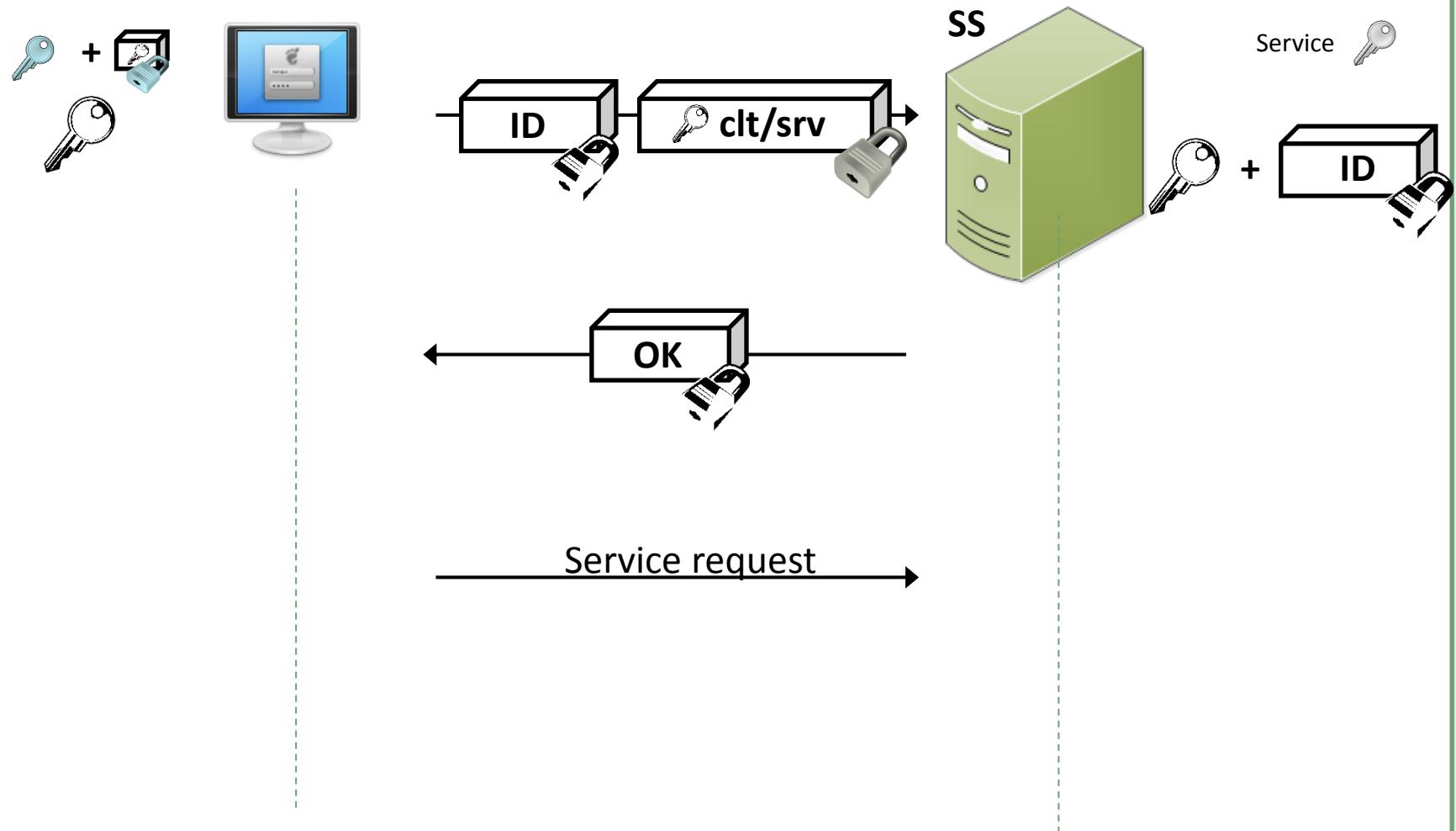
Ticket permettant d'accéder au TGS



- Autorisation: Kerberos: Authentification / Autorisation



- Autorisation: Kerberos: Authentification / Autorisation



• Autorisation : KERBEROS

Faiblesse

- Point unique de défaillance (serveur central doit être constamment disponible)
- Basé sur horodatage, toutes les horloges doivent être synchronisées (NTP)
- Protocol d'administration non standard
- Si le KDC est compromis → tout est compromis
- Le trafic n'est pas protégé par KERBEROS



- **Autorisation : SESAME**

- ❑ Secure European System for Applications
in a Multi-vendor Environment

- ❑ Objectif:

- Technologie d'identification unique
 - Basé sur KERBEROS
 - Contrôle d'accès distribué
 - Utilisation du chiffrement asymétrique



- **Autorisation : SESAME**

- Concepts

AS: Authentication Serveur

Authentifier l'utilisateur et fournisseur de jetons pour communiquer avec le PAS

PAS: Privilège Attribut Service

Fournisseur de PAC permettant d'accéder aux ressources

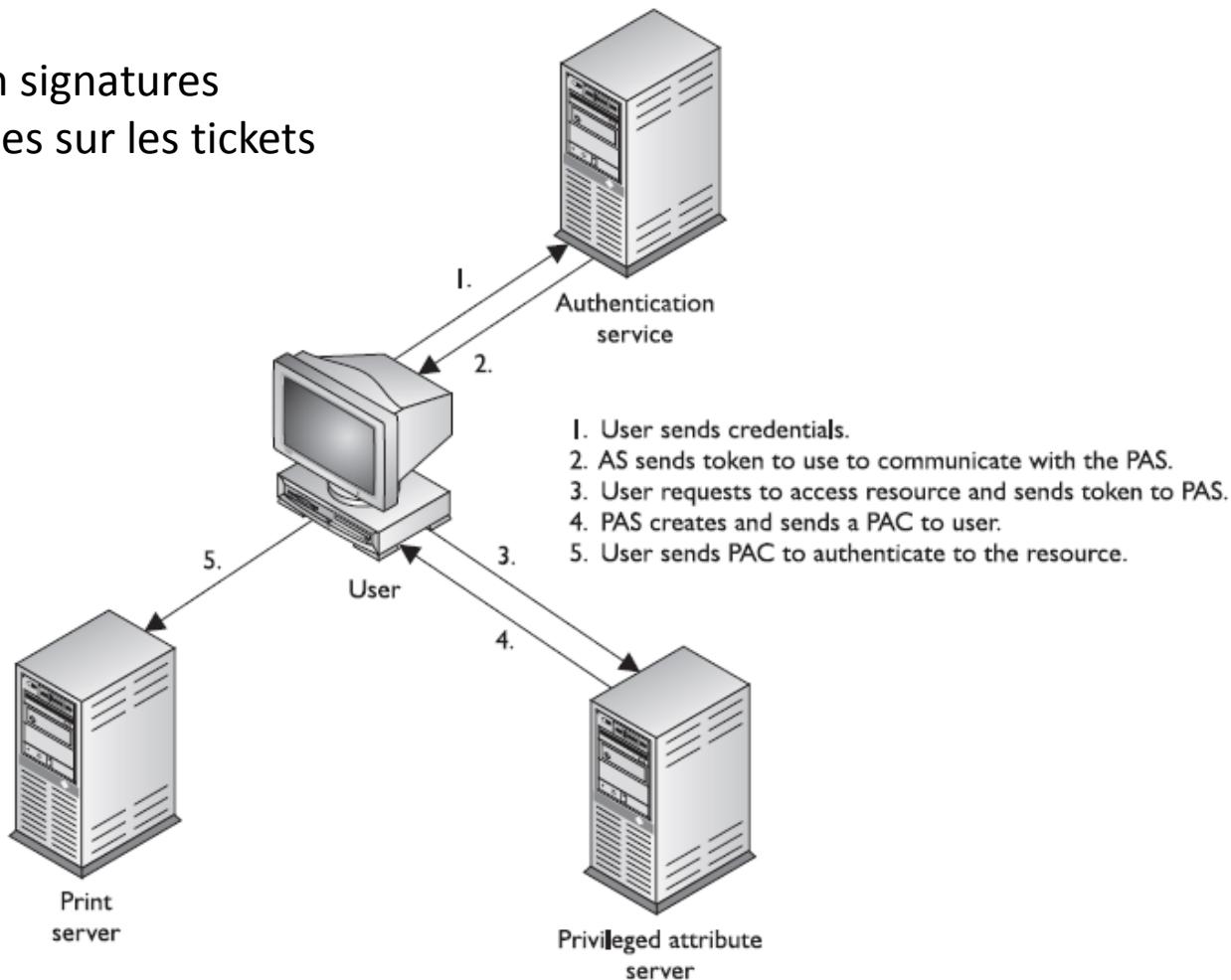
PAC: Privilège Attribut Certificate

Ticket permettant d'accéder aux ressources



• Autorisation: SESAME

Utilisation signatures
numériques sur les tickets



Modèles de contrôle d'accès

- DAC
- MAC
- RBAC

- **Modèle de contrôle d'accès**

- **Définition**

Framework définissant comment les sujets ont accès aux objets.



- **Principaux modèles:**

- **DAC - Discretionary Access Control**
 - **MAC - Mandatory Access Control**
 - **RBAC - Role Based Access Control**

- **DAC - Discretionary Access Control**

- **Histoire**

Modèles discrétionnaires (Trusted Computer System Evaluation Criteria, DoD, 1985)

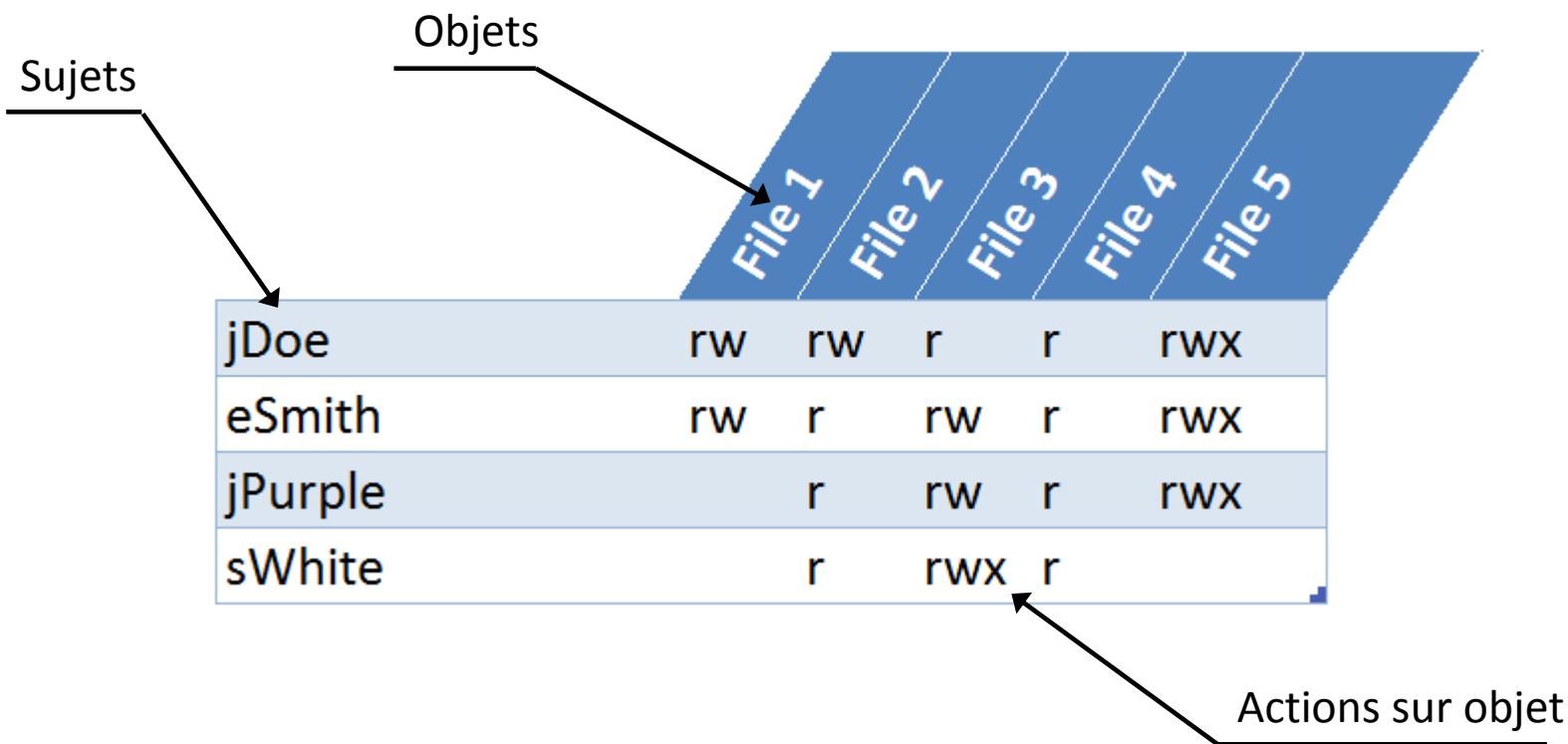
... a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).



- **Propriétés**

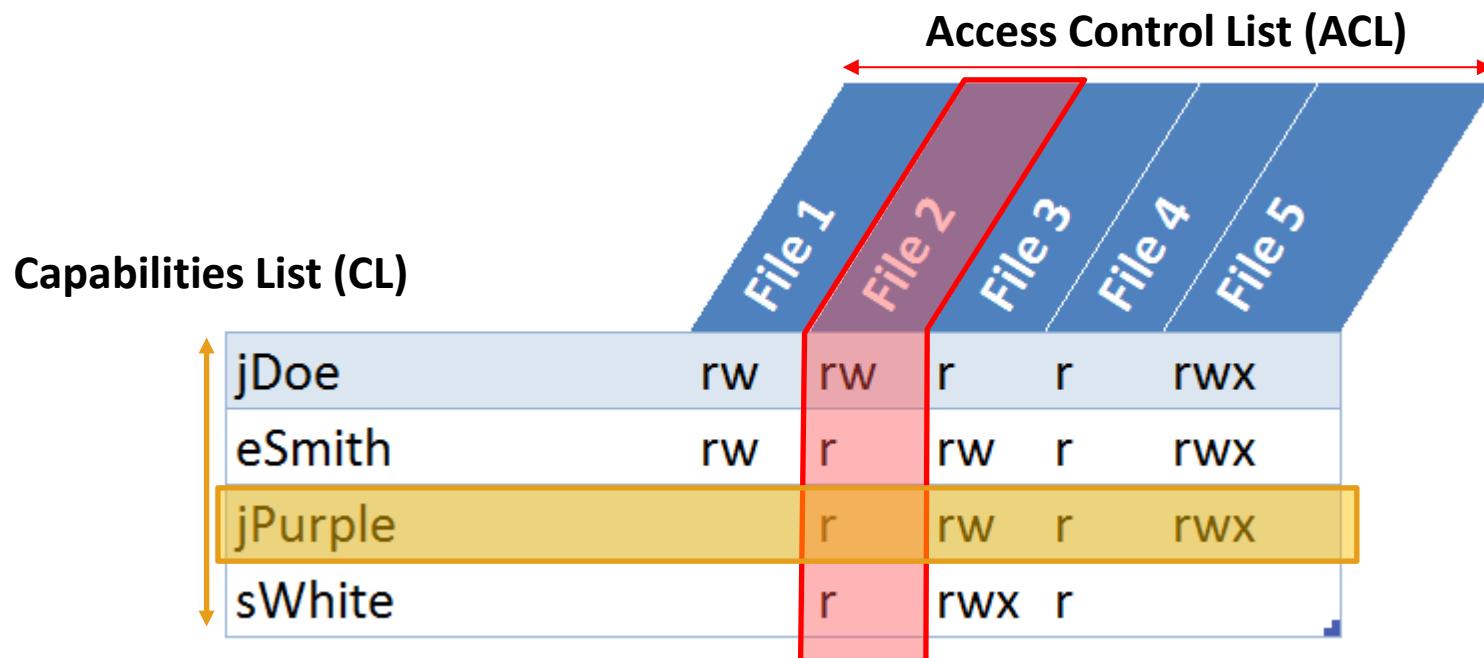
- Les droits sont organisés en matrice
 - La définition des droits est laissée à la discréction des propriétaires des objets.

- **DAC - Discretionary Access Control**



Droits UNIX/LINUX

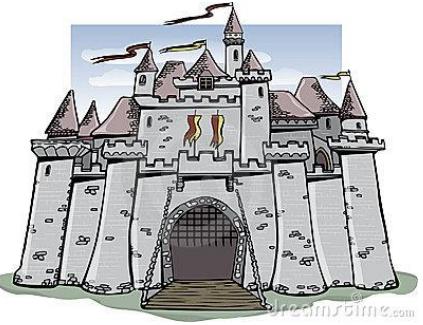
- DAC - Discretionary Access Control



- **DAC - Discretionary Access Control**

- **Limites**

- fastidieux
 - Pas de structuration
 - Fastidieux → erreurs
 - Pas d'assurance que le système est sûr



- **MAC- Mandatory Access Control**

- Définition**

Le contrôle d'accès mandataire est exprimé en termes de niveaux de sécurité associés aux sujets et aux objets et à partir desquels sont dérivés les actions autorisées. Il vise à contrôler le flux de l'information entre les classes de confidentialité.

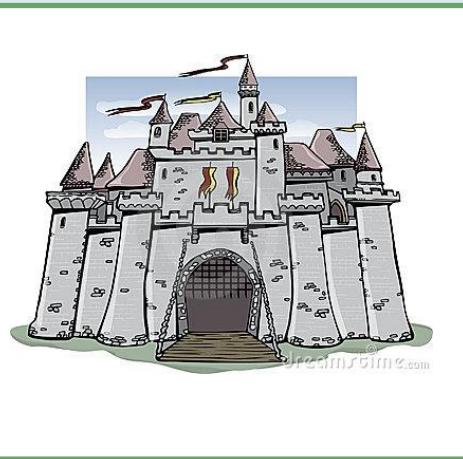
- Propriétés**

- Niveau d'indirection intermédiaire,
 - Autorisations fortement centralisées,
 - Rigide mais évaluable,
 - Mise en œuvre dans les langages (e.g., typage).
 - Basé sur des labels

- Chaque sujet reçoit une **habilitation** (ou accréditation)

- Chaque objet reçoit une **classification**

→ Principalement utilisé dans les milieux militaires



- **MAC- Mandatory Access Control**

- ***Confidentiel Défense (Confidential Defence)***: Information deemed potentially harmful to national defence, or that could lead to uncovering an information classified at a higher level of security.
- ***Secret Défense (Secret Defence)***: Information deemed very harmful to national defence. Such information cannot be reproduced without authorisation from the emitting authority, except in exceptional emergencies.
- ***Très Secret Défense (Very Secret Defence)***: Information deemed extremely harmful to national defence, and relative to governmental priorities in national defence. No service or organisation can elaborate, process, stock, transfer, display or destroy information or protected supports classified at this level without authorisation from the Prime Minister or the national secretary for National Defence. Partial or exhaustive reproduction is strictly forbidden.

Less sensitive information is "protected". The levels are

- ***Non Protégé (unprotected)***
- ***Diffusion restreinte administrateur*** ("administrative restricted information")
- ***Diffusion restreinte*** ("restricted information")
- ***Confidentiel personnels Sous-Officiers*** ("Confidential non-commissioned officers")
- ***Confidentiel personnels Officiers*** ("Confidential officers")

- **MAC- Mandatory Access Control**

2 règles de base pour la dérivation des autorisations

NO READ UP

Un sujet accrédité d'un niveau n ne peut pas accéder en lecture à un niveau $n+1, n+2, \dots, n+i$

NO WRITE DOWN

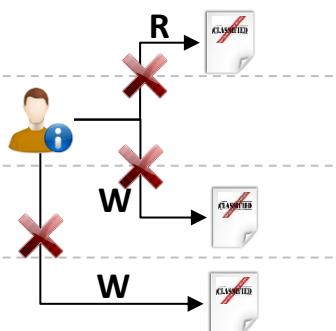
Un sujet accrédité d'un niveau n ne peut pas accéder en écriture à des objets de classification $n-1, n-2, \dots, n-j$

Très secret défense

Secret défense

Confidentiel Défense

Non Classé



- **MAC- Mandatory Access Control**

□ Limites

- Tout se base sur les règles et niveaux
 - lourdeur administrative
- Adapté aux systèmes très contraints (communication limitée)
- Structure rigide peu évolutive
- Difficulté de passage à l'échelle (utilisateurs, objets)



□ Exemple d'utilisation

- Mandatory Integrity Control (MIC) – Windows
- SELinux -Linux

- **RBAC- Role Based Acces Control**

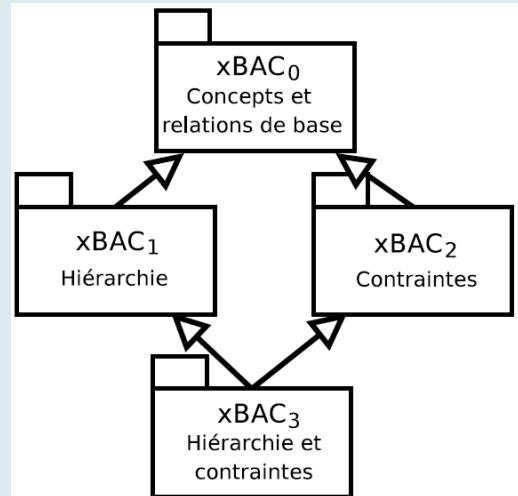
- **Définition**

RBAC ou nondiscretionary access control utilise un système de contrôle centralisé déterminant le type d'accès d'un sujet à un objet en fonction de son rôle (job, fonction)

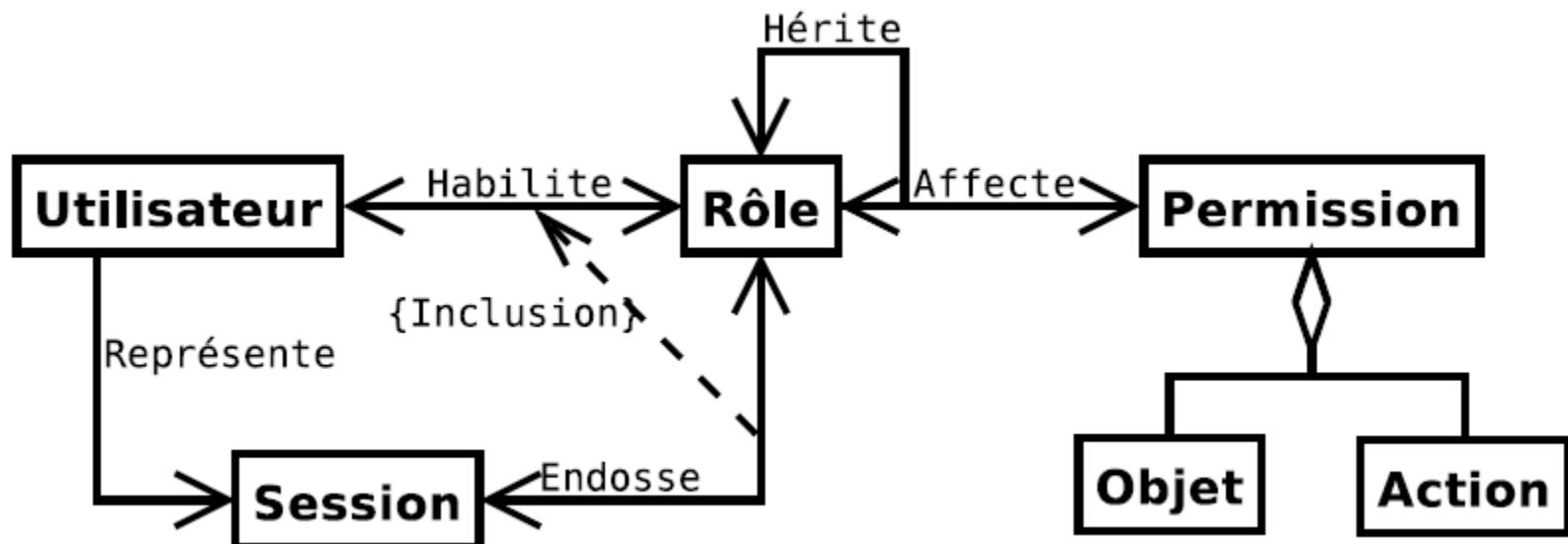


- **Propriétés:**

- de nombreuses implémentations (Tivoli, Oracle, Sybase, Informix, Apache, Linux, Microsoft, Sun),
 - de nombreux modèles dérivés
 - Standard ANSI, RBAC⁰, RBAC¹, RBAC², RBAC³



- RBAC- Role Based Access Control



- RBAC- Role Based Acces Control: RBAC_0

	Notation	Description
Concepts	\mathcal{U}	ensemble fini d'utilisateurs
	\mathcal{R}	ensemble fini de rôles
	\mathcal{A}	ensemble fini d'actions
	\mathcal{O}	ensemble fini d'objets
	\mathcal{S}	ensemble fini de sujets (sessions)
Relations	$\mathcal{P} \subseteq \mathcal{O} \times \mathcal{A}$	une action sur un objet
	$URA \subseteq \mathcal{U} \times \mathcal{R}$	affectation de rôles aux utilisateurs
	$PRA \subseteq \mathcal{R} \times \mathcal{P}$	affectation de permissions aux rôles
	$SU \subseteq \mathcal{S} \times \mathcal{U}$	relation entre sessions et utilisateurs
	$SR \subseteq \mathcal{S} \times \mathcal{R}$	relation entre sessions et rôles
	$RH \subseteq \mathcal{R} \times \mathcal{R}$	relation d'héritage entre rôles

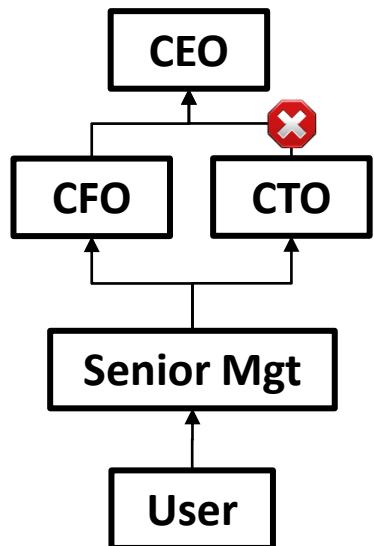
- RBAC- Role Based Acces Control: RBAC₀

URA		CEO CFO CTO SeniorMgt User				
jDoe	X			X		
eSmith		X	X	X		
jPurple		X	X	X		
sWhite				X		

PRA		File 1 File 1 File 1 File 1 File 1 File 1					
CEO	X X			X X			
CFO	X		X X X X				
CTO	X				X X		
Senior Mgt					X X X		
User					X X X X X X		

- RBAC- Role Based Acces Control: RBAC₁

Possibilité de bloquer l'héritage en utilisant des rôles «privés»



	File 1			File 1			File 1			File 1			File 1			File 1		
	R	W	X	R	W	X	R	W	X	R	W	X	R	W	X	R	W	X
CEO	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CFO	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CTO		X					X	X	X	X	X	X	X	X	X	X	X	X
Senior Mgt							X	X	X	X	X	X	X	X	X	X	X	X
User							X	X	X	X	X	X	X	X	X	X	X	X

Contrôle d'Accès

- RBAC- Role Based Acces Control: RBAC₂

URA

	CEO	CFO	CTO	Senior Mgt	User
jDoe	X			X	
eSmith	X		X	X	
jPurple		X	X	X	
sWhite				X	

Contraintes

- Acceptable, Non-Acceptable
- Exclusion mutuelle, cardinalité, rôle prérequis

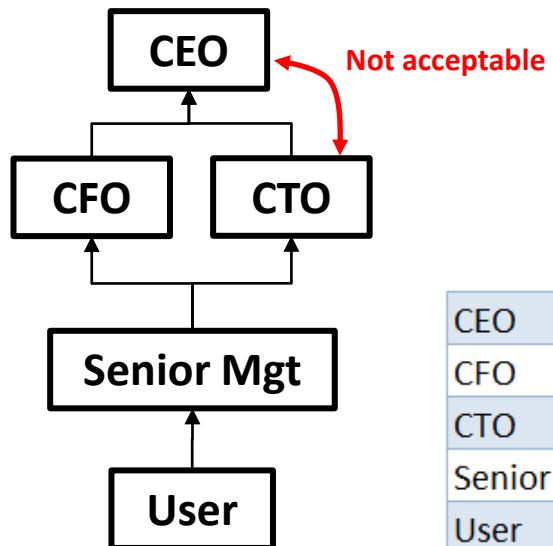
PRA

File 1 | File 1

	R	W	X	R	W	X	R	W	X	R	W	X	R	W	X
CEO	X	X			X	X									
CFO	X			X	X	X	X								
CTO	X							X	X						
Senior Mgt								X	X	X					
User								X	X	X	X	X	X	X	X

- RBAC- Role Based Access Control: RBAC₃

Contraintes & Hiérarchie



	File 1			File 2			File 3			File 4			File 5			File 6		
	R	W	X	R	W	X	R	W	X	R	W	X	R	W	X	R	W	X
CEO	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CFO		X		X	X	X	X		X	X	X	X	X	X	X	X	X	X
CTO		X				X		X	X	X	X	X	X	X	X	X	X	X
Senior Mgt							X	X	X	X	X	X	X	X	X	X	X	X
User								X	X	X	X	X	X	X	X	X	X	X

Un arc rouge entre CTO et Senior Mgt est étiqueté "Not acceptable".

- **RBAC- Role Based Acces Control:**

□ Avantages

- Passage à l'échelle
- S'adapte facilement aux organisations:
 - Organisation flexible
 - Turn over
- Customisation des droits (contraintes et hiérarchies)



□ Limites

- Difficile à mettre en œuvre si la hiérarchie et les rôles sont faiblement documenté
- Politique organisationnelle trop détaillée peut freiner la croissance de l'entreprise

□ Exemple d'utilisation

- Produit CISCO, OS Windows, Solaris, HP

Gestion des Contrôles d'Accès

- [-] Protocoles d'authentification
- [-] Technologies des contrôles d'accès

• Gestion des Contrôles d'Accès

- ❑ Administration des contrôles d'accès centralisée
 - Une entité surveille les accès de toutes les ressources
 - Une seule entité peut changer les droits d'accès
- ❑ Administration des contrôles d'accès décentralisé
 - Contrôle d'accès aux entités proches des ressources
 - Plus de flexibilité et rapidité
 - Pas d'uniformisation de contrôle d'accès
 - Plusieurs entités sont habilitées à changer les droits d'accès
- ❑ Technologies du contrôle d'accès centralisé (AAA)
 - Radius
 - Tacacs
 - Diameter



- **Protocol d'authentification**

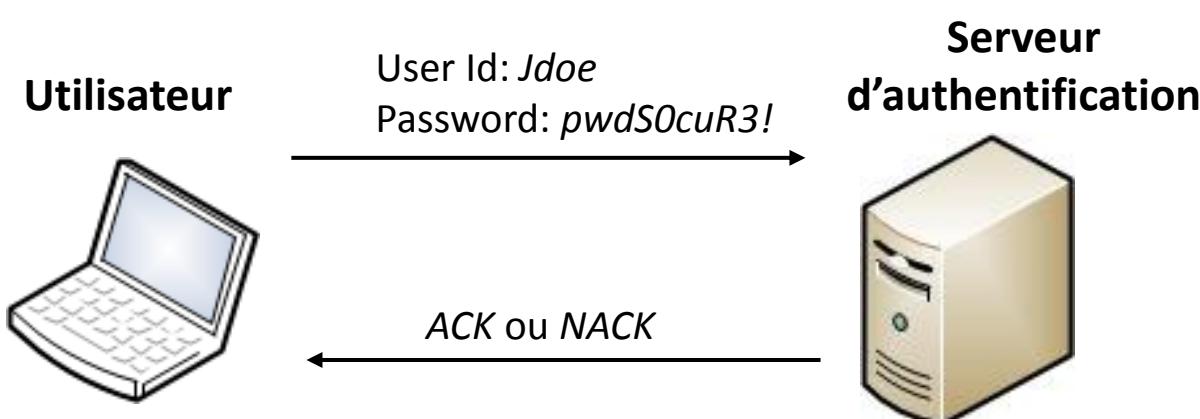
- Password Authentication Protocol (**PAP**)
- Challenge-Handshake Authentication Protocol (**CHAP**)
- Extensible Authentication Protocol (**EAP**)



• Protocol d'authentification

❑ Password Authentication Protocol (PAP)

- Transmet le mot de passe en clair au serveur d'authentification
 - Plus vraiment utilisé (faible niveau de sécurité)
 - Supporté par tous les réseaux
- Vulnérable sniffing et man in the middle attack



- **Protocol d'authentification**

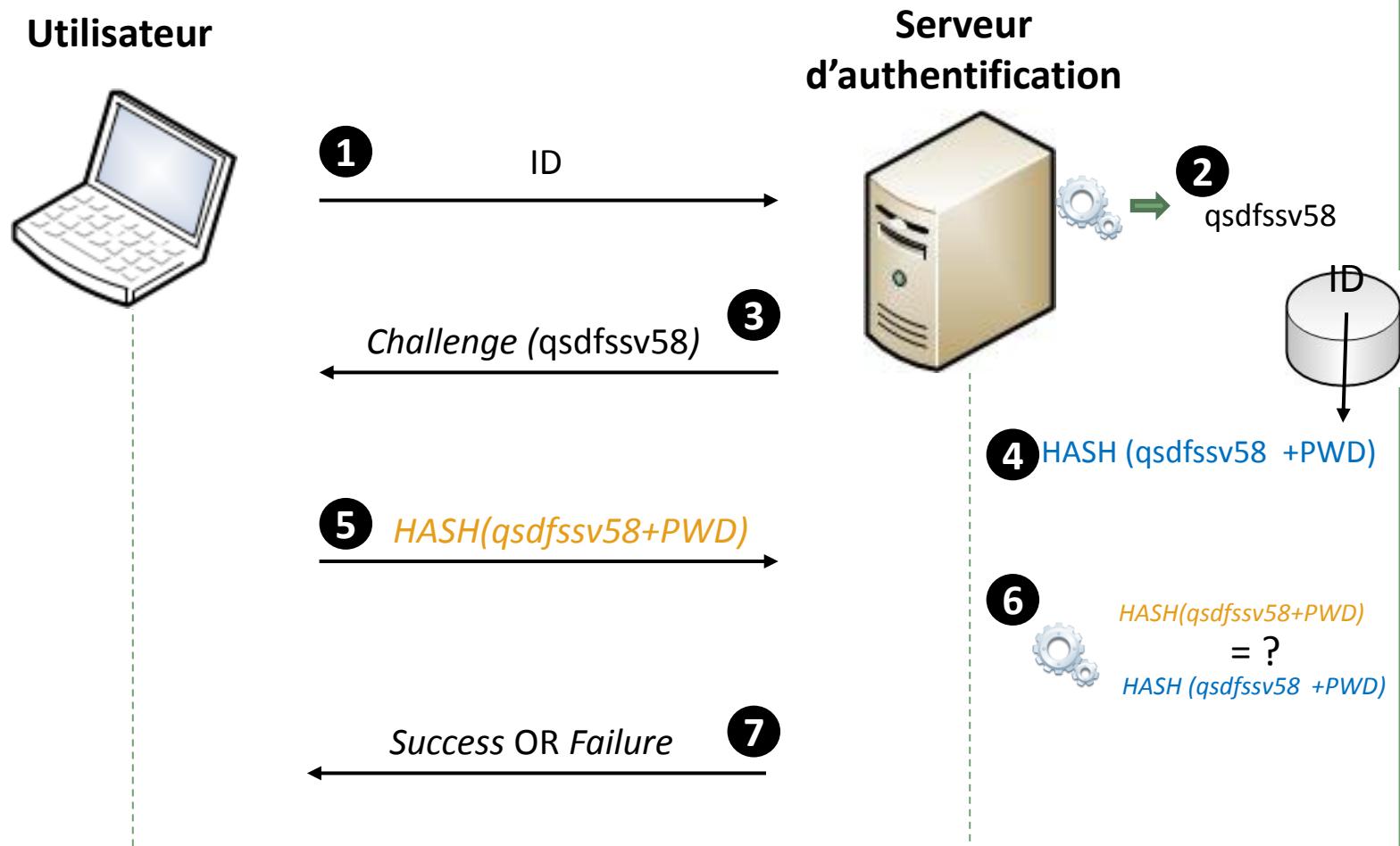
- **Challenge-Handshake Authentication Protocol (CHAP)**

- Authentification via Challenge réponse
 - Pas de mot de passe transmis en clair

→ Non Vulnérable à man in the middle attaque car challenge réponse tout au long de la connexion



- CHAP - Challenge-Handshake Authentication Protocol



• Protocol d'authentification

Extensible Authentication Protocol (EAP)

- Universel, utilisé surtout dans les réseaux sans fils et les liaisons Point à Point
- Extensible, les méthodes d'authentification peuvent être personnalisées
- Des méthodes d'authentification par défaut (MD5, Generic Token Card...)
- L'authentification peut être mutuelle

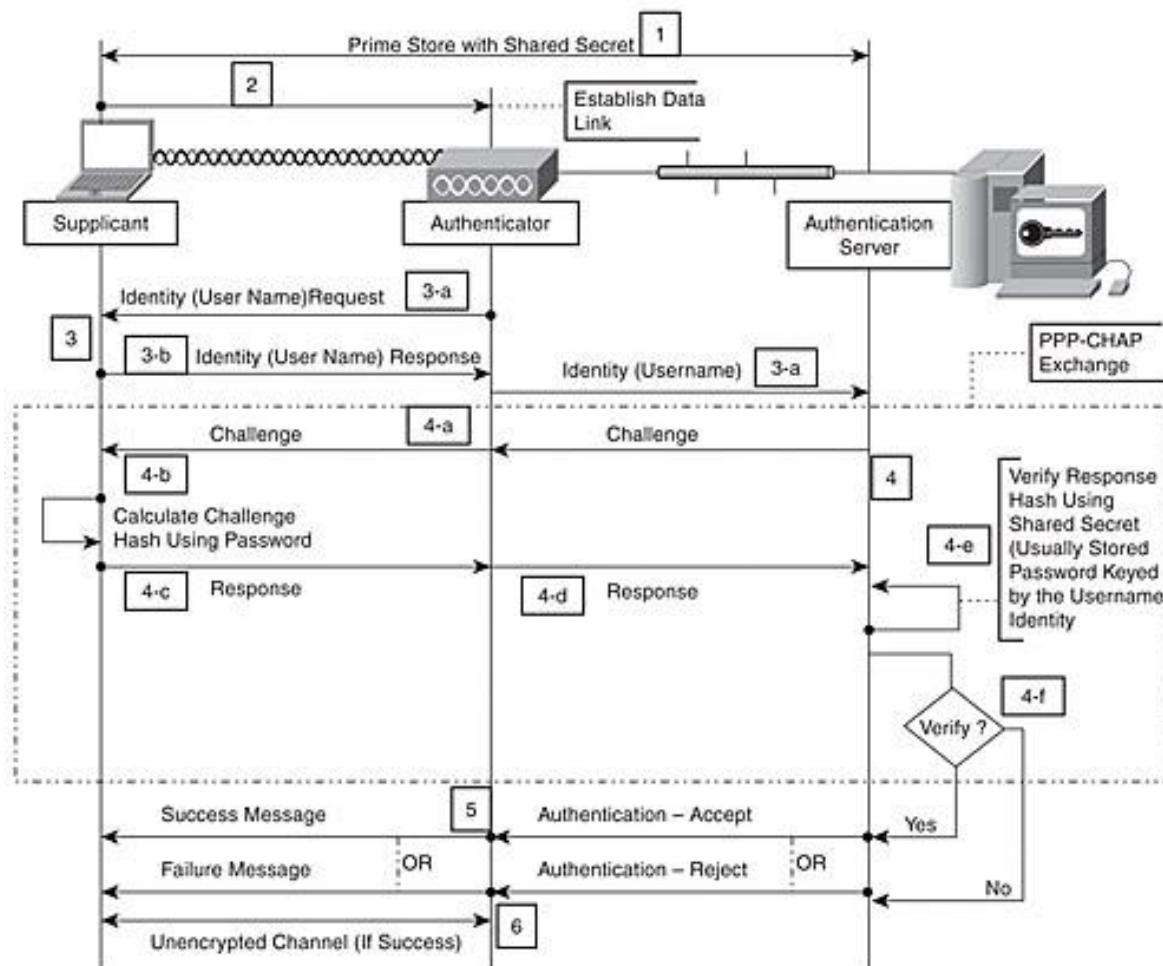
Exemples de protocoles:

- EAP-TLS (Transport Level Security)
- EAP-MD5 (Message Digest 5)
- EAP-PEAP (Protected Extensible Authentication Protocol)
- EAP-TTLS (Tunneled Transport Level Security)

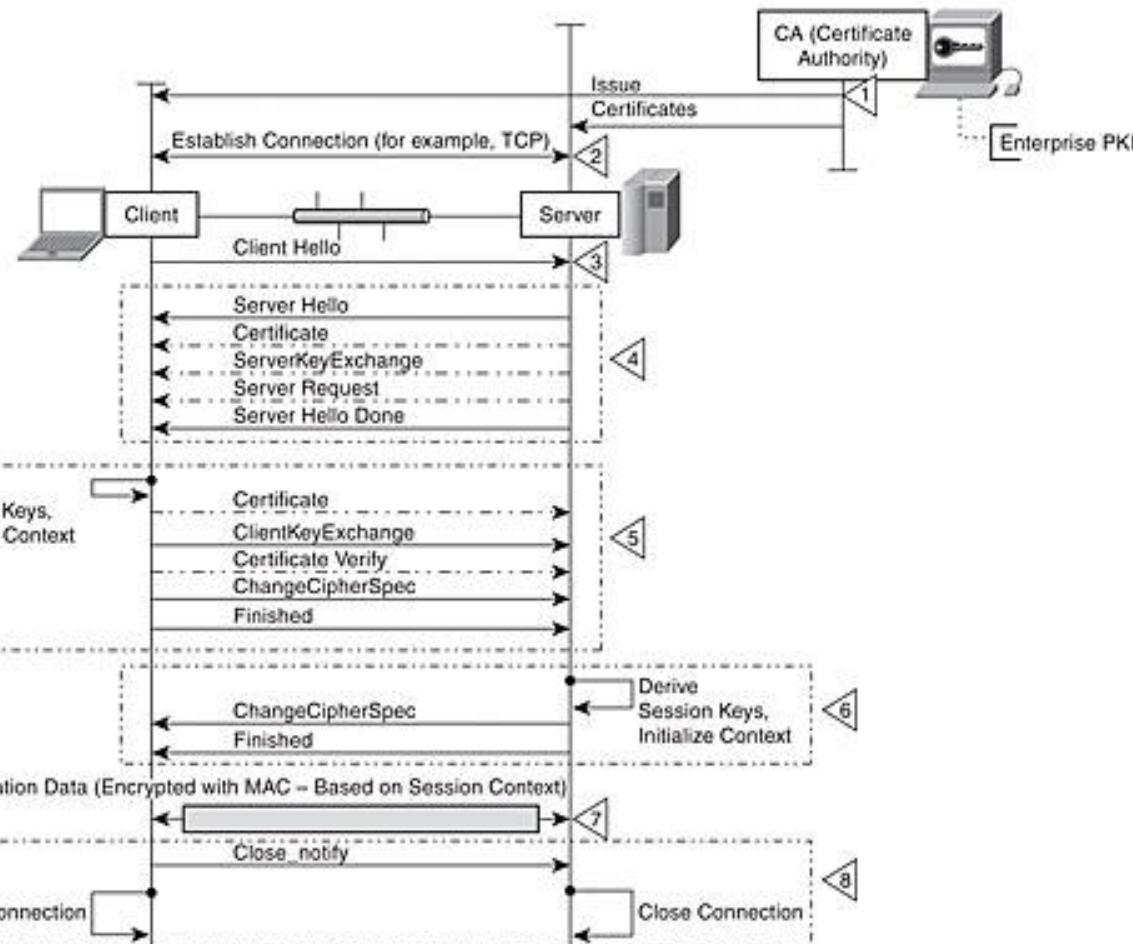


Contrôle d'Accès

EAP-MD5 - Extensible Authentication Protocol - Message Digest 5



- EAP-TLS - Extensible Authentication Protocol - Transport Level Security



<http://www.securityskeptic.com/CH07-2.html>

Gestion des Contrôles d'Accès

- [-] Protocoles d'authentification
- [-] Technologies des contrôles d'accès

- Technologies du contrôle d'accès centralisé

- Remote Authentication Dial-In User Service
RADIUS (RFC2865)
- Terminal Access Controller Access Control System
TACACS (xtabacs RFC1492)
- Diameter (RFC3588)



- Technologies du contrôle d'accès centralisé: Radius

- Propriétés de base

Utilise le protocole AAA pour transporter les informations

d'authentification d'un client (e.g Network Access Server) vers un serveur AAA

- Propriétés

- Modèle client/serveur

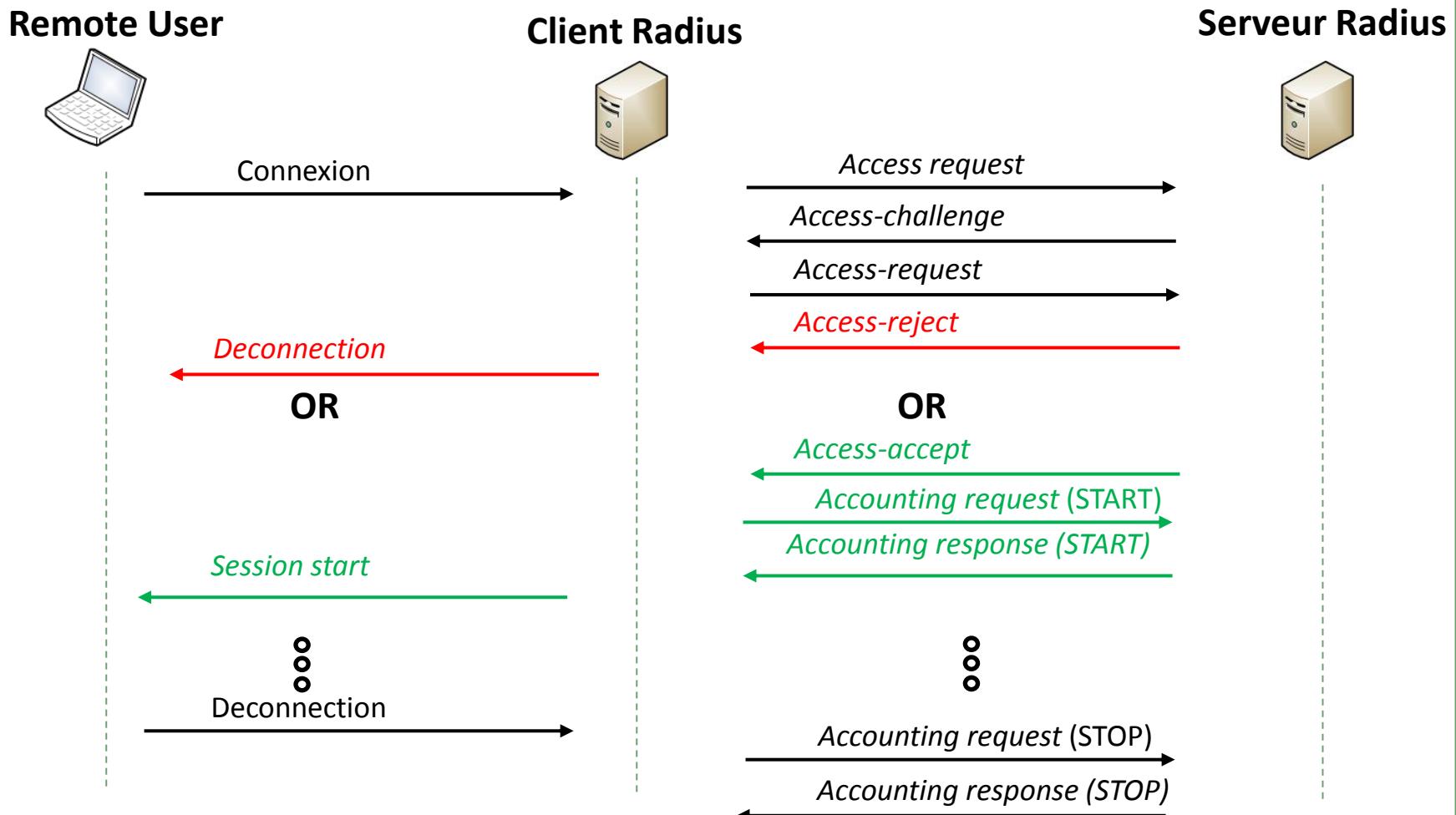
- Client: NAS (Network Access Server) → génère des requêtes d'authentification AAA
 - Serveur: serveur Radius traite les requêtes AAA (joue également le rôle de proxy)

- Sécurité réseau

- Transactions authentifiées via un secret partagé entre le client et le serveur
 - Tous les mots de passe sont masqués (utilisation de Hash MD5)
 - Supporte plusieurs protocoles d'authentification (PAP, CHAP, EAP)
 - Utilise UDP comme couche de transport

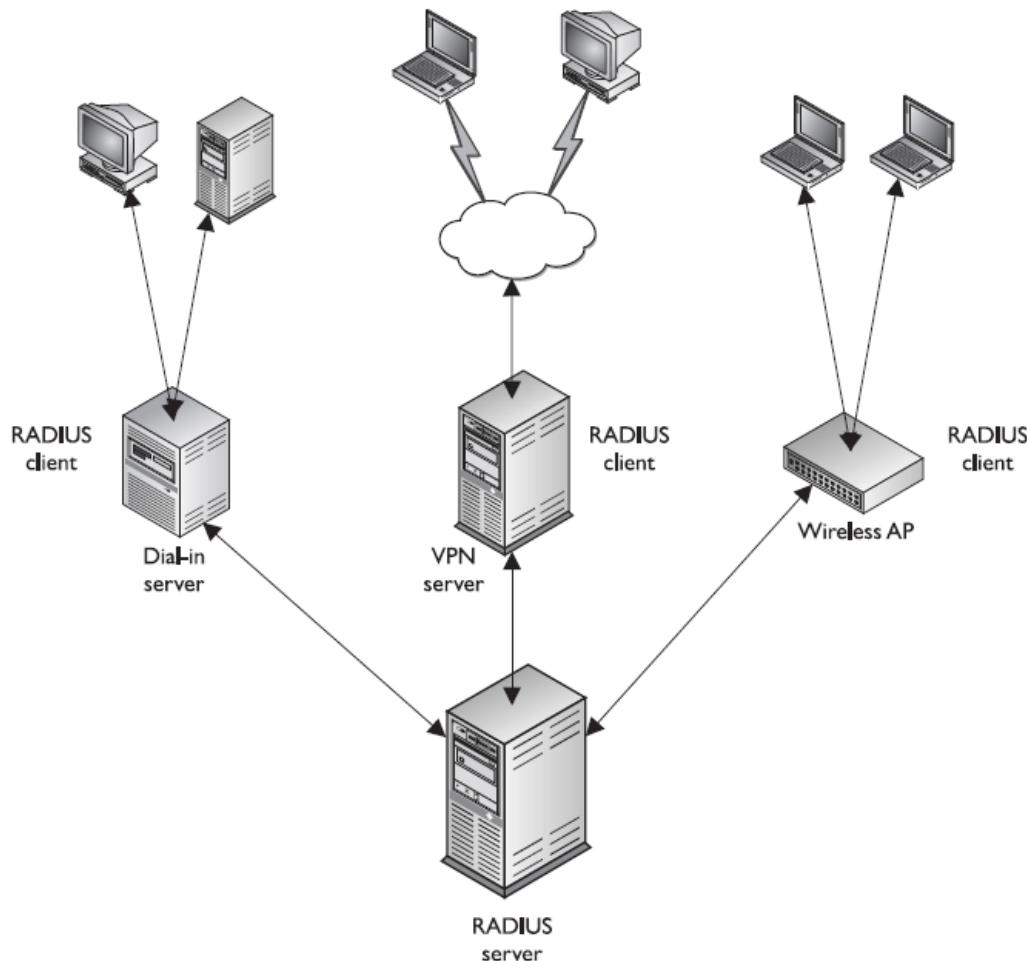


- Technologies du contrôle d'accès centralisé: Radius



Contrôle d'Accès

- Technologies du contrôle d'accès centralisé: Radius



- Technologies du contrôle d'accès centralisé: Radius

- Avantages

- Nature non-connectée
 - Possibilité de faire des rebonds d'authentification sur un autre serveur



- Limites

- Les couches applicatives doivent gérer la prise en compte de perte de paquets
 - UDP non adapté aux congestions réseaux (TCP oui)

- Technologies du contrôle d'accès centralisé: Tabacs

- 3 Générations

- **TACACS** (1984): combinaison des processus d'authentification et d'autorisation (système UNIX)
 - **XTACACS** (1993): Séparation des processus d'authentification, d'autorisation et d'audit (accounting)
 - **TACACS+** (1998): ajout de l'authentification selon 2 facteurs, possibilité d'utiliser des mots de passe à usage unique (CISCO)

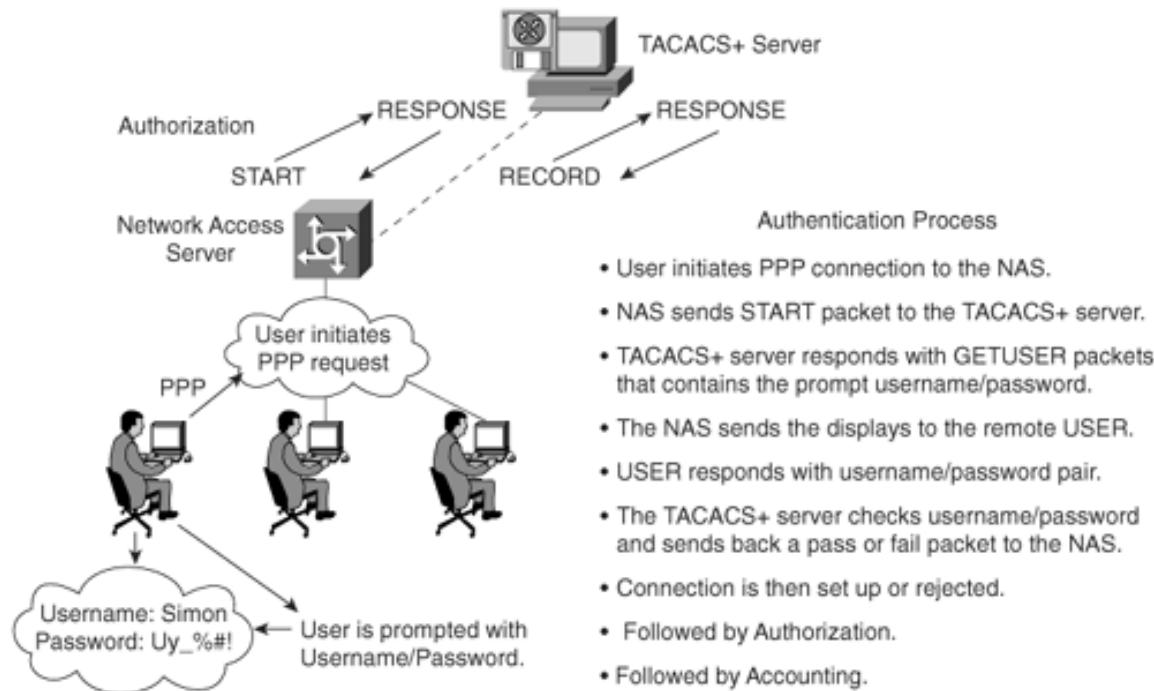
- Mêmes fonctions que RADIUS

- Mais des particularités

- Utilise TCP
 - Toutes les informations d'authentification sont chiffrées
 - Administration plus flexible due à la séparation authentification, autorisation, audit (accounting)



- Technologies du contrôle d'accès centralisé: TACACS



- Technologies du contrôle d'accès centralisé: RADIUS VS TACACS

	RADIUS	TACACS+
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password from the RADIUS client to the server.	Encrypts all traffic between the client and server.
AAA support	Combines authentication and authorization services.	Uses the AAA architecture, separating authentication, authorization, and auditing.
Multiprotocol support	Works over PPP connections.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Responses	Uses single-challenge response when authenticating a user, which is used for all AAA activities.	Uses multiple-challenge response for each of the AAA processes. Each AAA activity must be authenticated.

- Technologies du contrôle d'accès centralisé: Diameter

- Dérivé de Radius

- Mais en plus

- Framework général pour les futures applications AAA
 - Architecture Peer to Peer
 - Notification d'erreurs
 - Service de base pour les applications (support de session utilisateur, audit maintenance de l'état d'une session)
 - Communication entre les composants de Diameter en IPSec (TLS possible optionnel)
 - Authentification entre chaque « nœud » par secret partagé
 - Transport sur TCP et SCTP (client agent et serveur)



- Technologies du contrôle d'accès centralisé: Diameter

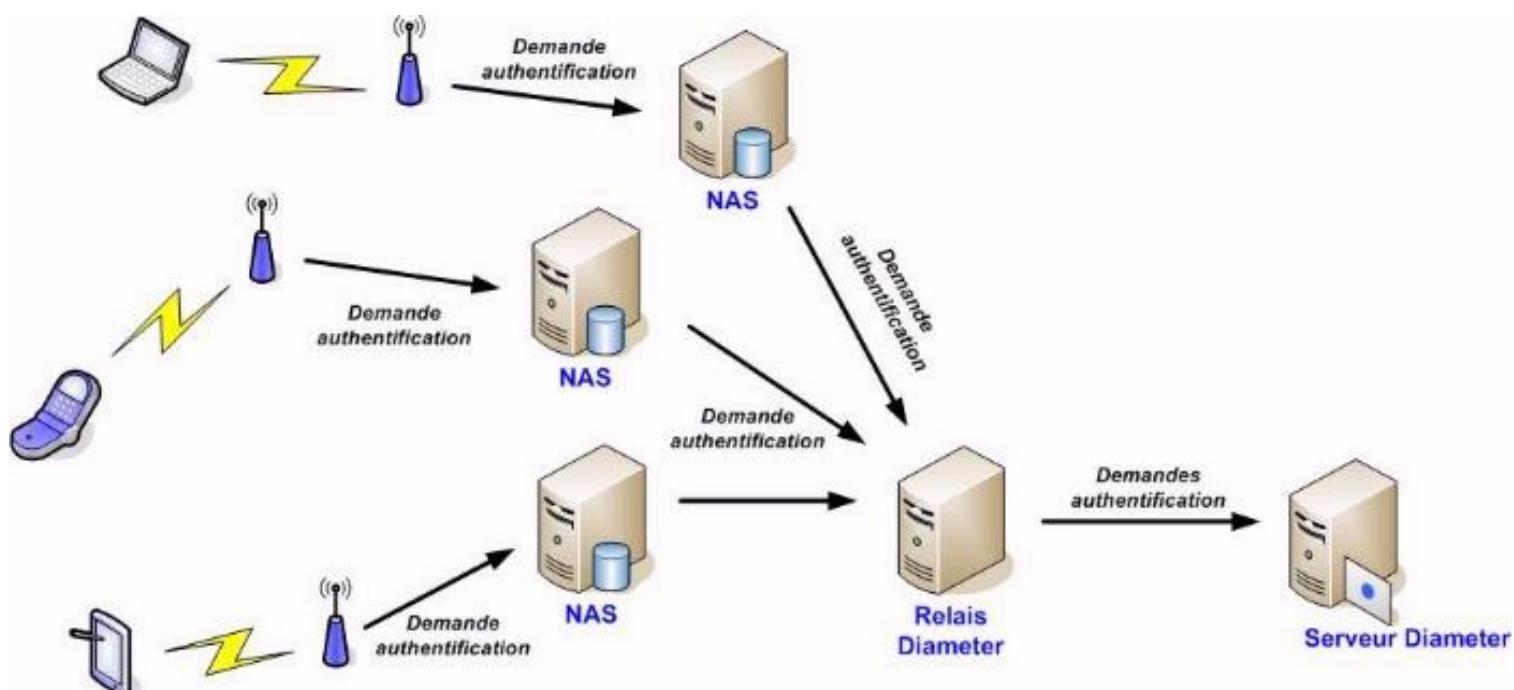
Les composants

- **Node:** *Diameter Client, Diameter Agent, Diameter Client*
- **Diameter Client:** *Nœud recevant les requêtes de connection*
- **Diameter Agent**
 - **Relay Agent:** *Nœud transférant les messages aux destinations appropriées. Sert d'aggregateur de message d'authentification.*
 - **Proxy Agent:** *Nœud transférant les messages aux destinations appropriées, contrairement au Relay agent, il peut modifier les messages*
 - **Redirect Agent, Translation Agent**
- **Diameter Serveur:** *Nœud authentifiant les utilisateurs et délivrant les autorisations*

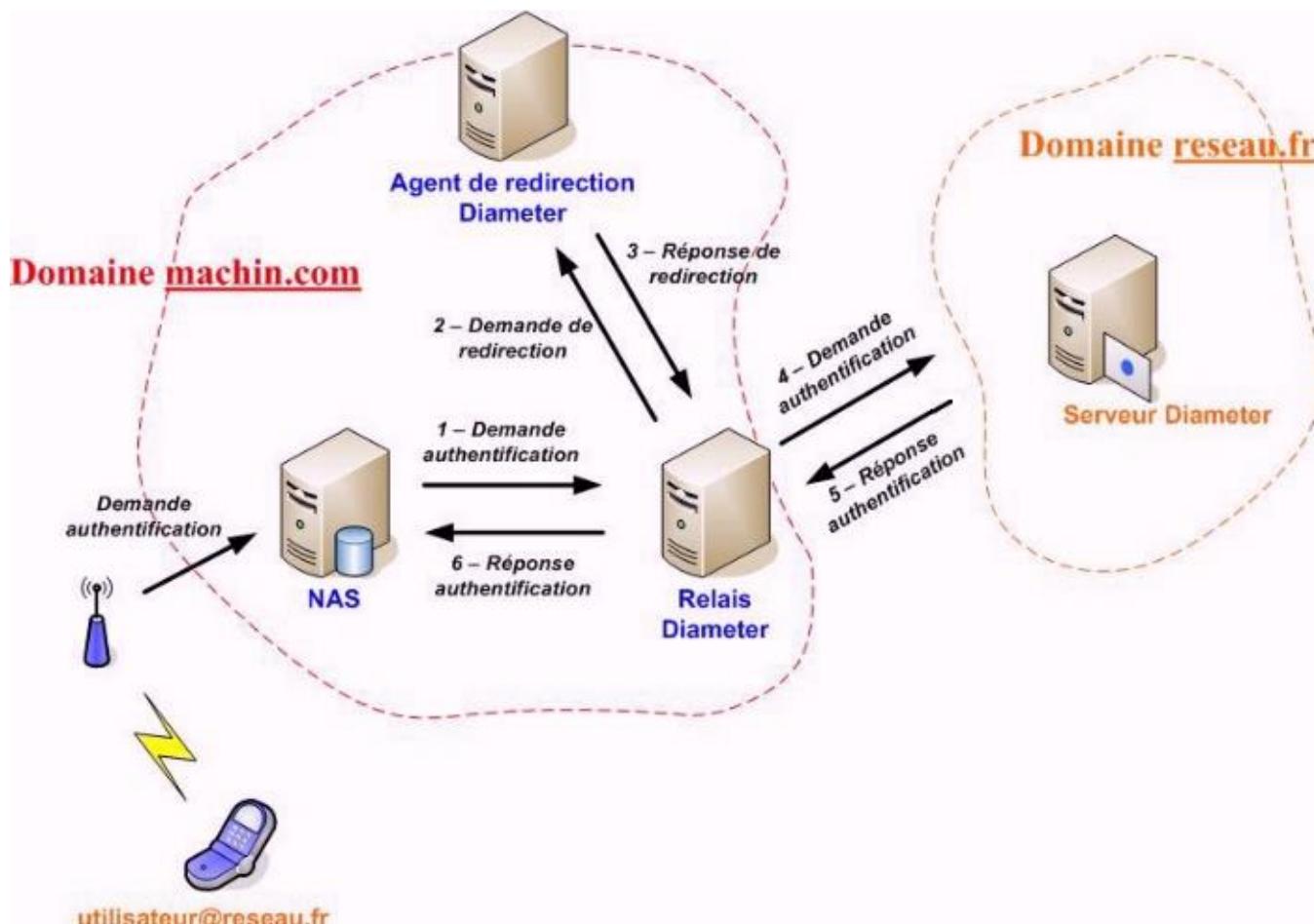


Contrôle d'Accès

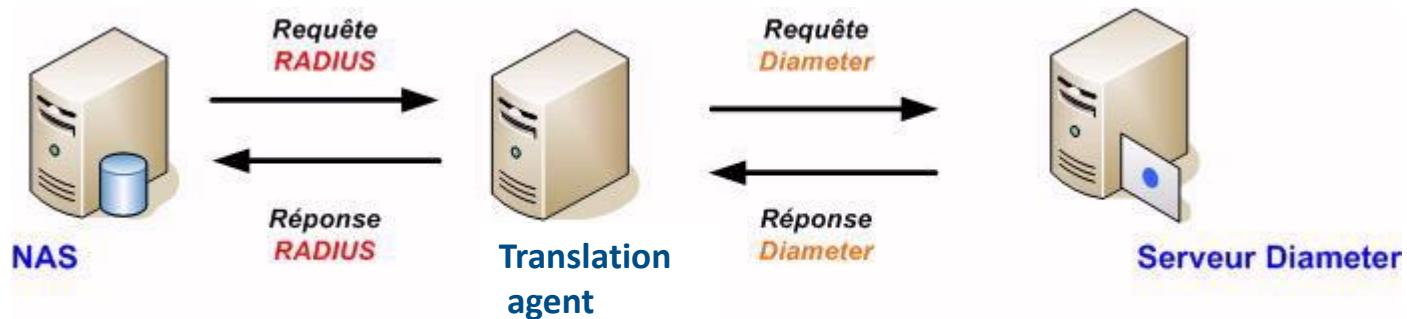
- Technologies du contrôle d'accès centralisé: Diameter



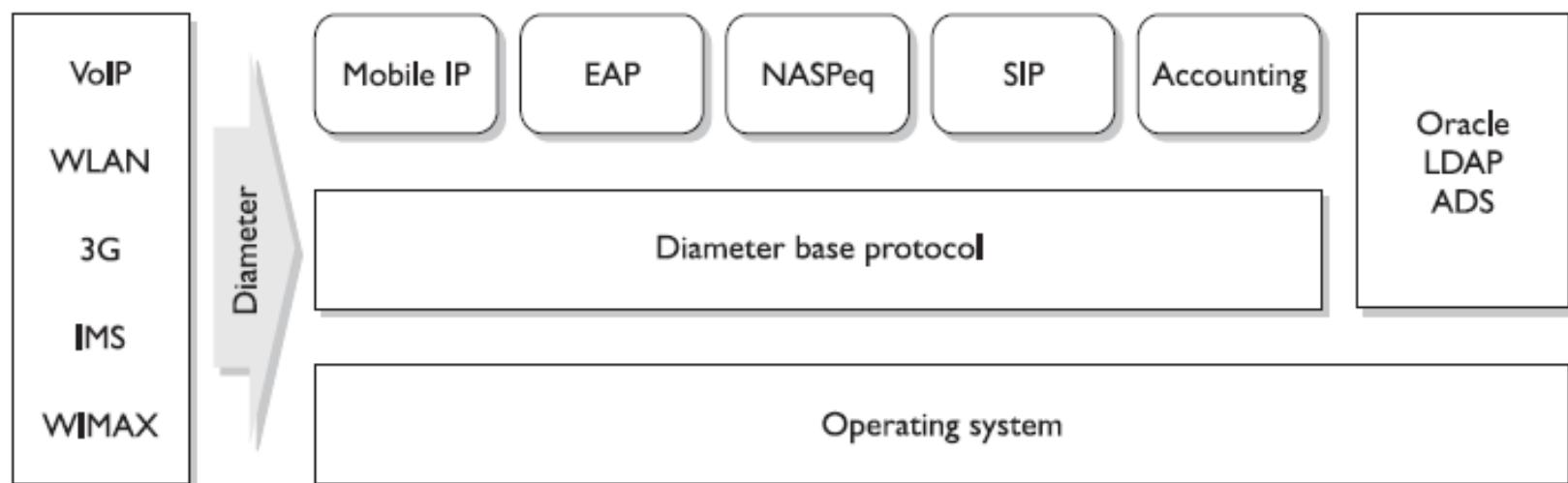
- Technologies du contrôle d'accès centralisé: Diameter



- Technologies du contrôle d'accès centralisé: Diameter



- Technologies du contrôle d'accès centralisé: Diameter



Famille de Contrôles d'Accès

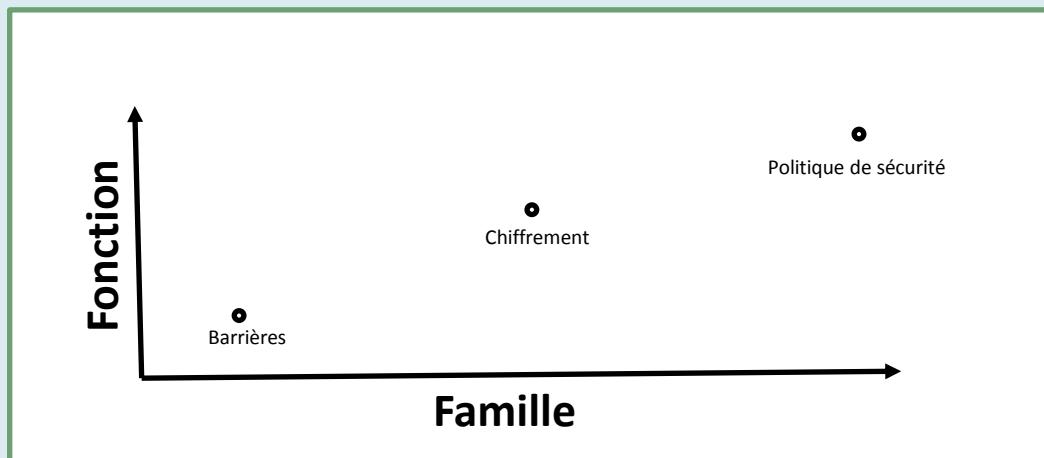
- Famille
- Fonction

- Famille de contrôle d'accès

- Découpage en 2 axes

- **Famille:** Détermine la nature du contrôle d'accès
 - **Fonction:** Détermine à quelle fin est utilisé un contrôle d'accès

SoleStocks



- Famille de contrôle d'accès

- Famille

- Physique

- Périmètre de sécurité, ségrégation des réseaux
 - Contrôle des postes de travail
 - Séparation des zones de travail
 - Câbles
 - Verrous, porte, alarme, détecteurs

- Technique

- Architecture réseau
 - Système de contrôle d'accès
 - Accès réseau
 - Chiffrement et protocole
 - Audit

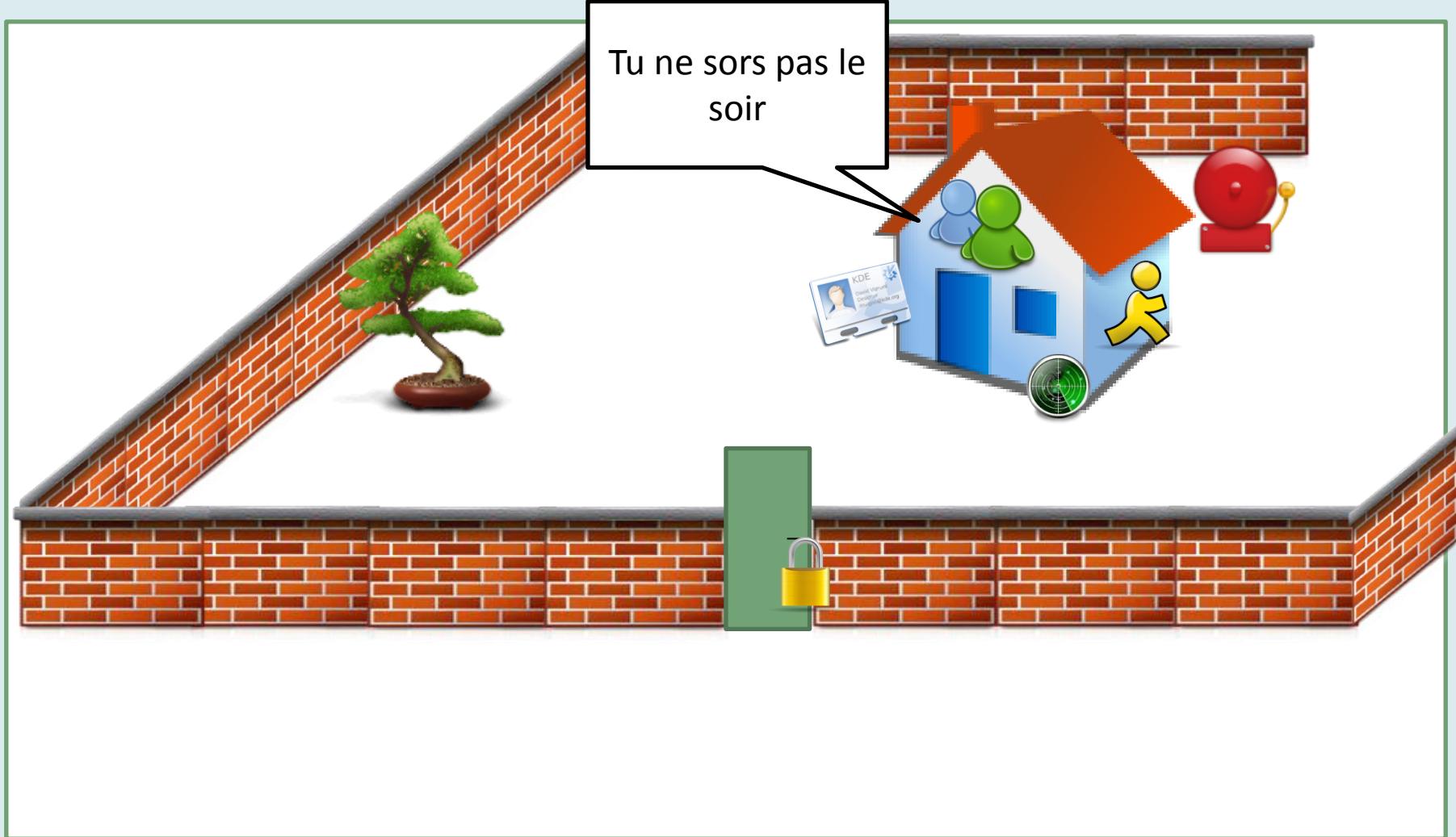
- Administrative

- Politiques et procédures
 - Contrôle du personnel
 - Supervision des structures
 - Formation à la sécurité
 - Tests, validation

SoleStocks



- Famille de contrôle d'accès: Famille



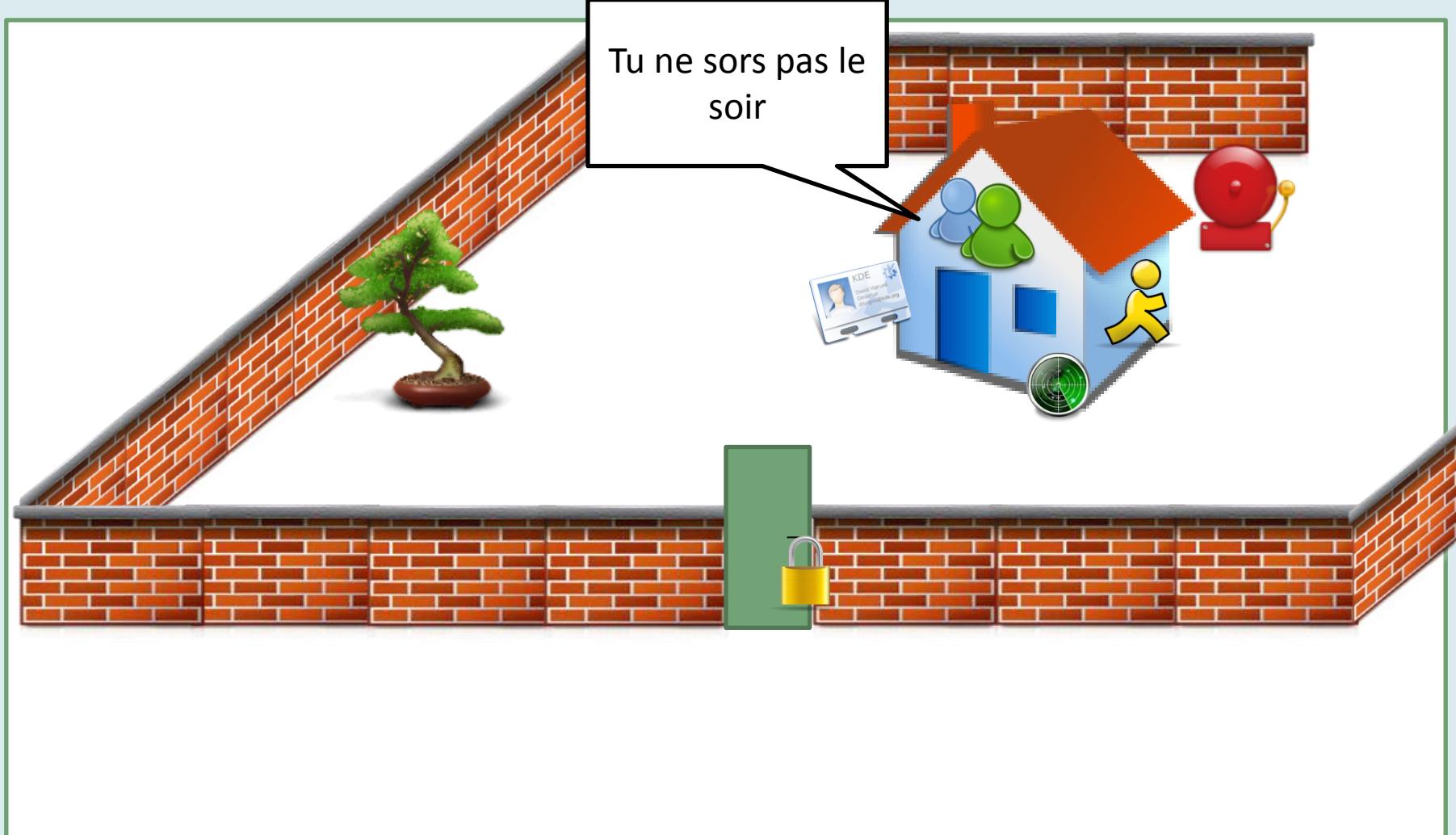
- Famille de contrôle d'accès

- Fonction

- **Dissuasion:** Décourage un attaquant potentiel
 - **Prévention:** Eviter un incident, une attaque
 - **Correction:** Réparer des composants ou système après un incident ou une attaque
 - **Récupération:** Retourner à une situation stable
 - **Détection:** Aider à identifier les activités d'un incident ou d'une attaque
 - **Compensation:** Fournir une alternative à des contrôles existants
 - **Directive:** Contrôle obligatoire due à des contraintes réglementaires ou des besoins environnementaux



- Famille de contrôle d'accès: Famille



- Famille de contrôle d'accès**

Type of Control:	Preventive	Detective	Corrective	Deterrent	Recovery	Compensative
	Avoid undesirable events from occurring	Identify undesirable events that have occurred	Correct undesirable events that have occurred	Discourage security violations	Restore resources and capabilities	Provide alternatives to other controls
Category of Control:						
Physical						
Fences				X		X
Locks	X					X
Badge system	X					X
Security guard	X					X
Biometric system	X					X
Mantrap doors	X					X
Lighting				X		X
Motion detectors		X				X
Closed-circuit TVs		X				X
Offsite facility					X	X
Administrative						
Security policy	X					X
Monitoring and supervising		X				X
Separation of duties	X					X
Job rotation		X				X

- Famille de contrôle d'accès**

Type of Control:	Preventive	Detective	Corrective	Deterrent	Recovery	Compensative
Information classification	X				X	
Personnel procedures	X				X	
Investigations		X			X	
Testing	X				X	
Security-awareness training	X				X	
Technical						
ACLs	X				X	
Routers	X				X	
Encryption	X				X	
Audit logs		X			X	
IDS		X			X	
Antivirus software	X		X		X	
Server images			X		X	
Smart cards	X				X	
Dial-up call-back systems	X				X	
Data backup				X	X	

Conclusion

Confidentialité

Intégrité

Disponibilité

Objectifs de sécurité

Concepts et définitions

Sujet Objet Accès

Identification AAA

3 facteurs d'authentification

Management d'identité

Gestion des mots de passe

Gestion Id web

Gestion des Comptes

Annuaire

X500- LDAP

Moyen d'authentification

Mots de Passe

Memory/Smart Cards

Biométrie

Concepts et définitions

Sujet Objet Accès

Identification AAA

3 facteurs d'authentification

Confidentialité

Intégrité

Disponibilité

Management d'identité

Gestion des mots de passe

Gestion Id web

Gestion des Comptes

Annuaire

X500- LDAP

Moyen d'authentification

Mots de Passe

Memory/Smart Cards

Biométrie

Concepts et définitions

Sujet Objet Accès

Identification AAA

3 facteurs d'authentification

Authorisation

Règles

Outils
Kerberos
SESAME

Confidentialité
Intégrité

Objectifs de sécurité

Disponibilité

CONTRÔLE D'ACCÈS

Management d'identité

Technologies et protocoles de contrôle d'accès

Gestion des mots de passe

Gestion Id web

Gestion des Comptes

Technologie de contrôle d'accès

Radius, Tabacs, Diameter

Protocol d'auth

PAP,CHAP,EAP

Annuaire

X500- LDAP

Authorisation

Règles

Outils
Kerberos
SESAME

Moyen d'authentification

Modèle de Contrôle d'accès

Mots de Passe

Memory/Smart Cards

Biométrie

DAC MAC RBAC

Concepts et définitions

Sujet Objet Accès

Identification AAA

3 facteurs d'authentification

Confidentialité

Intégrité

Disponibilité

Questions ?
