Sécurité :
Contrôle d'Accès

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

J. Saraydaryan

CPE LYON

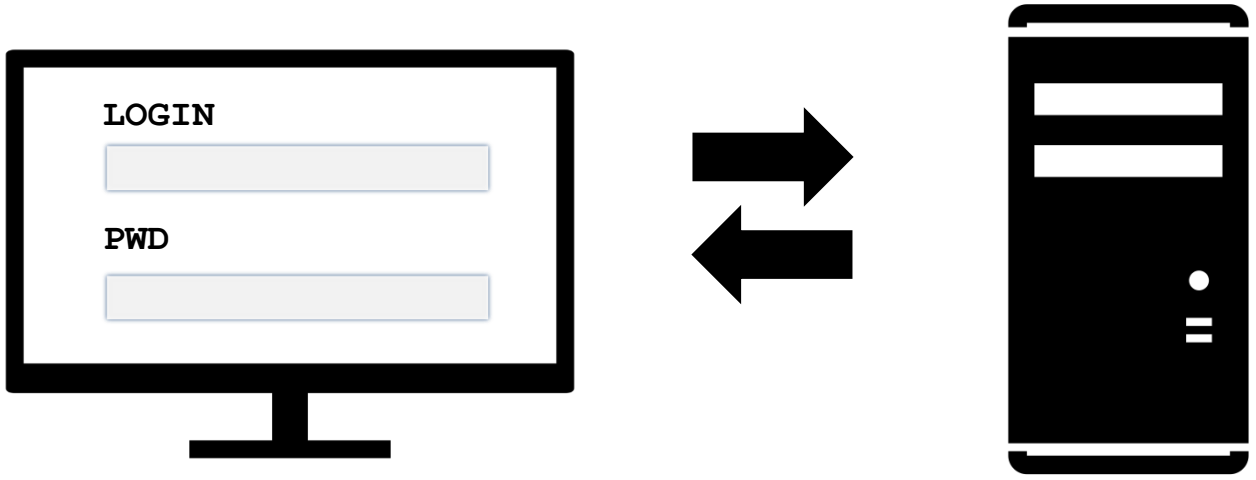
OutLine

- Besoins et définitions
- Gestion des contrôles d'accès
- Autorisation
- Modèles de contrôle d'accès
- Familles de contrôle d'accès

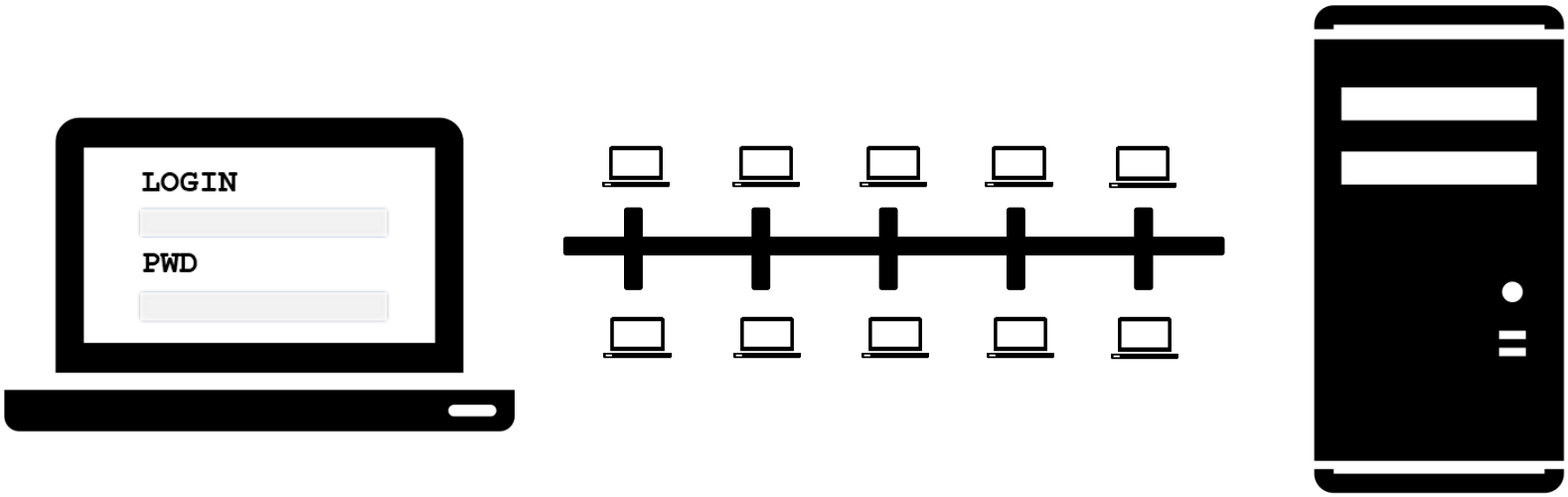
CPE LYON

Besoins et définition

Contrôle d'accès : Besoins



Contrôle d'accès : Besoins



Contrôle d'accès : Besoins

- **Comment prouver son identité ?**
- **Qu'est ce qui définit notre identité?**
- **Comment mon identité va me permettre d'accéder à des ressources/services ?**

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**

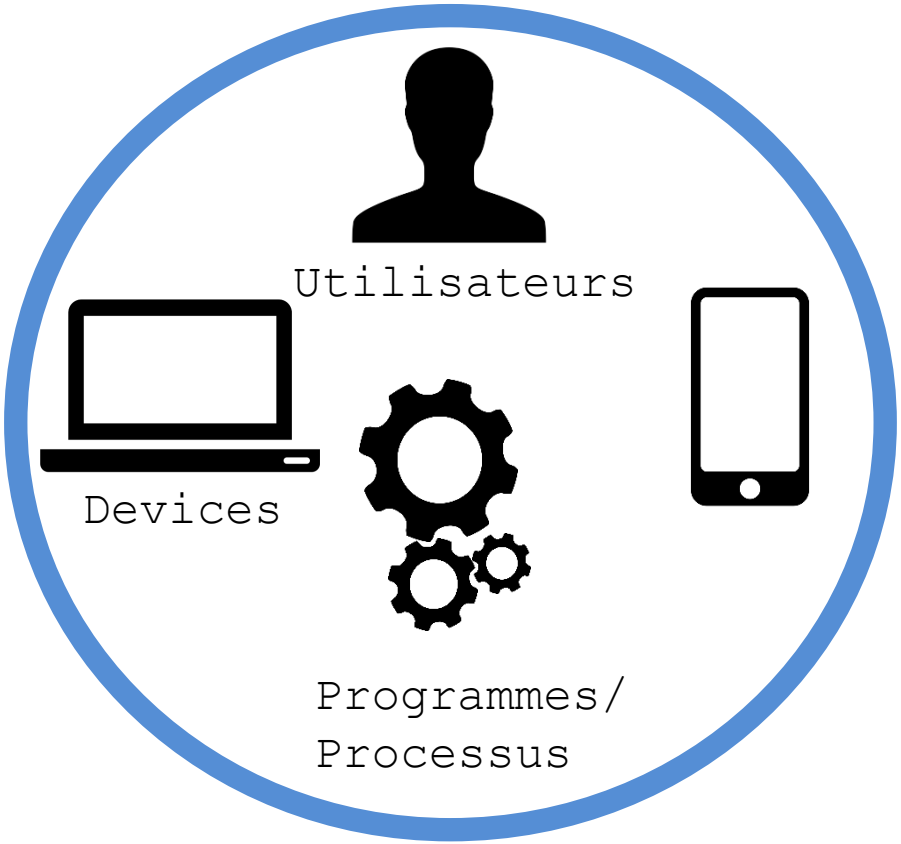
    L'accès est le flux d'information entre un sujet et un objet
  - **Sujet**

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

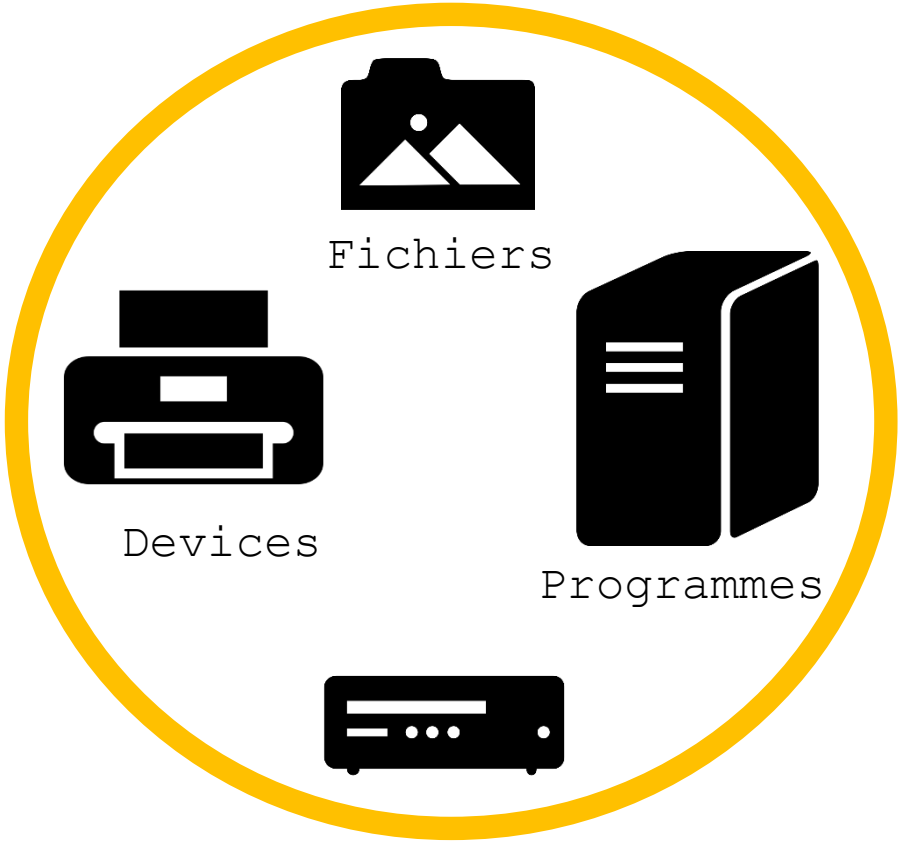
    Entité passive contenant de l'information.

CPE LYON

Contrôle d'accès

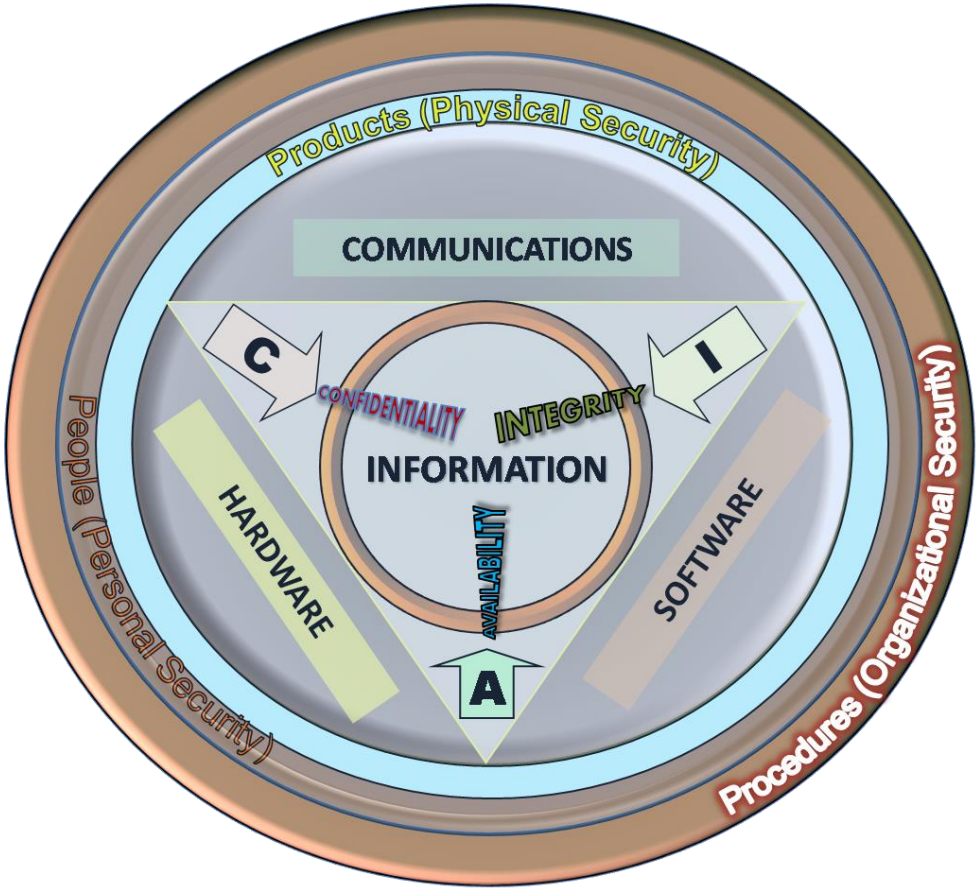


Sujets



Objets

Contrôle d'accès



Identification

- Comment un sujet peut-il être authentifié?
- 3 facteurs:
  - Quelque chose que le sujet connait
  - Quelque chose que le sujet possède
  - Quelque chose qui définit le sujet (ce qu'il est)

Identification

Vérification 1:1	VS	Vérification 1:N
Suis la personne que je prétend être ?		Quelle est cette personne?

Identification

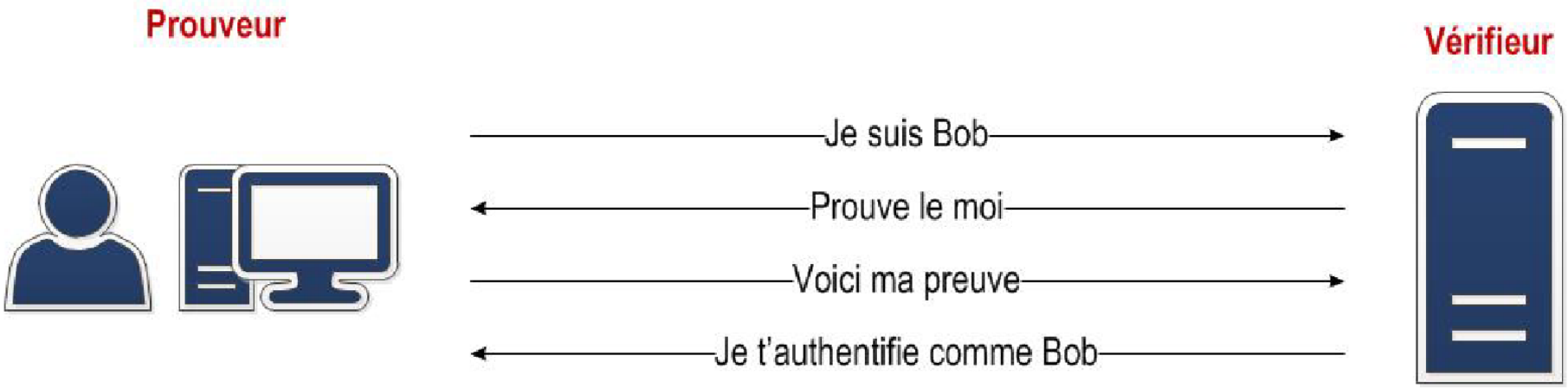


FIGURE 1 – Représentation générique d'une authentification

https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf

Facteurs d'authentification

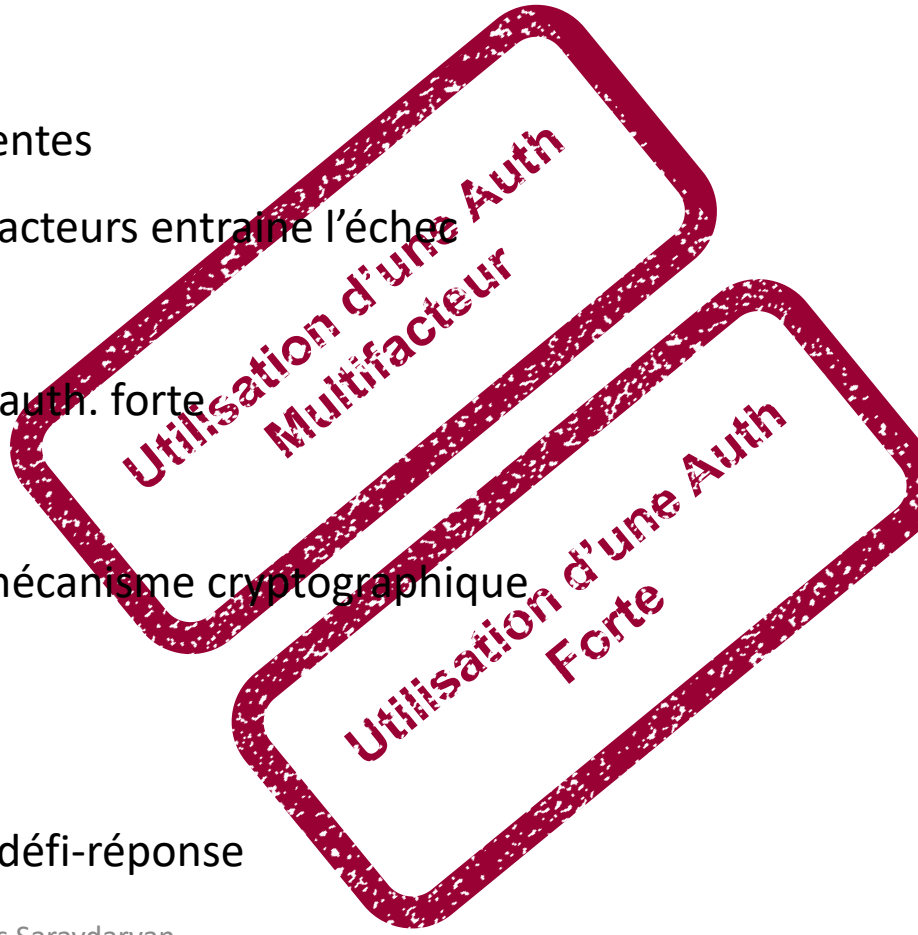
- Quelque chose que le sujet connait
  - Mot de passe
  - Séries de questions
  - Code Pin
- Quelque chose que le sujet possède
  - Clé
  - Badge
  - Certificats numériques / token
- Quelque chose qui définit le sujet (ce qu'il est)
  - Biométrie
  - Comportement

Facteurs d'authentification

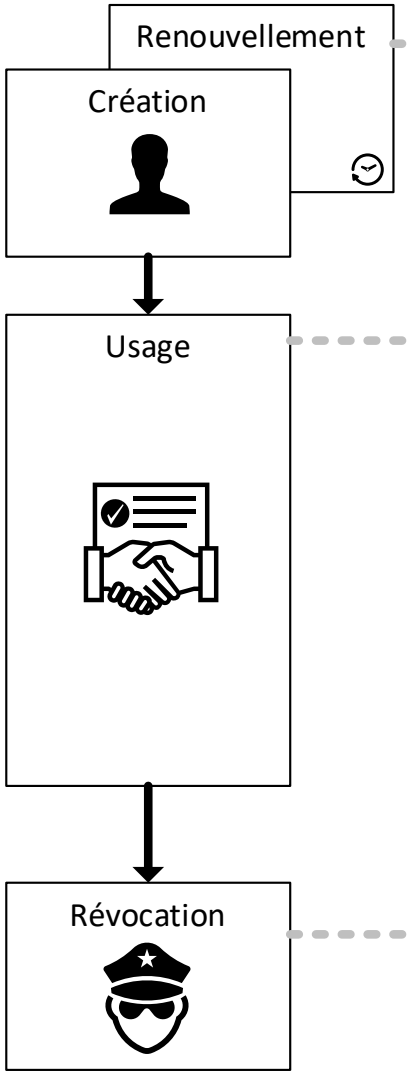
- Quelque chose que le sujet connait
  - Mot de passe
  - Séries de questions
  - Code Pin
- Quelque chose que le sujet possède
  - Clé
  - Badge
  - Certificats numériques / token
- Quelque chose qui définit le sujet (ce qu'il est)
  - Biométrie
  - Comportement

Auth multifacteurs Vs Auth forte

- Authentification MultiFacteurs
  - Utiliser 2 facteurs de nature différentes
  - La non vérification d'un des deux facteurs entraine l'échec d'authentification
  - Multifacteurs pas nécessairement auth. forte
- Authentification Forte
  - Authentification reposant sur un mécanisme cryptographique robuste
- Protocole d'Auth. Fort
  - Repose souvent sur le principe de défi-réponse



Cycle de vie des facteurs



Création du facteur d'auth.

- Présence d'aléatoire
- Usage d'un env. maitrisé
- Protéger les données stockées

Transmission du facteur d'auth

- Vérification de l'identité
- Remise en main propre

Transmission du facteur d'auth

- Usage d'un canal sécurisé
- Ne pas utiliser uniquement les SMS pour le multifacteur

Vérification du facteur d'auth

- Conservation des historiques
- Limitation du nombre de tentatives
- Augmentation du temps entre chaque tentative
- Ne pas informer l'utilisateur sur le type d'échec d'auth
- Vérifier l'expiration du facteur d'auth

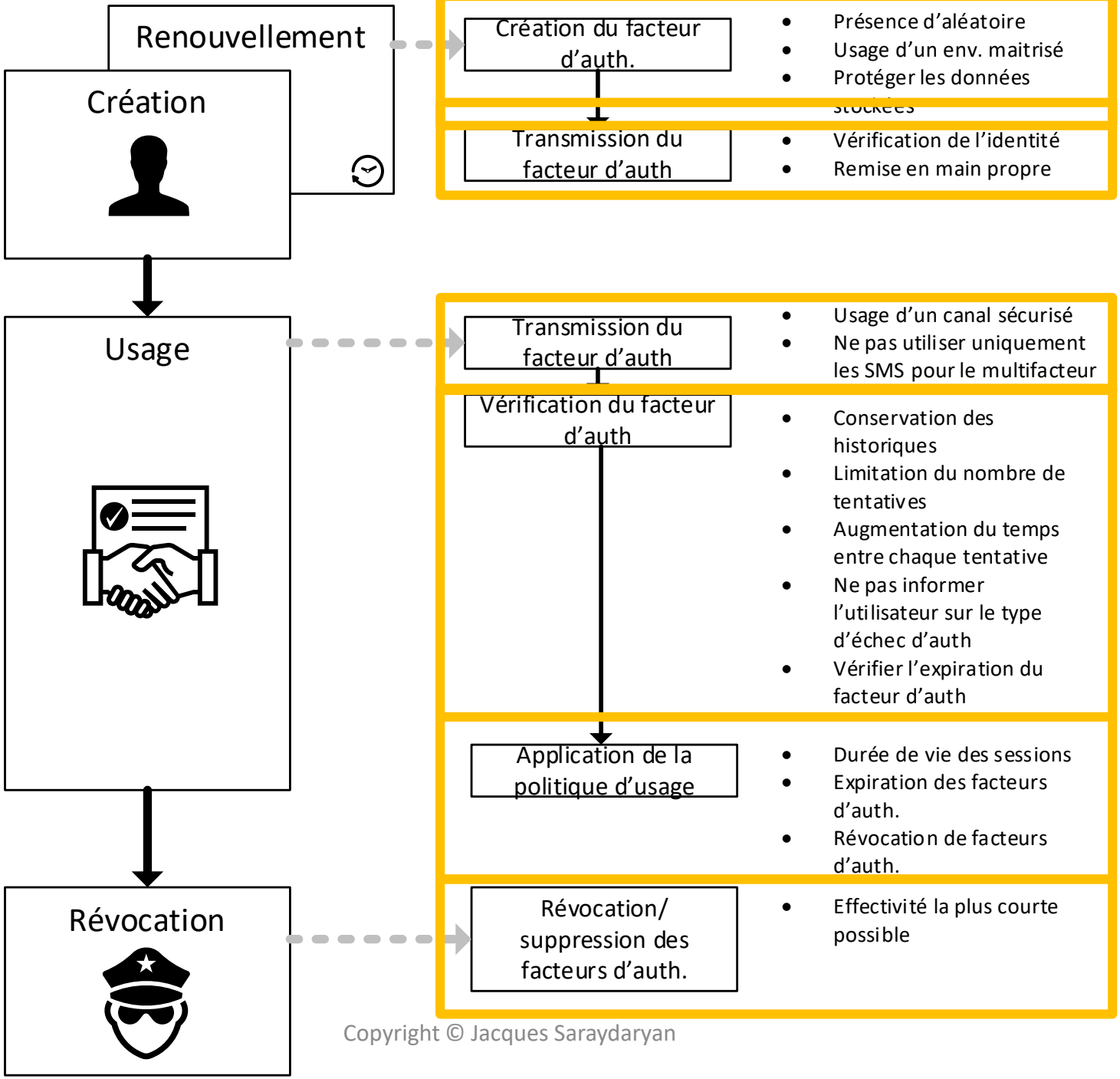
Application de la politique d'usage

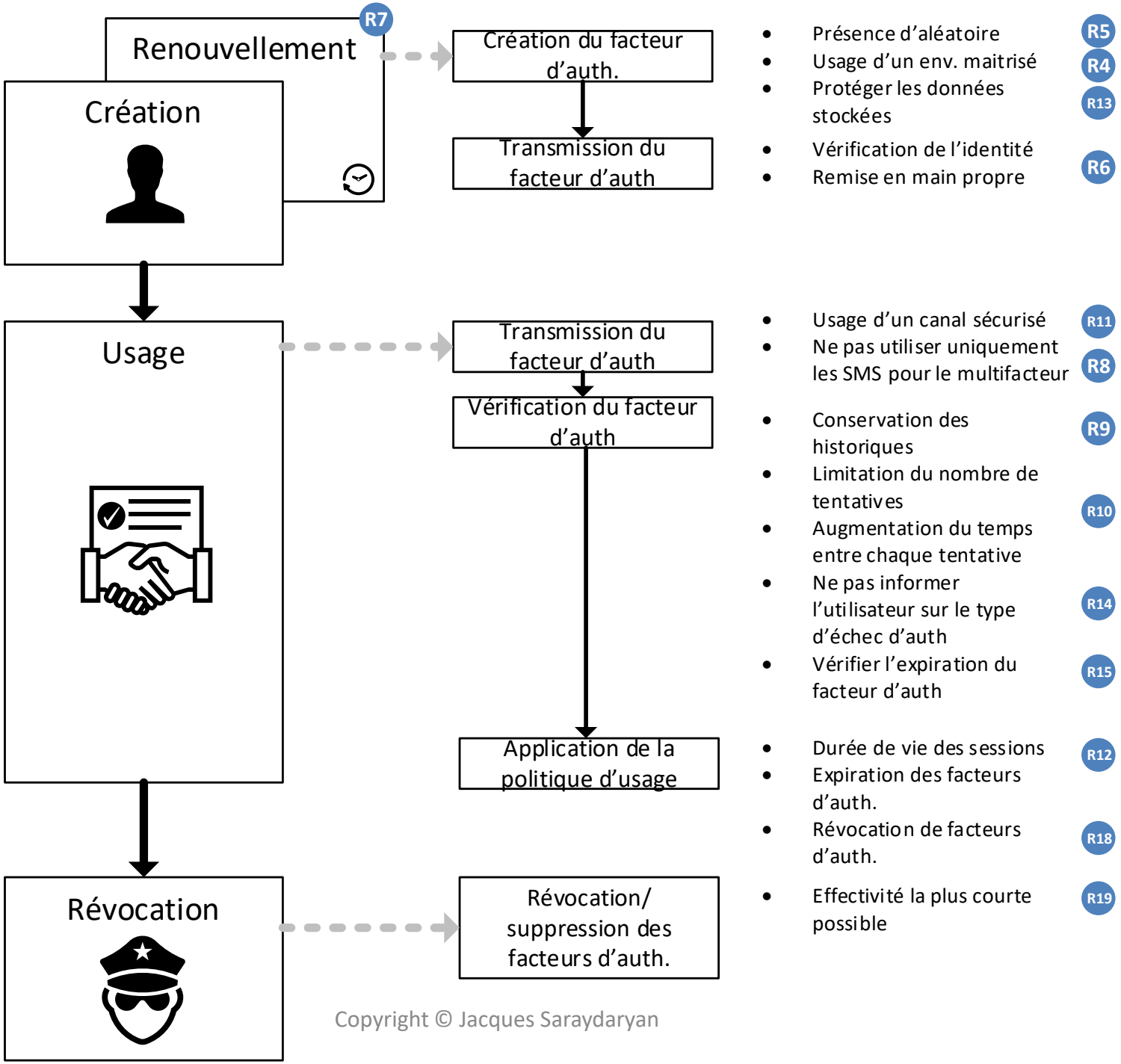
- Durée de vie des sessions
- Expiration des facteurs d'auth.
- Révocation de facteurs d'auth.

Révocation/ suppression des facteurs d'auth.

- Effectivité la plus courte possible

https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf

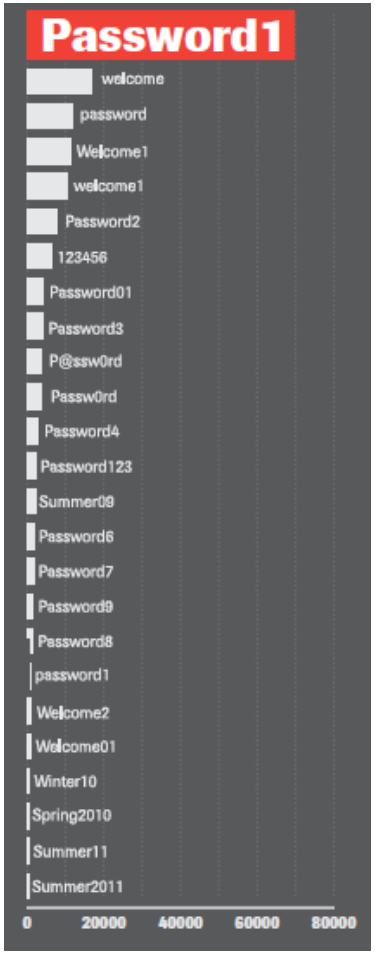




Les mots de passe

- Gestion des mots de passes
  - Les plus utilisés pour l'authentification
  - Complexité et taille élevées nécessaires pour être sûr
- Cible d'attaques
  - Sniffing
  - Accès aux fichiers/base de pwd (serveur auth)
  - Brute force
  - Attaque par dictionnaire
  - Social Engineering
  - Rainbow tables (hash format)

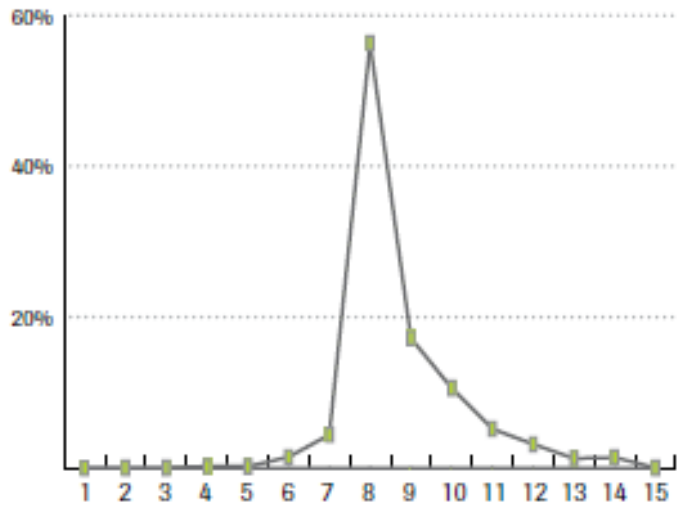
Les mots de passe



Months	27,191 passwords used English spelling of months (January – December)
U.S. States	72,389 passwords used U.S. States (Illinois, California)
Seasons	74,368 passwords used seasons (spring, fall)
Baby Names	170,013 passwords used names in the "top 100 male and female baby names of 2011" list.

TrustWave 2012 Global Security Report

Les 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

TrustWave 2012 Global Security Report

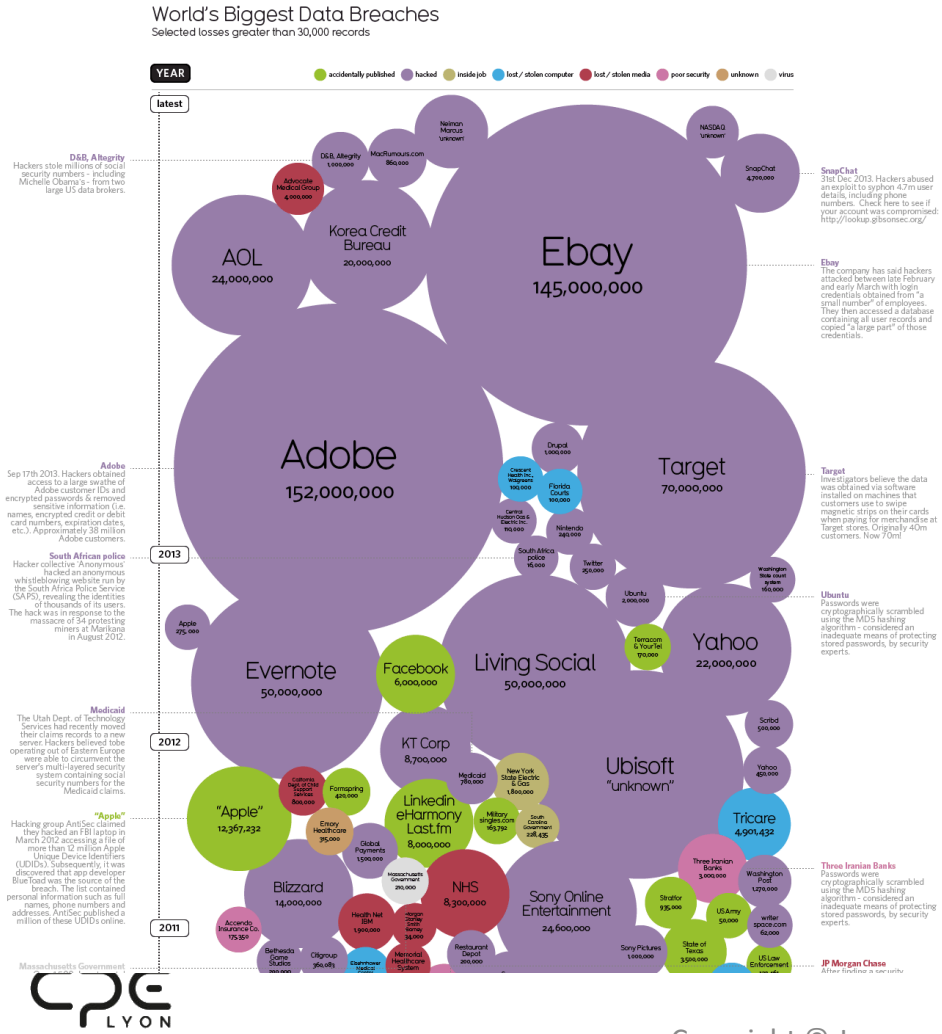
Les mots de passe

TOP PASSWORDS USED IN IOT ATTACKS (YEAR)

PASSWORDS	PERCENT
123456	24.6
[BLANK]	17.0
system	4.3
sh	4.0
shell	1.9
admin	1.3
1234	1.0
password	1.0
enable	1.0
12345	0.9

Symantec 2019 Internet Security Thread Report

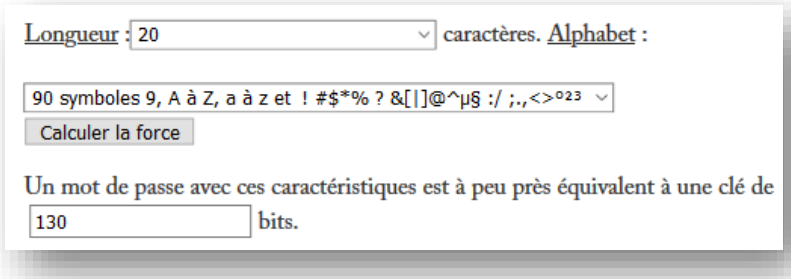
Les mots de passe



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-static/

Les mots de passe

- Sécurisé les mots de passe
  - Complexité
    - Taille
    - Caractère
    - Mémorisable
    - Difficile à deviner



https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

  - Stockage: chiffrement ou Hash (MD4, MD5, bcrypt)
  - Nombre de tentatives
  - Durée de vie

Les mots de passe

R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

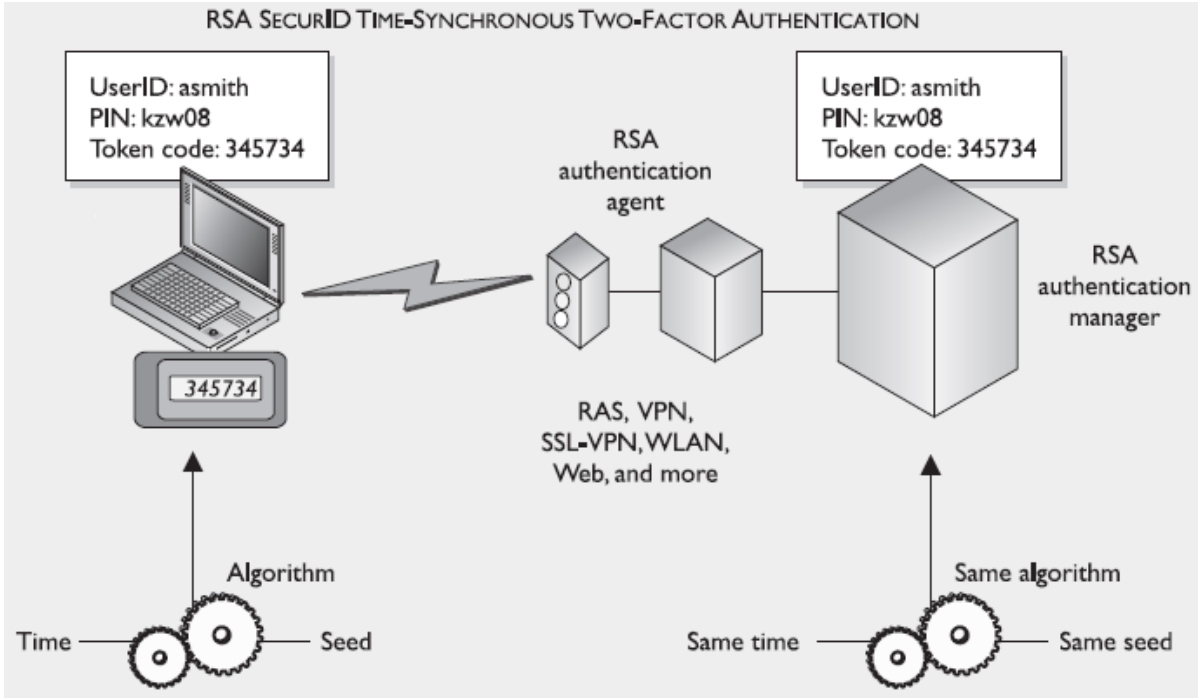
CPE LYON

Autres types de mots de passe

- Mots de passe cognitif (série de questions)
- Mots de passe à usage unique
  - Token synchrones (incluant les TOTP)
  - Token asynchrones (challenge/response, HOPT)

Autres types de mots de passe

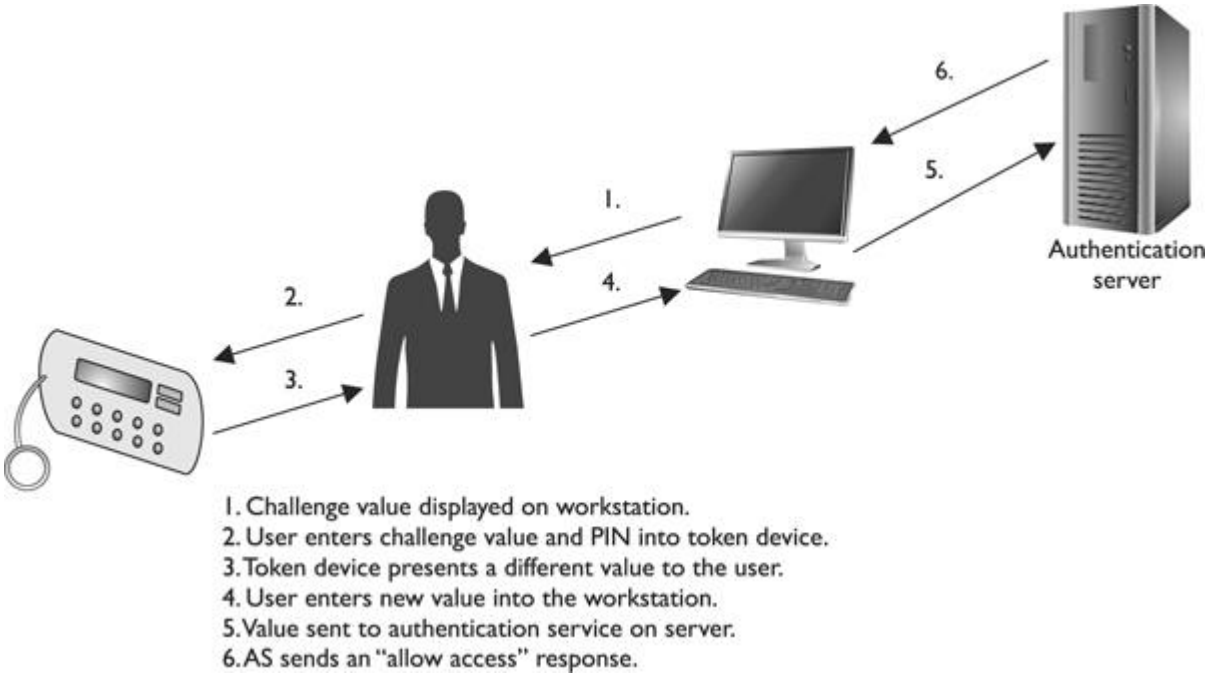
- Token Synchrone



RSA Security

Autres types de mots de passe

- Token asynchrone



https://compsecurityconcepts.files.wordpress.com/2013/11/asynchronous-token-device.jpg

Autres types de mots de passe

- HMAC (keyed-Hash Message Authentication Code)

Shared Secret

Message

HASH function ( )

HASH(secret XOR 0x5C…. || HASH(Secret XOR 0x36… || message))

|| Opérateur concaténation

XOR Opérateur ou exclusif

0x36…. Valeur 0x36 répéter B fois dépendant de la taille choisie (e.g B=2 0X3636)

0x5C…. Valeur 0x5C répéter B fois dépendant de la taille choisie (e.g B=2 0X5C5C)

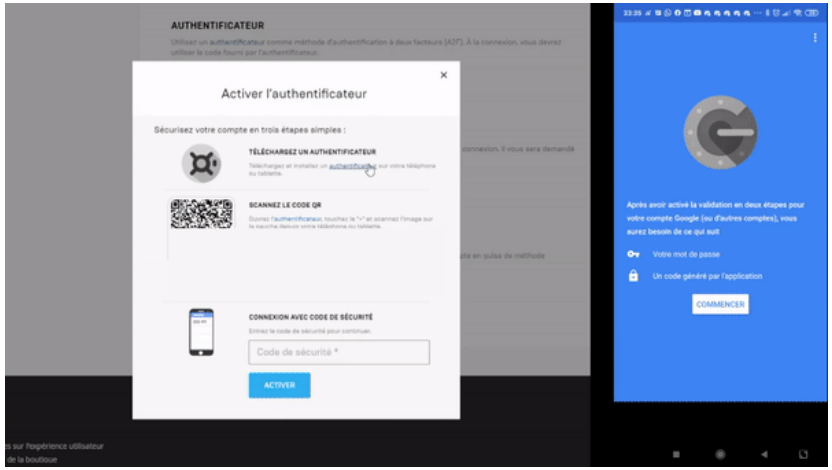
https://datatracker.ietf.org/doc/html/rfc2104

https://www.youtube.com/watch?v=BjInMA-b8ZE

Autres types de mots de passe

- Hmac-based One Time Password[1]

e.g Google Authenticator



https://www.youtube.com/watch?v=BvM6r2hW1Ks

[1] RFC 4226 : https://datatracker.ietf.org/doc/html/rfc4226#page-7

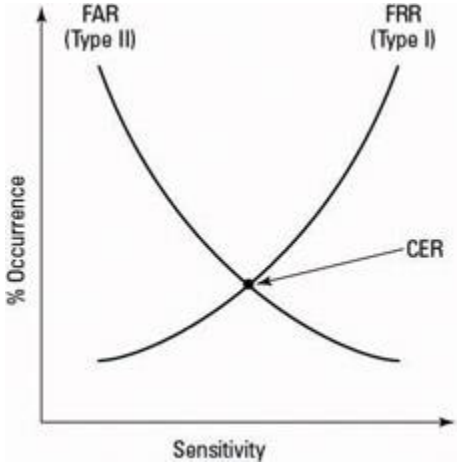
La biométrie

- Définition

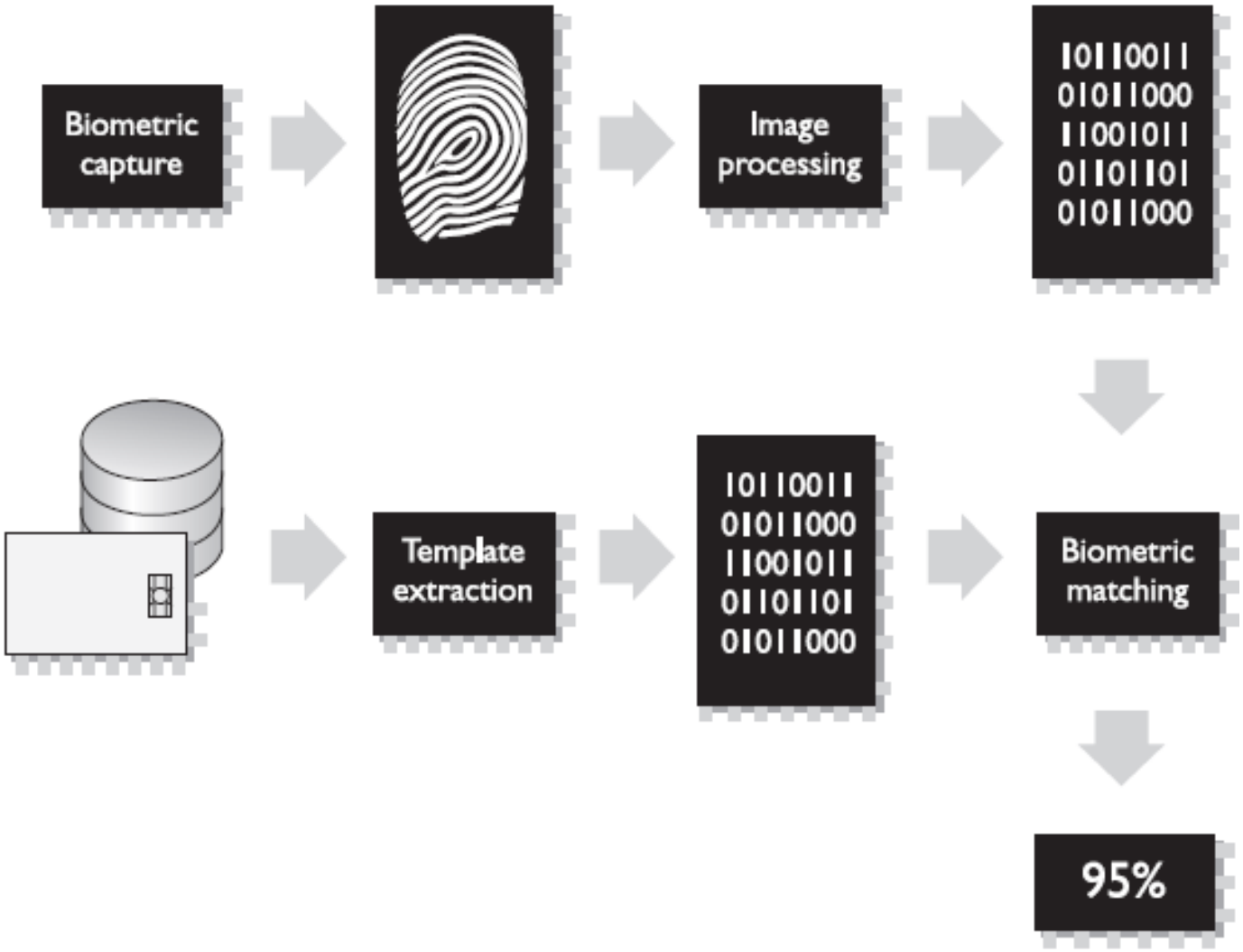
  Vérifier l'identité *d'un individu en* ***analysant*** *un* ***attribut*** *ou un* ***comportement unique****.*

- Notion de Crossover error rate (CER)

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

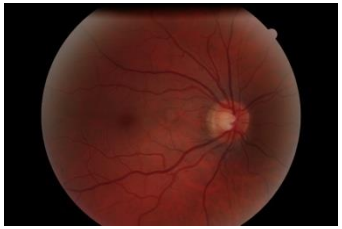


La biométrie



La biométrie

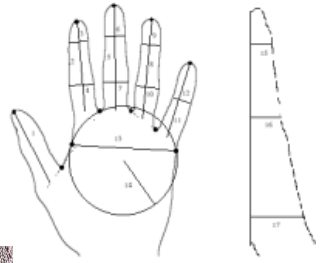
Rétine



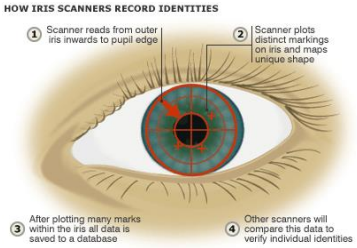
Signature (mouvement)

Clavier (mouvement)

Géométrie des mains

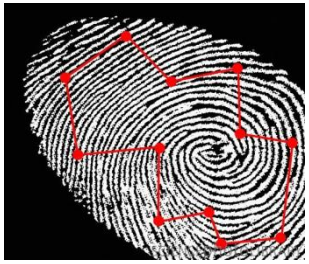


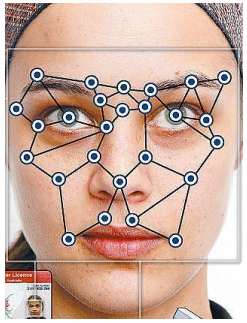
Iris



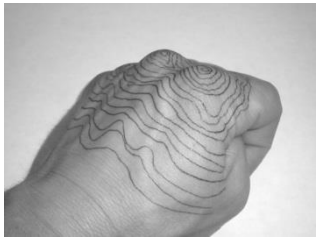
Empreinte

Empreinte vocale

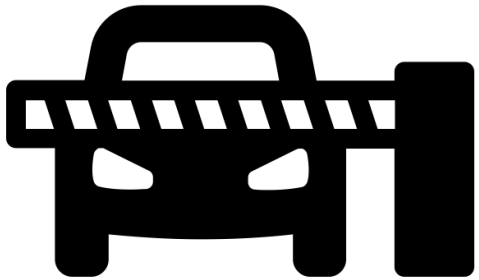




Visage



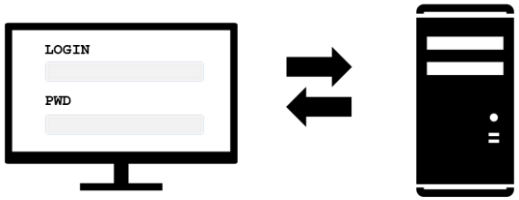
Topographie de la main

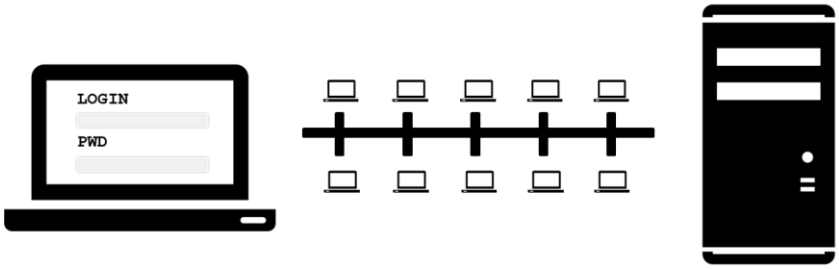


Gestion des Contrôles d'Accès

Contrôle d'accès

Contrôle d'accès





Identification,

Authentication,

Authorization,

Accounting

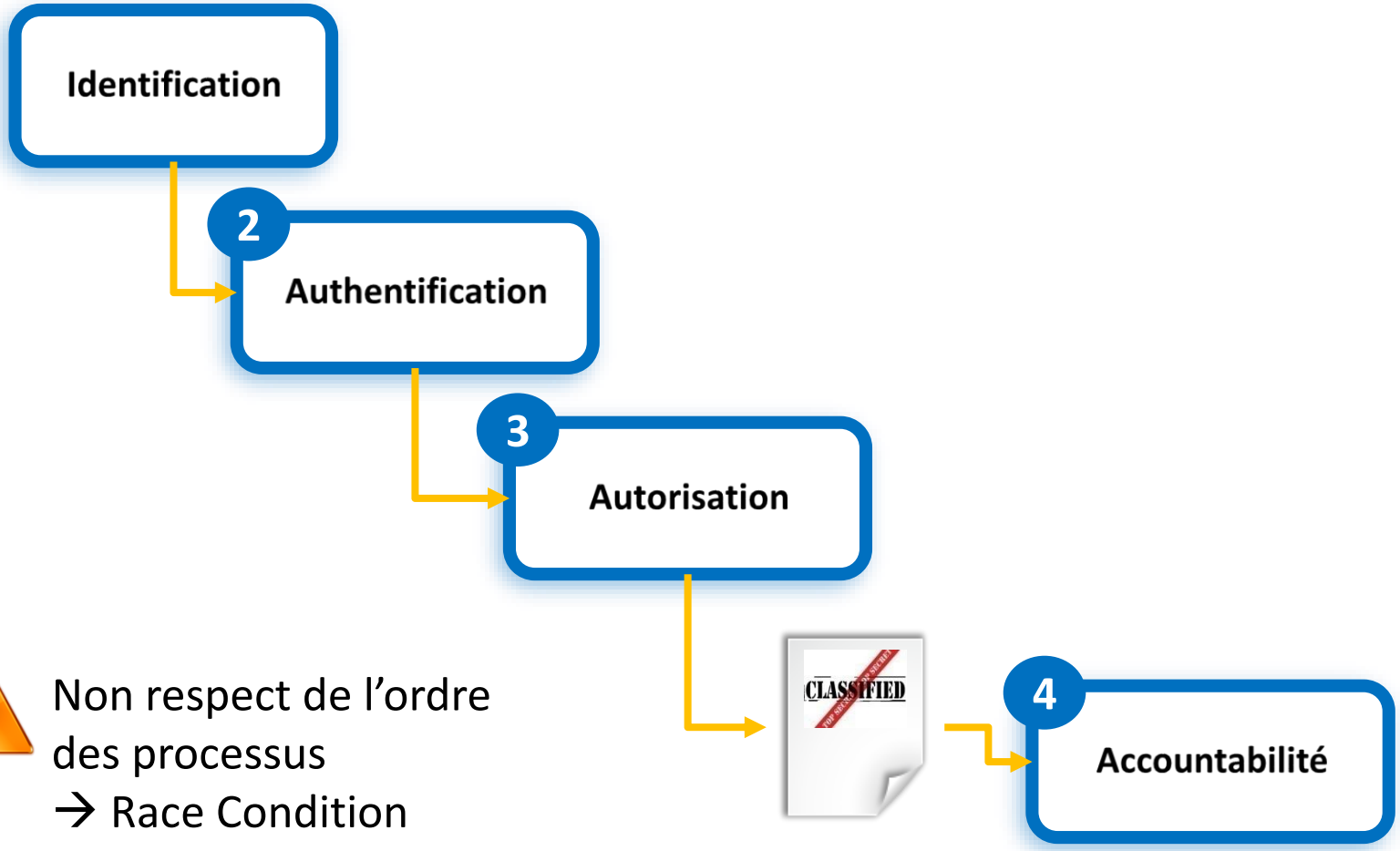
Contrôle d'accès : Identification, Authentication, Authorization, Accounting (AAA)

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

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

- Concepts standardisés par l'IETF, e.g.:
  - Generic AAA architecture (RFC2903)
  - AAA Authorization Application Examples (RFC2905)
  - AAA Authorization Framework (RFC2904)

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



Non respect de l'ordre des processus
→ Race Condition

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

Vuln ID	Summary	CVSS Severity
CVE-2019-1992	In bta_hl_sdp_query_results of bta_hl_main.cc, there is a possible use-after-free due to a race condition. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-116222069. **Published:** February 28, 2019; 12:29:00 PM -05:00	*V3:* 7.5 HIGH *V2:* 7.6 HIGH

CVE-2019-1992 Detail

Current Description

In bta_hl_sdp_query_results of bta_hl_main.cc, there is a possible use-after-free due to a race condition. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-116222069.

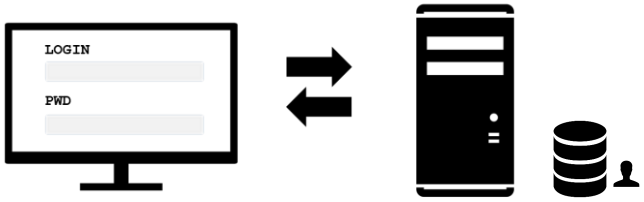
Source: MITRE

Description Last Modified: 02/28/2019

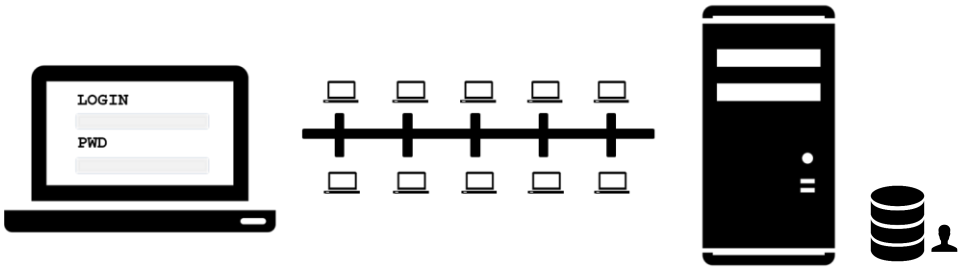
− Hide Analysis Description

Analysis Description

Contrôle d'accès



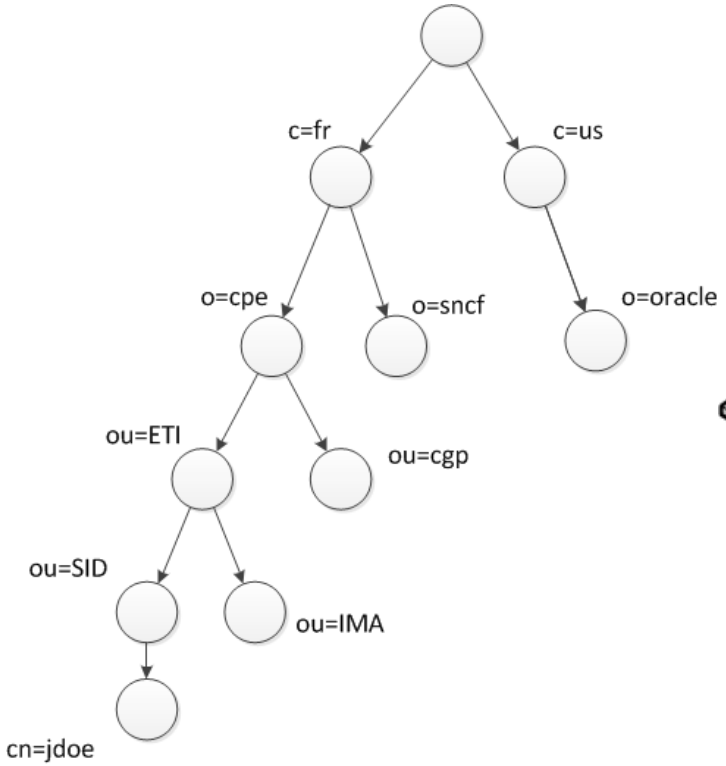
Stockage des Identités



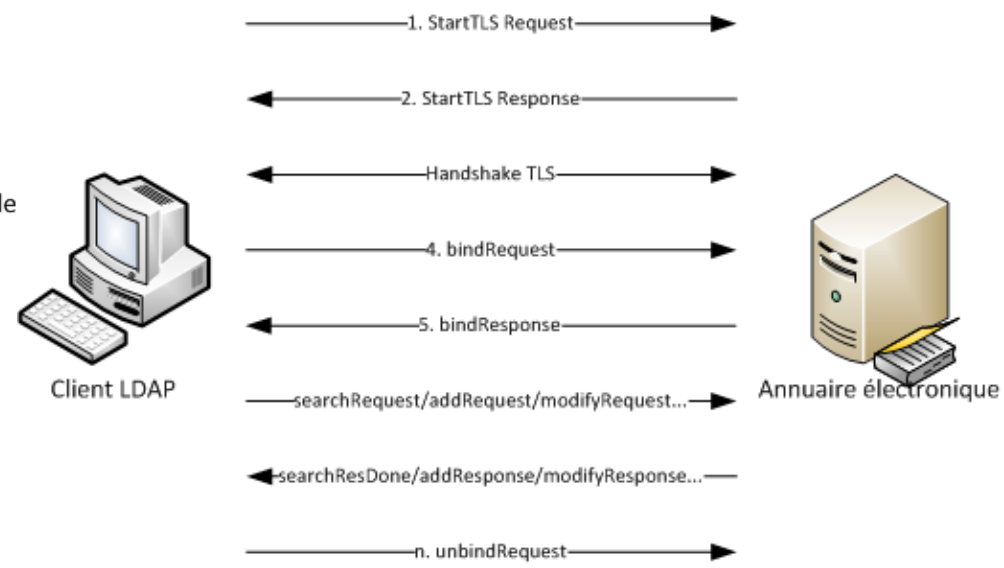
Management des identités

- Annuaire : 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)
  - L'administration de l'annuaire

Management des identités



Format de données X500

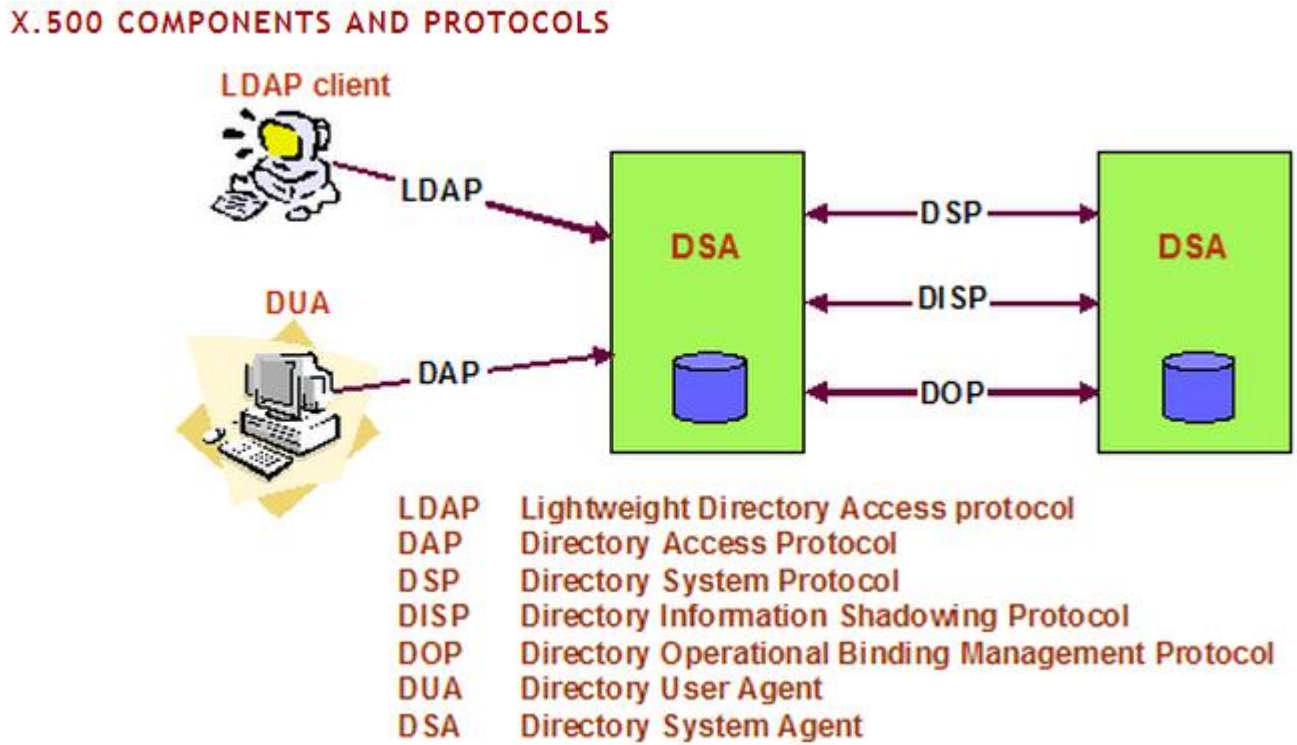


Protocole LDAP

Management des identités

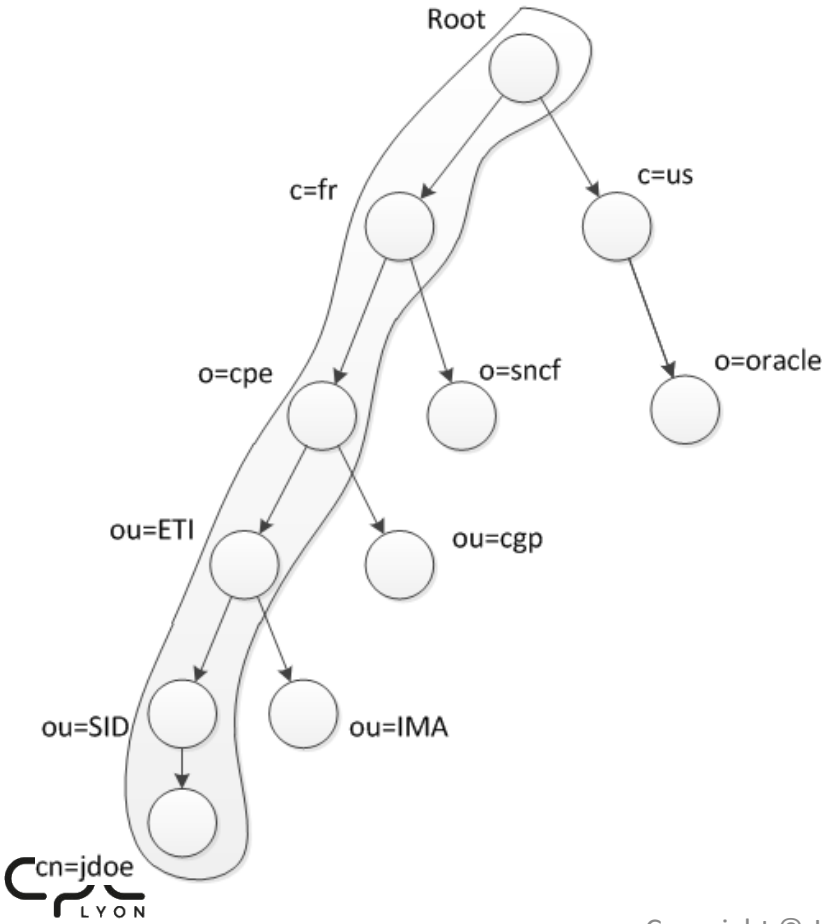
- X500
  - Service d'annuaire global
    - Structure de modèle
    - Protocoles de communication
    - Procédures de distribution
  - X500 UIT-T, ISO/CEI 9594-1 (1990)
  - X500 directory: stocker des informations d'organisation (personnes, liste, groupe…)

Management des identités



Management des identités

- X500 espace de nommage



Dn: {c=fr, o=cpe, ou=ETI, ou=SID, cn=jdoe}

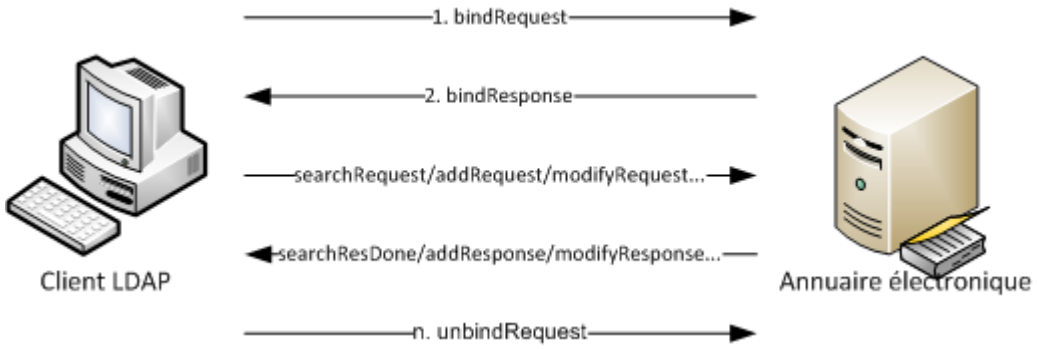
Management des identités

- LDAP (Lightweight Directory Access Protocol)
  - Protocole applicatif (sur TCP/IP)
  - Mode connecté
  - Port 389, 636 (ldap et ldap over TSL/SSL)
  - Modèle de communication resquest-response

Management des identités

- LDAP (Lightweight Directory Access Protocol)

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 *Distinguished Name* de l'annuaire (cf. section modèles de données)



http://www-igm.univ-mlv.fr/~dr/XPOSE2007/vboistua_ldap/ldap_concept_protocol.html

Management des identités

- LDAP (Lightweight Directory Access Protocol)
  - **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'habitant 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~=febvre))
    (&(objectclass=person)(cn=*f*vre))

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

CPE LYON

Management des identités

- LDAP (Lightweight Directory Access Protocol)
  - **Exemple d'URL LDAP:**

    ldap://ldap.mit.edu/ou=employees,dc=mit,dc=edu

  - **Exemple de requêtes**

    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?(objetclass=person)

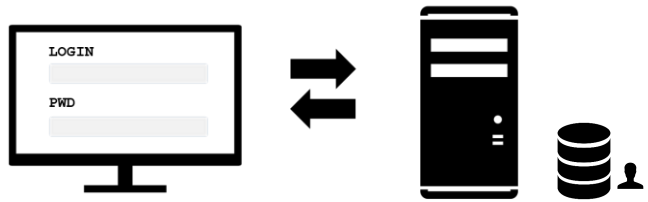
    Exemple 3.6. Lecture des objets personnes d'un annuaire
    ldap://localhost:389/??sub?objectclass=person

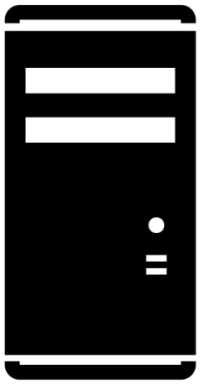
    Exemple 3.7. Recherche de Valery Febvre
    ldap://ldap.easter-eggs.fr/cn=Valery%20Febvre,ou=Moyens%20Informatiques,dc=easter-eggs,dc=fr

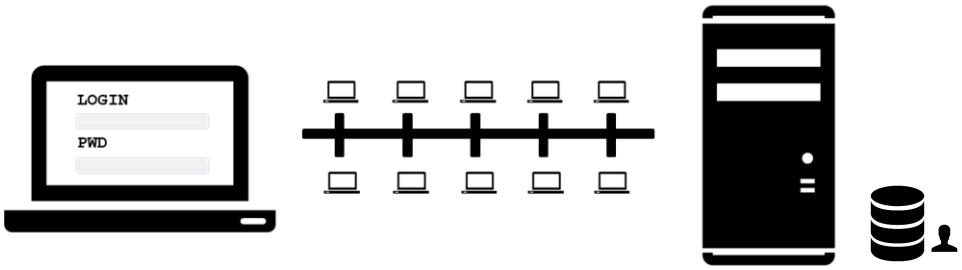
    Exemple 3.8. Recherche approximative d'une personne
    ldap://ldap.easter-eggs.fr/o=easter-eggs,dc=fr?mail,uid,sub?(sn=Febvre)

CPE LYON

Technologies des contrôles d'accès



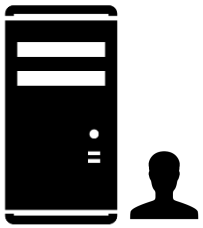




authentification

Serveur d'authentification
Contrôleur de domaine

Serveur d'authentification



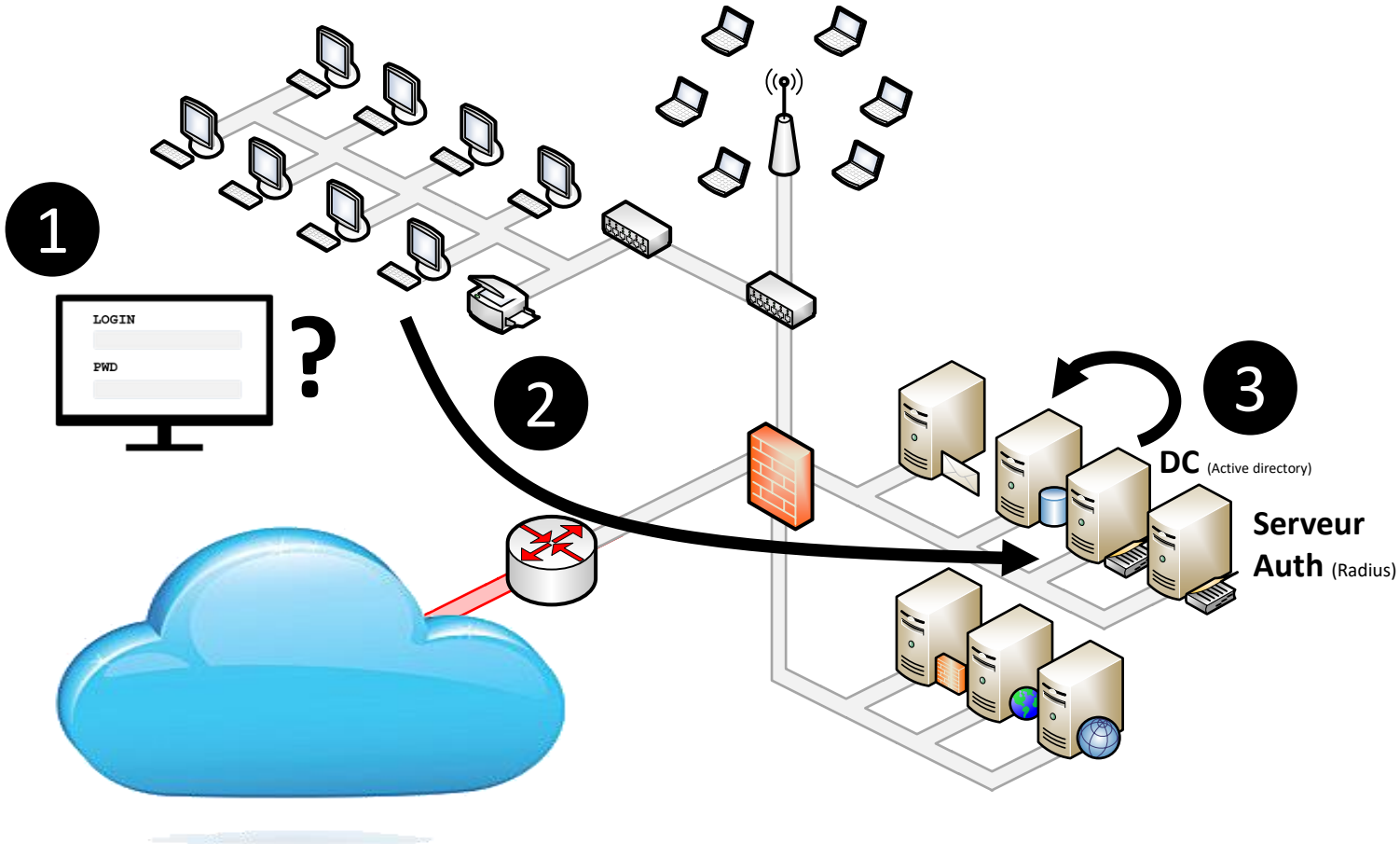
- Serveur d'authentification et contrôleur de domaine
  - **Contrôleur de domaine (e.g ActiveDirectory, Samba)**

    Permet d'authentifier et de délivrer des autorisations aux entités d'un domaine (même zone e.g segment LAN)

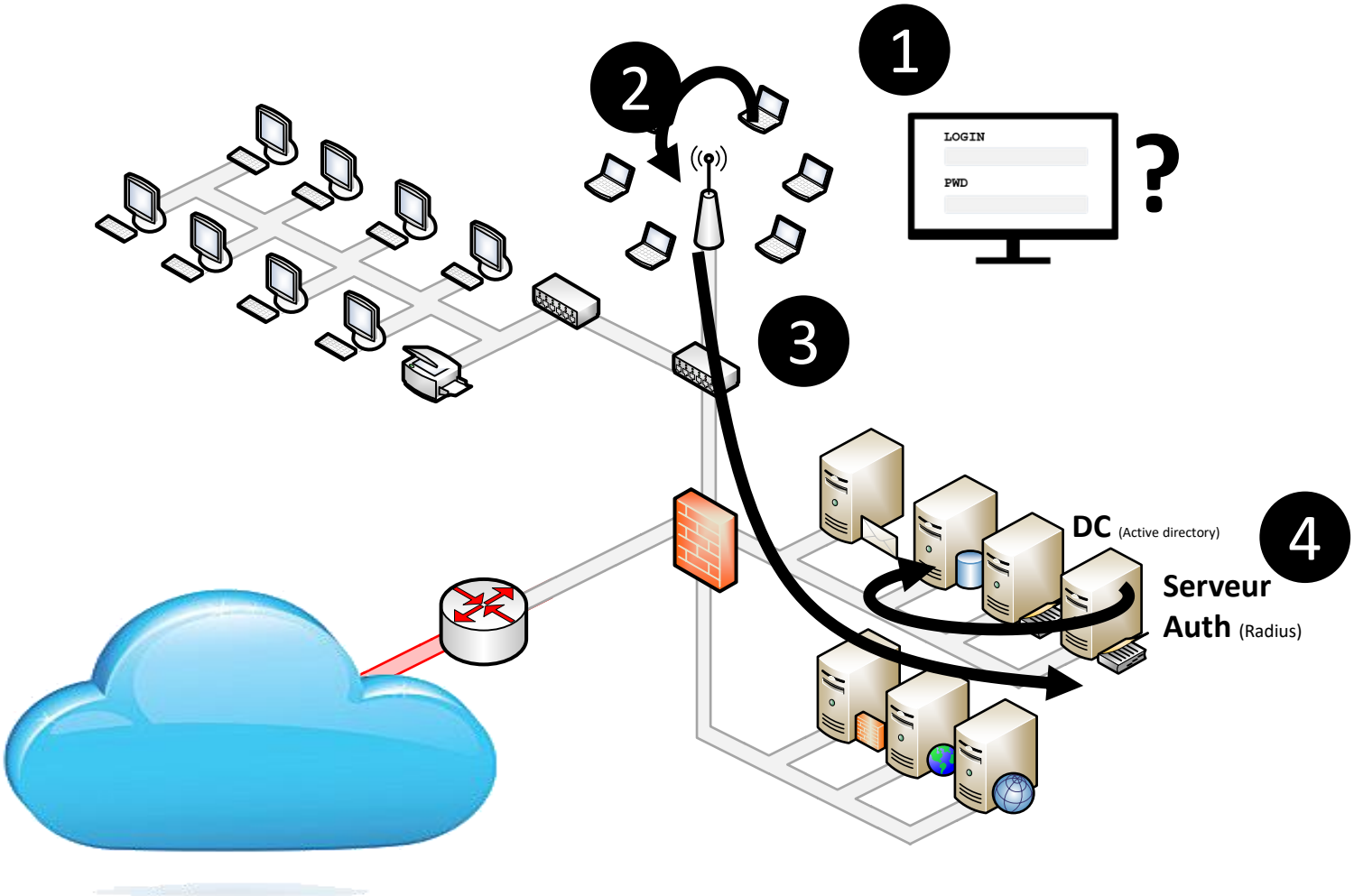
  - **Serveur d'authentification (e.g Radius, Tacacs)**

    Permet d'identifier des devices, le rebond d'authentification afin de ne pas exposer directement le contrôleur de domaine (e.g 802.1x)

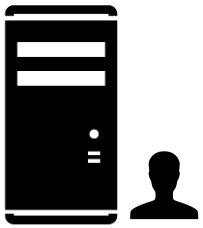
Serveur d'authentification



Serveur d'authentification



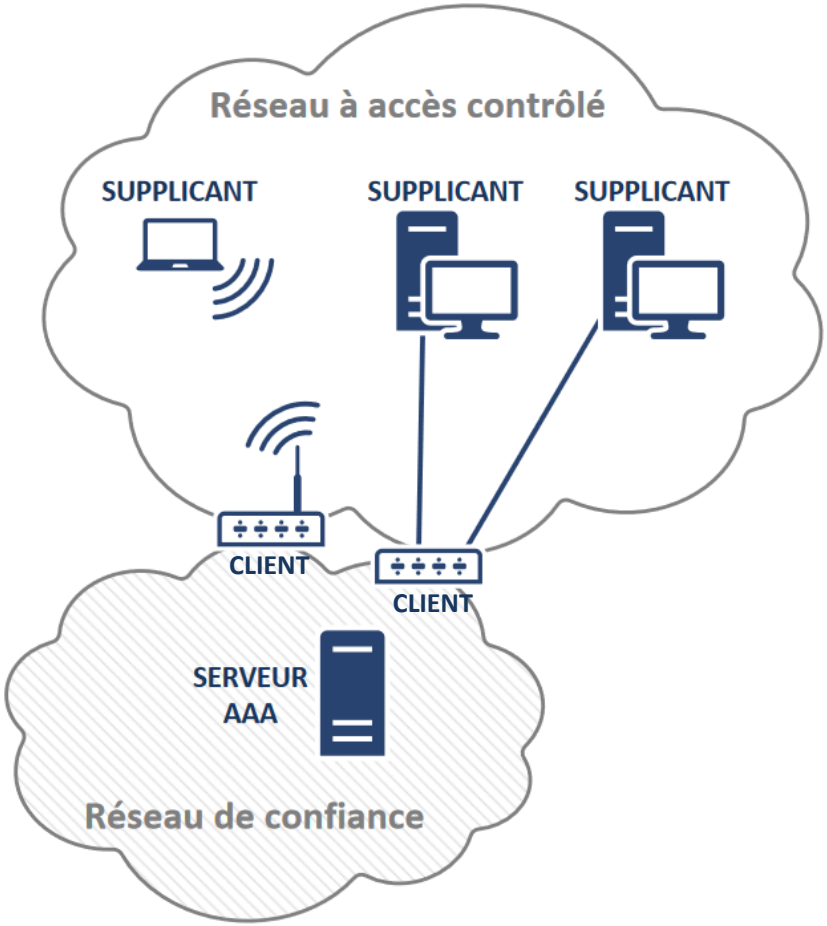
802.1X: réseau à accès contrôlé



*Protocole permettant de **controller l'accès** aux réseaux de différents **devices***

- Objectifs:
  - Contrôle des connections filaires à un réseau local
  - Contrôle des connexions sans fil
- Entités:
  - Serveur AAA
  - Client
  - Supplicant
  - Réseau à accès contrôlé
  - Réseau de confiance

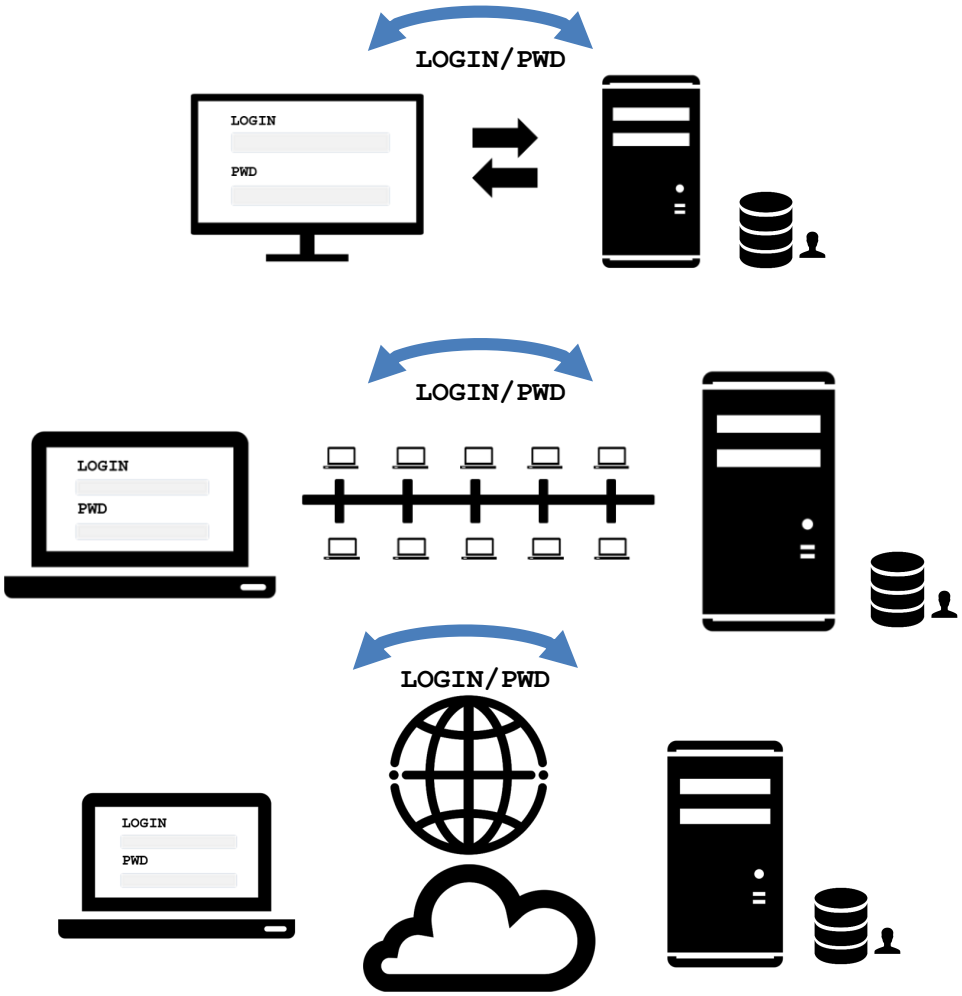
802.1X: réseau à accès contrôlé



1. Client envoie une demande d'identification
2. Supplicant retourne au client son identité
3. Le client transmet l'identité du supplicant au serveur
4. Le serveur envoie au client la méthode d'authentification
5. Le client transmet la demande au supplicant
6. Le client procède à l'authentification
7. Le serveur et le supplicant échangent des messages d'auth. par l'intermédiaire du client en fonction du mode d'auth
8. Le serveur fournit une réponse:
   - **Access-Accept** : le client bascule le port de connexion dans l'état authorisé
   - **Access-reject**: le port reste dans l'état non autorisé

https://www.ssi.gouv.fr/uploads/2018/08/guide_802.1x_anssi_pa_043_v1.pdf

Protocoles d'authentification



Protocoles d'authentification

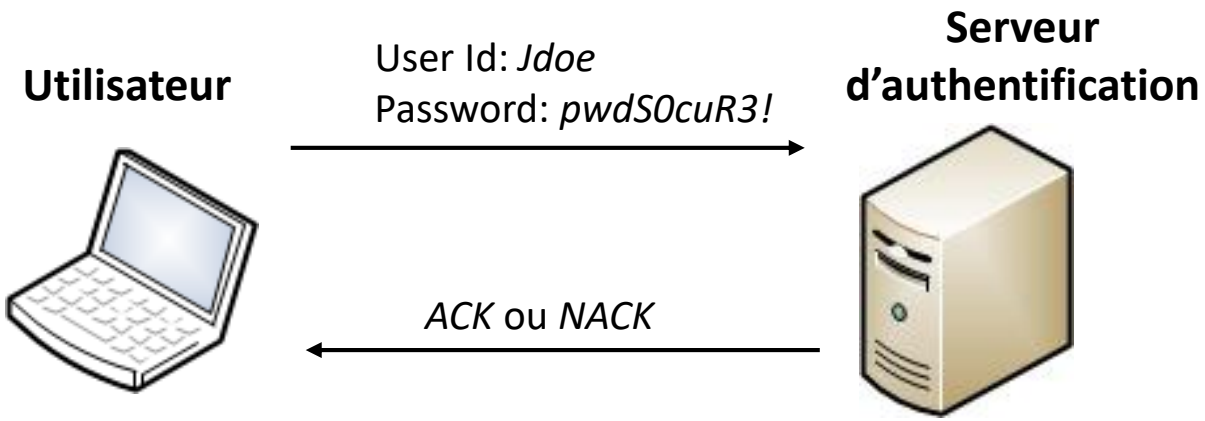
Protocoles d'authentification

- Standard
  - **PAP**
  - **CHAP**
  - **EAP**
  - **(Kerberos)**
- Propriétaire
  - **LMHash** (microsoft)
  - **NTLM** (microsoft)

Protocoles 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

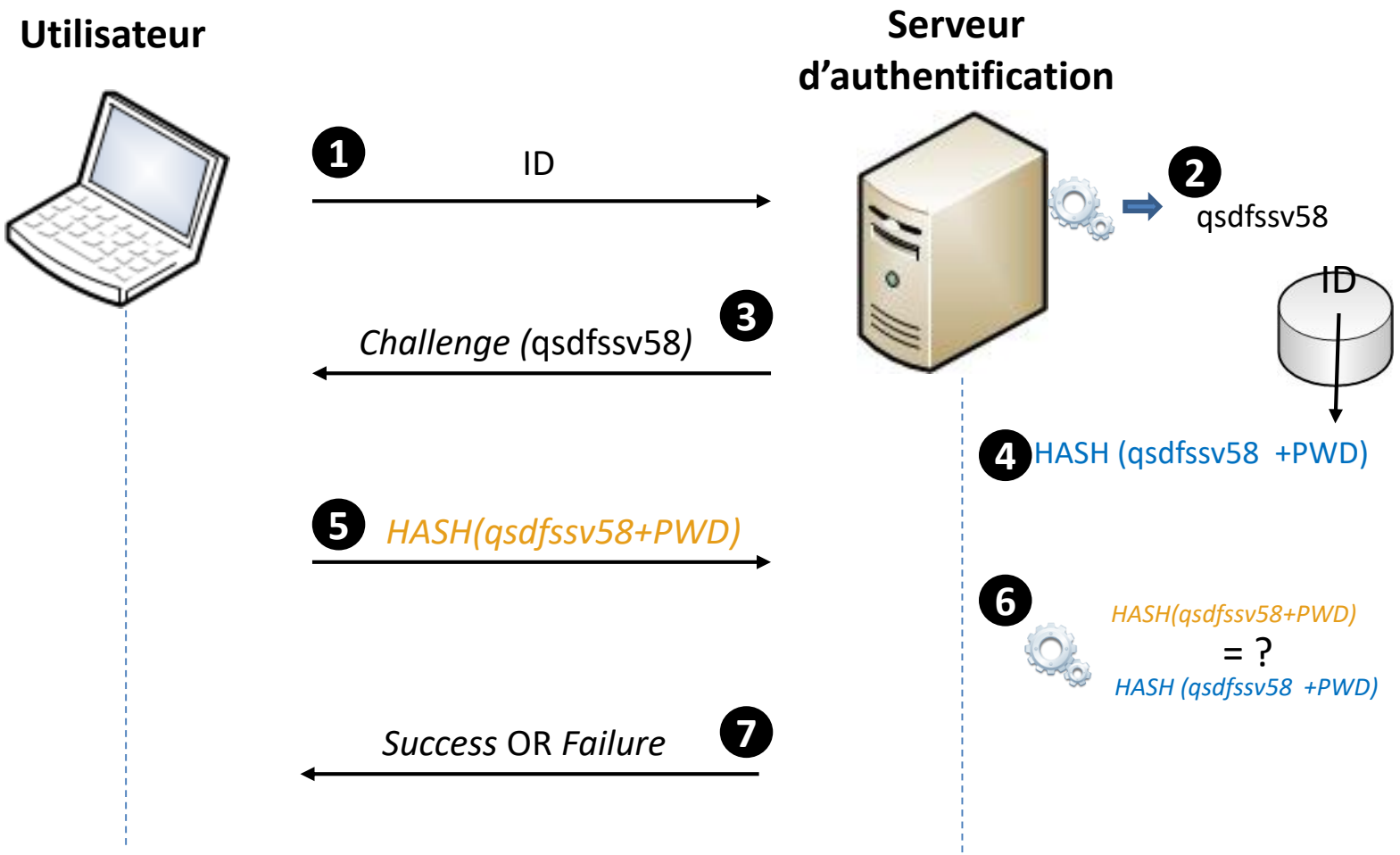


Protocoles d'authentification

- **C**hallenge-**H**andshake **A**uthentication **P**rotocol (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

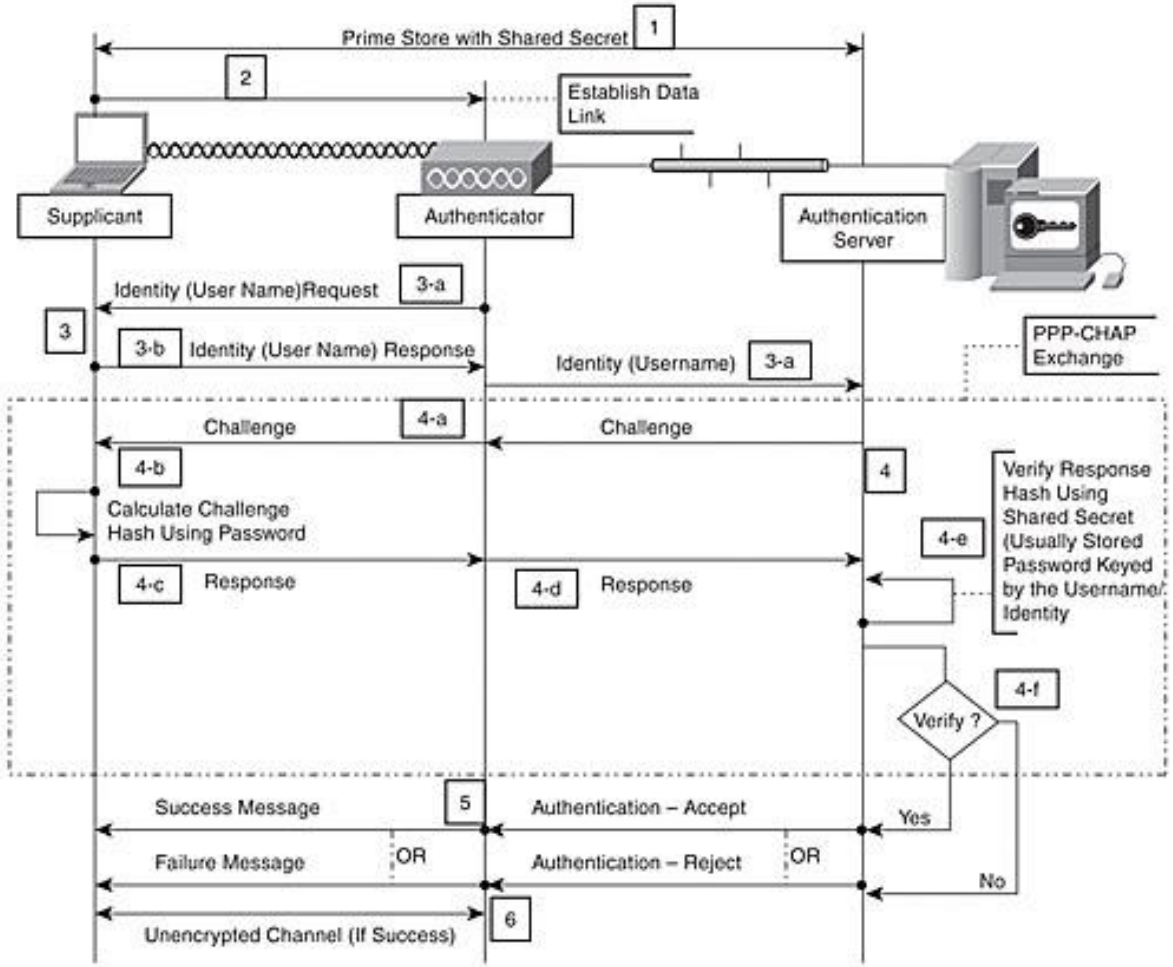
CHAP: Challenge Authentication Protocol



Protocoles d'authentification

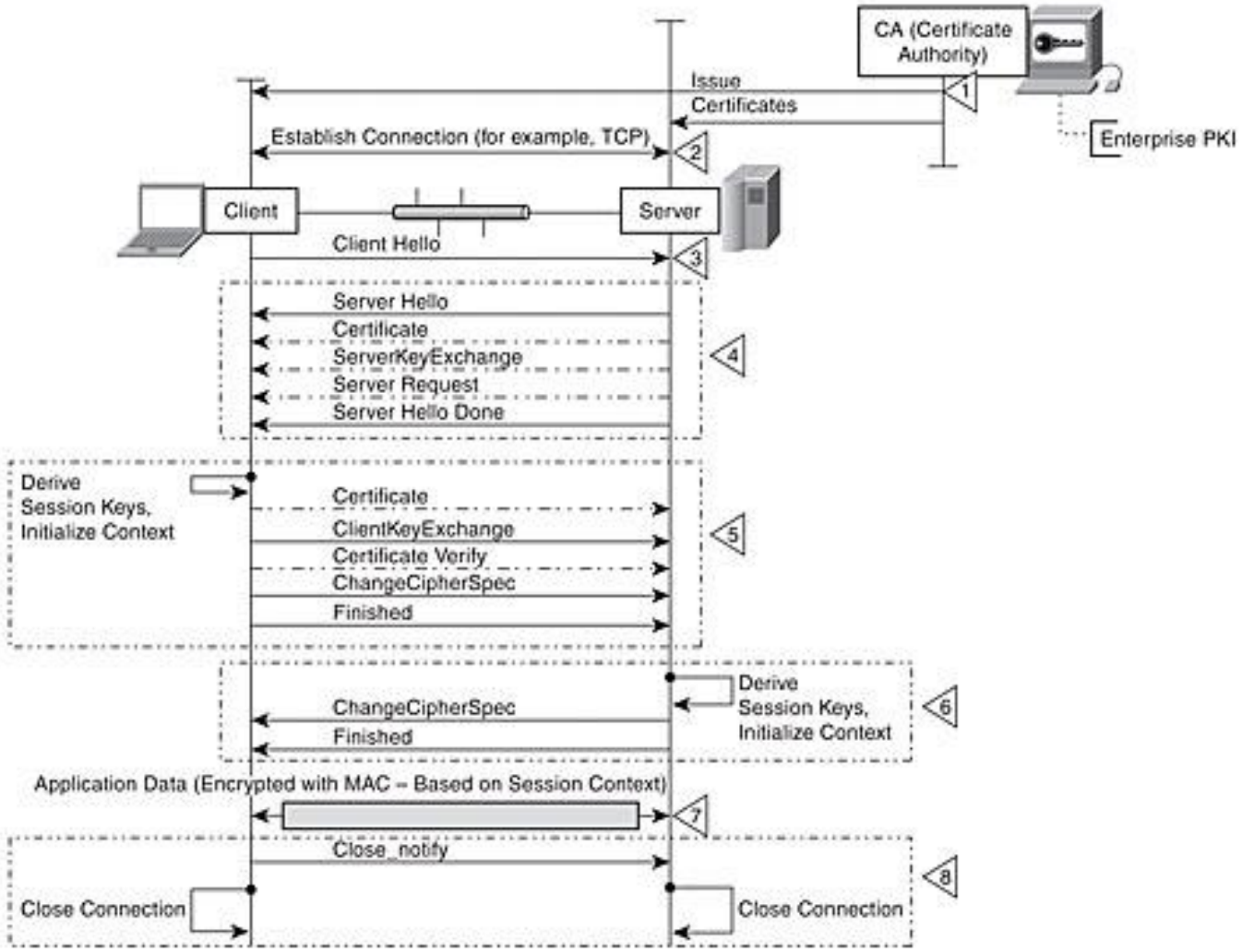
- Extensible Authentication Protocol (EAP)
  - Universel, utilisé surtout dans les réseaux sans fils et les liaisons Point à Point
  - Extensible, les méthodes d'authentification peuvent être customisées
  - Des méthodes d'authentification par défaut (MD5, Generic Token Card…)
  - L'authentification 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)

EAP-MD5: Extensible Authentication Protocol - Message Digest 5



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

EAP-TLS: Extensible Authentication Protocol – Transport Level Security



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

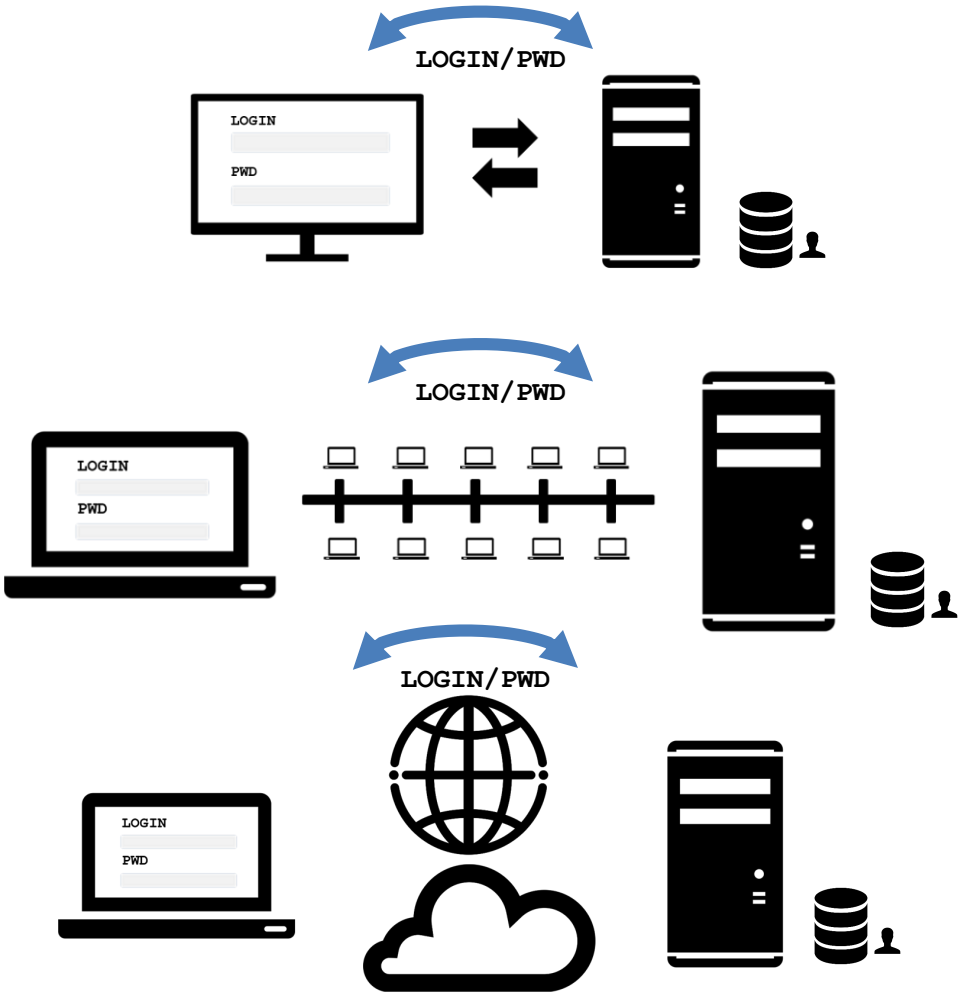
802.1X: Recommandations

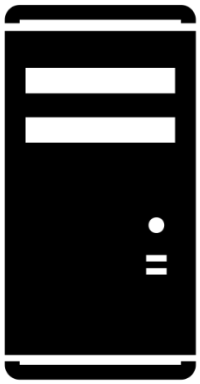
R1	Choix d'un protocole AAA dans un réseau à accès contrôlé
R2	Authentification des *supplicants*
R3	Autorisation des *supplicants*
R4	Secrets d'authentification
R5	Utilisation de protocoles d'authentification sécurisés
R6	Suppression du support des méthodes non encapsulées
R7	Mise en place d'un réseau sans fil 802.1X
R8	Négociation des clés cryptographiques à l'aide de TLS
R9	Liaison entre l'authentification externe et l'authentification interne
R10	Protection du serveur
R11	Durcissement du système
R12	Redondance des serveurs
R13	Cloisonnement des flux de fonctionnement
R14	Gestion des secrets partagés
R15	Protection physique du réseau de confiance
R15+	Authentification des *clients*
R15++	Protection des échanges sur le réseau de confiance
R16	Journalisation des évènements
R17	Affectation statique de VLAN
R17-	Affectation dynamique de VLAN utilisateurs
R18	Lutte contre les branchements de commutateurs
R19	Cloisonnement et supervision des réseaux utilisateurs
R20	Restreindre les services accessibles en authentification autom
R21	Maîtrise des équipements
R22	Sécurisation d'un réseau local sans fil
R23	Déploiement dans des conditions maîtrisés
R24	Gestion des prises en accès libre
R25	Connexion possible d'individus malveillants
R26	Lutte contre le piégeage des accès réseau
R27	Réduction des risques liés au piégeage des accès réseau

RECOMMANDATIONS DE DÉPLOIEMENTDU PROTOCOLE 802.1X POUR LECONTRÔLE D'ACCÈS À DES RÉSEAUXLOCAUX

https://www.ssi.gouv.fr/uploads/2018/08/guide_802.1x_anssi_pa_043_v1.pdf

Technologies des contrôles d'accès





Serveur d'authentification

(e.g Radius, Tacacs)

Technologies des contrôles d'accès

- **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice

  RADIUS (RFC2865)

- **T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem

  TACACS (xtabacs RFC1492)

- **Diameter** (RFC3588)

RADIUS

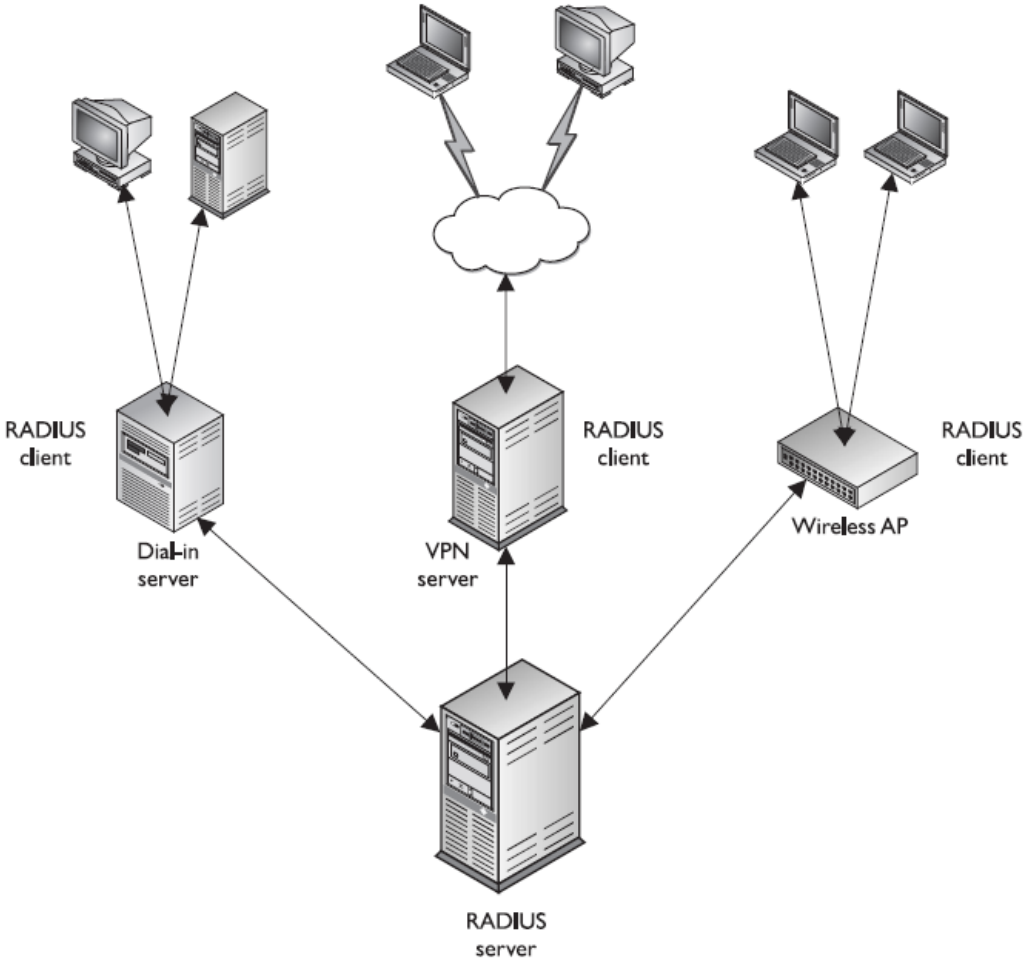
- Propriétés de base

  *Utilise le **protocole** AAA pour **transporter** les **informations d'authentification** d'un client (e.g Network Access Server) vers un **serveur** AAA*

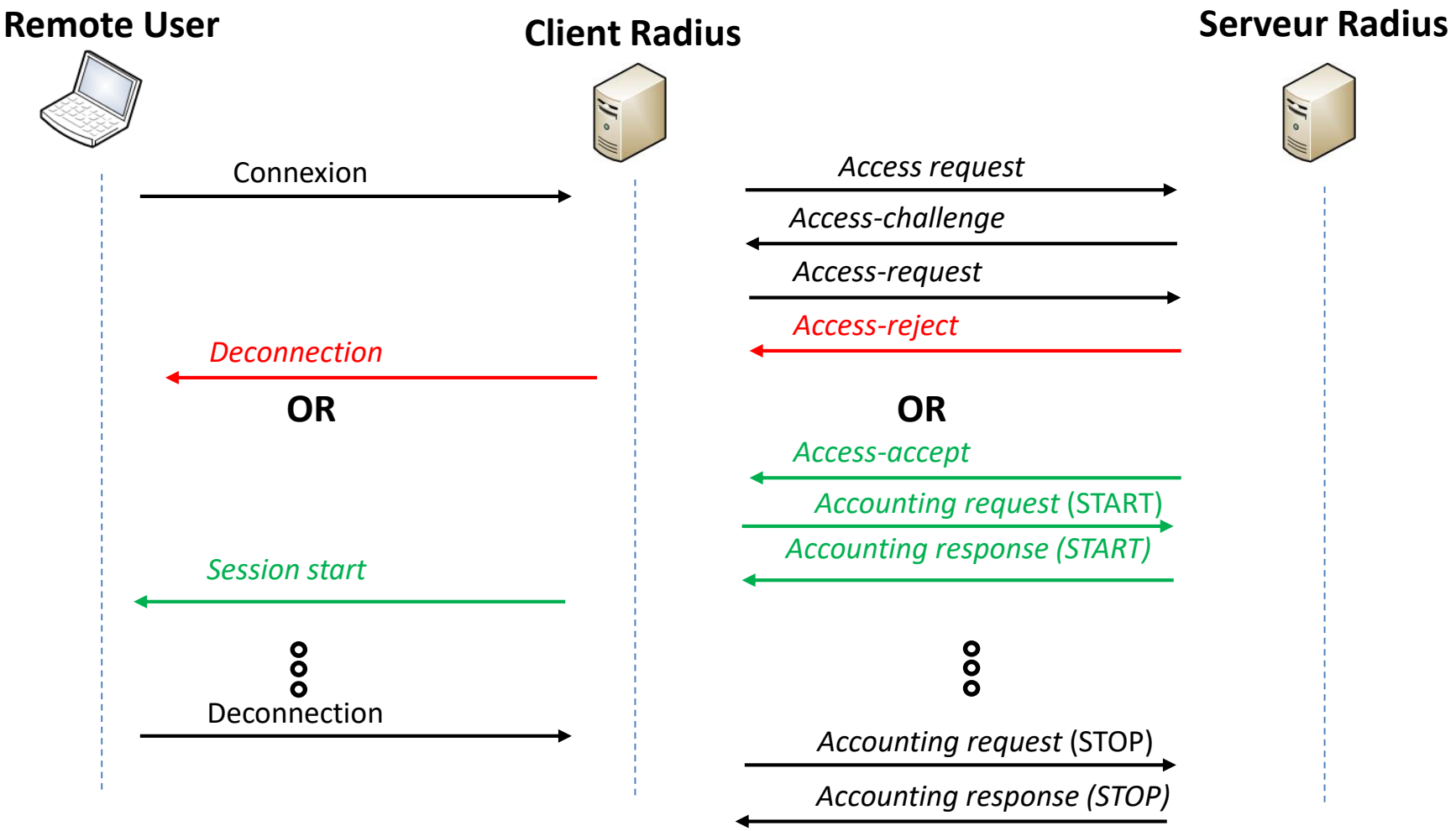
- Propriétés
  - Modèle client/serveur
    - Client: NAS (Network Access Server)→ génère des requêtes d'authentification AAA
    - Serveur: serveur Radius traite les requêtes AAA (joue également le rôle de proxy)
  - Sécurité réseau
    - Transactions authentifiées via un secret partagé entre le client 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

CPE LYON

RADIUS


RADIUS client
Dial-in server
VPN server
RADIUS client
Wireless AP
RADIUS client
RADIUS server

RADIUS


Remote User
Client Radius
Serveur Radius
Connexion
Access request
Access-challenge
Access-request
Access-reject
Deconnection
OR
OR
Access-accept
Accounting request (START)
Accounting response (START)
Session start
Deconnection
Accounting request (STOP)
Accounting response (STOP)

RADIUS

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

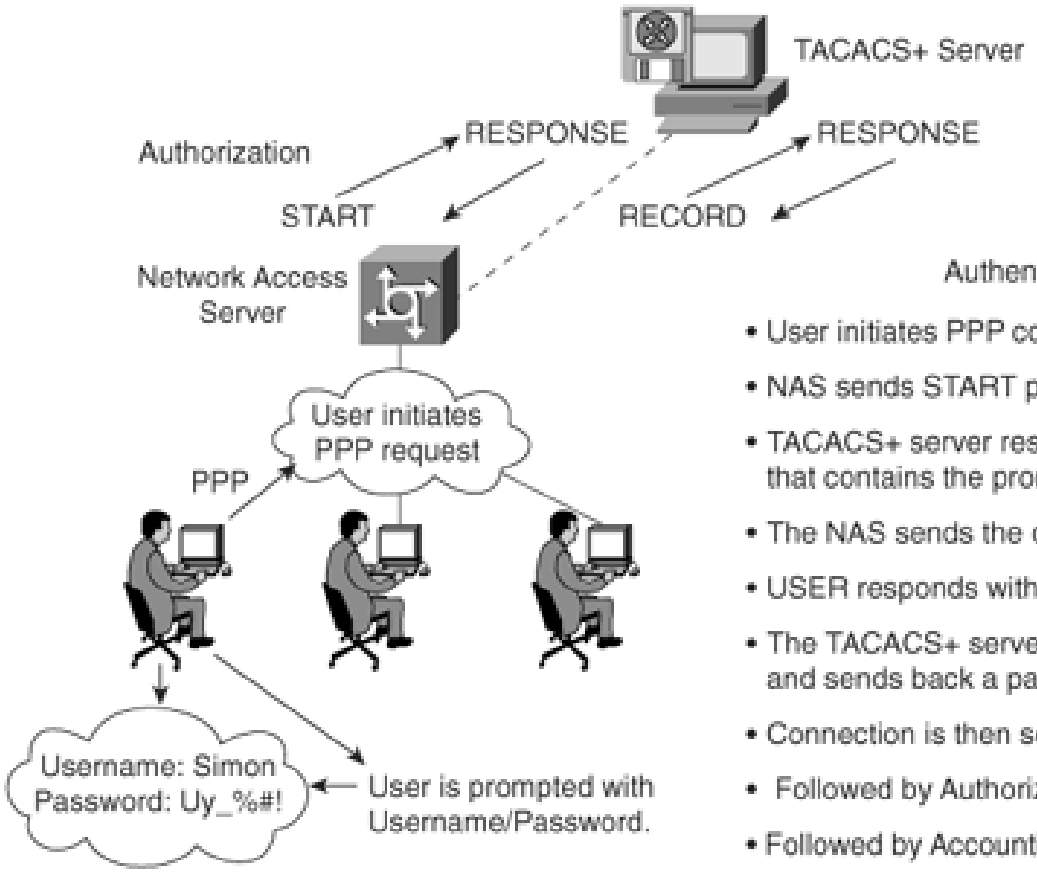
- **Limites**
  - Les couches applicatives doivent gérer la prise en compte de perte de paquets
  - UDP non adapté aux congestions réseaux (TCP oui)

TACACS

- 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)

TACACS



Authentication Process

- User initiates PPP connection to the NAS.
- NAS sends START packet to the TACACS+ server.
- TACACS+ server responds with GETUSER packets that contains the prompt username/password.
- The NAS sends the displays to the remote USER.
- USER responds with username/password pair.
- The TACACS+ server checks username/password and sends back a pass or fail packet to the NAS.
- Connection is then set up or rejected.
- Followed by Authorization.
- Followed by Accounting.

http://www.cathayschool.com/Terminal-Access-Controller-Access-Control-System-Plus-a608.html

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.

Autorisation

Autorisation

❑ Objectifs

*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

Règles de base

par défaut AUCUN ACCES

Seulement ce que le sujet à besoin de connaitre

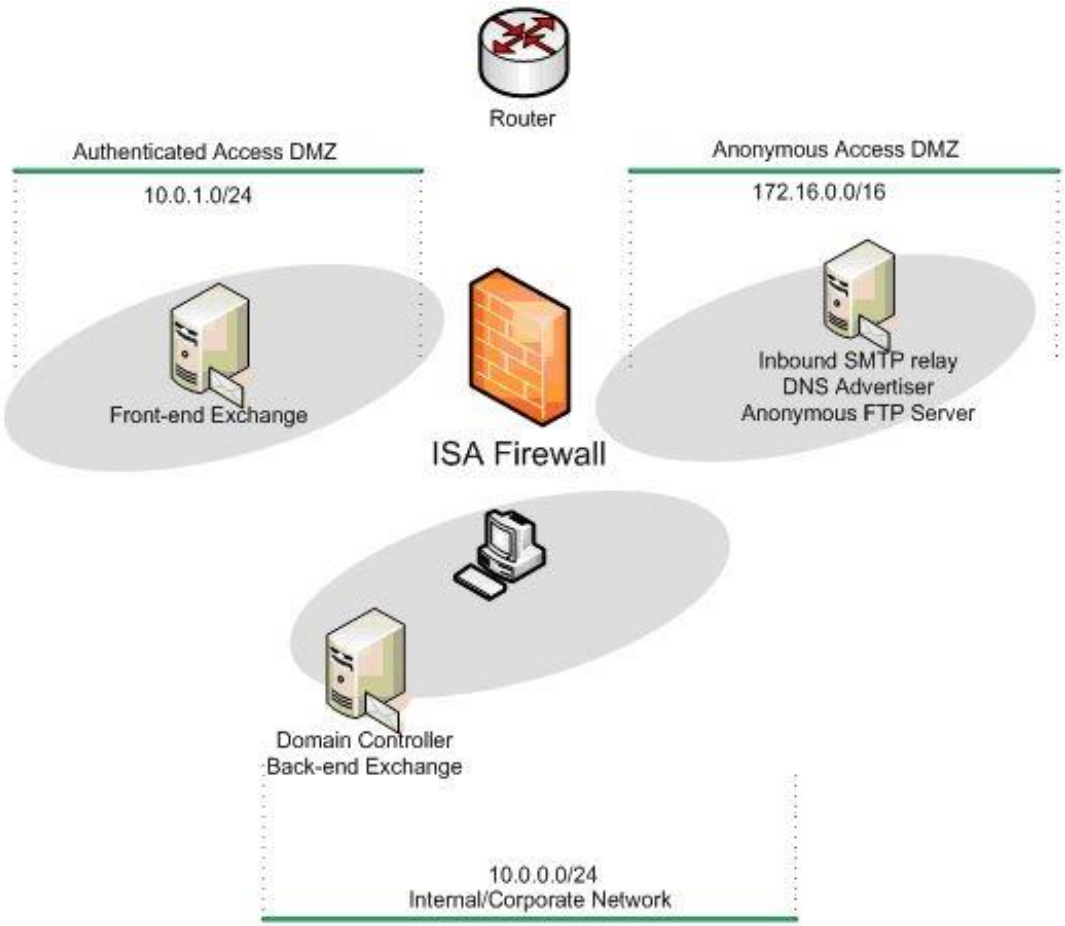
Domaine de sécurité

- **Objectifs**

  *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

Domaine de sécurité



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

Kerberos

Définition

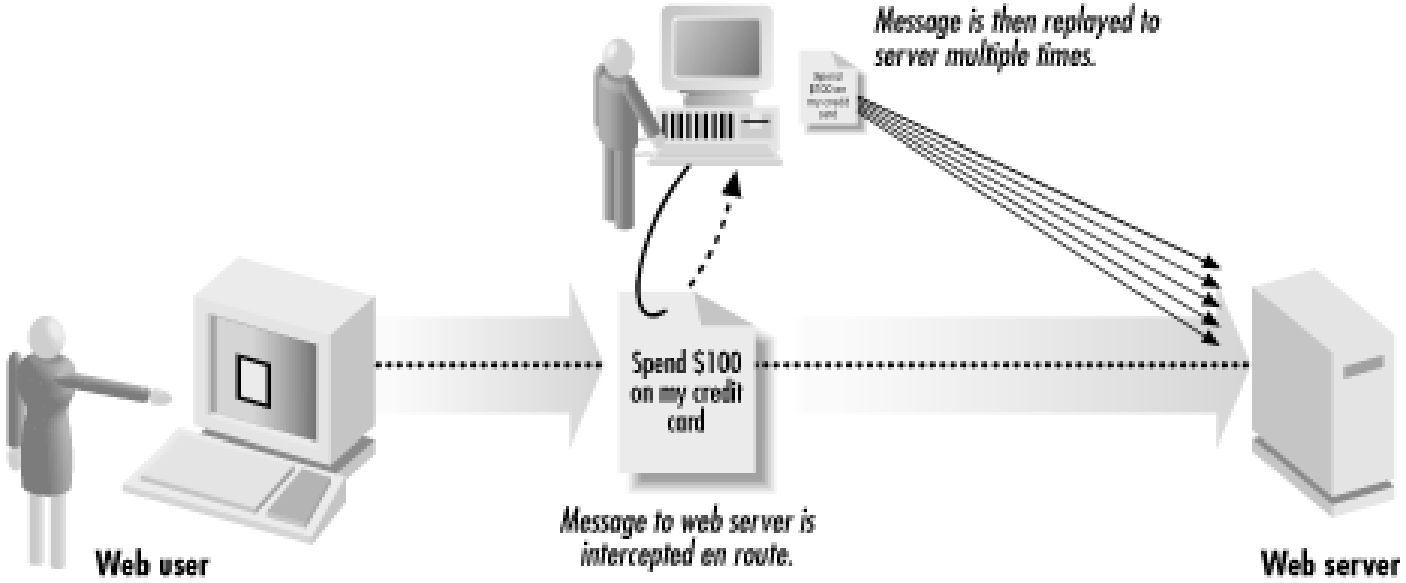
Protocole d'authentification délivrant des authorisations par le biais de « tickets ».

Propriétés

- Client serveur
- Authentifications et autorisations sécurisées sur réseaux non-sécurisés
- Authentification mutuelle sujet<->objet
- Protège contre les écoutes clandestines (eavedropping) et les replay attack
- Utilise le chiffrement symétrique (asymétrique en option)
- MIT v5 RFC 4121

Kerberos

Replay attack



http://flylib.com/books/en/2.513.1.29/1/

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

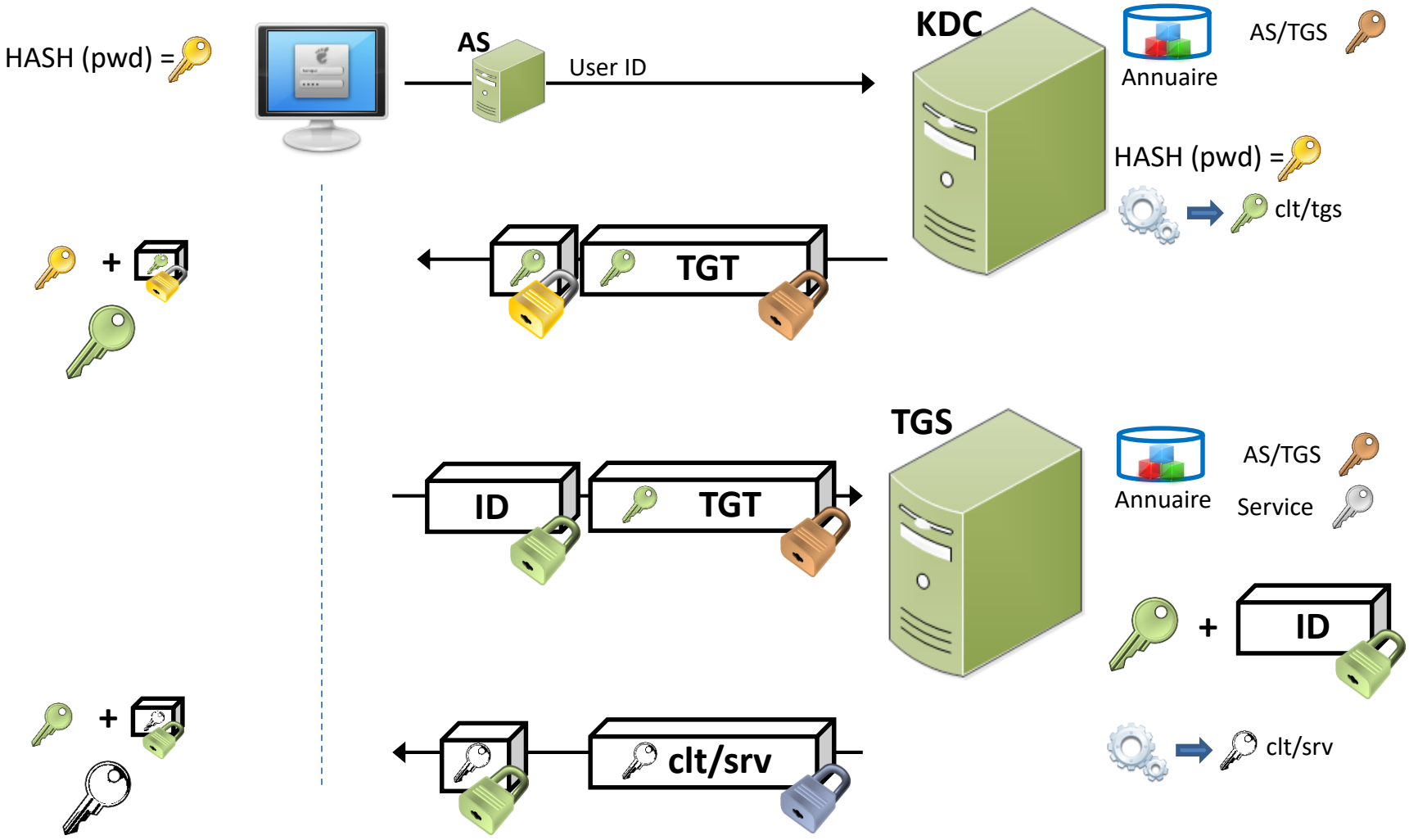
  - **SS**: Service Serveur

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

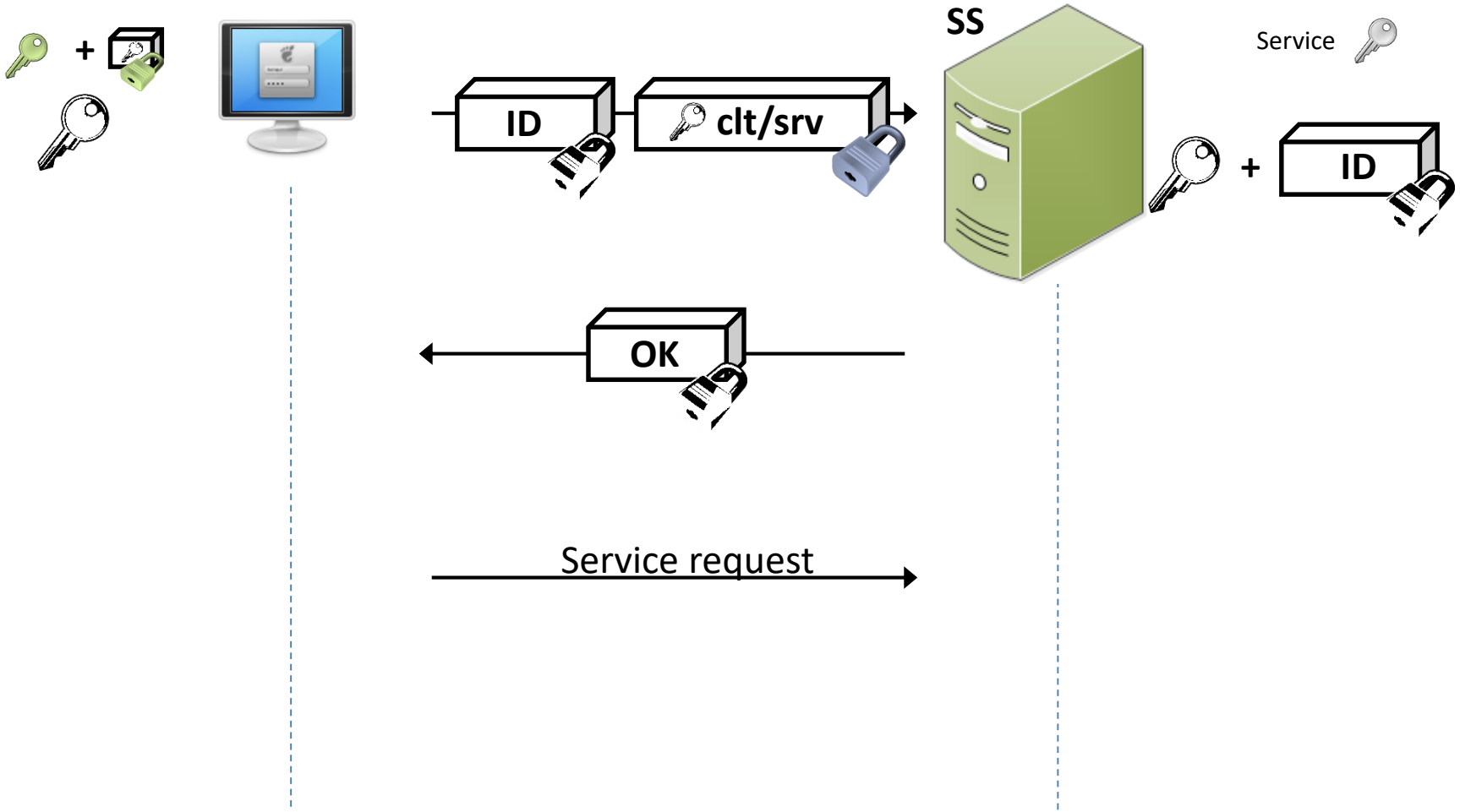
  - **TGT**: Ticket Granting Ticket

    Ticket permettant d'accéder au TGS

Kerberos


HASH (pwd) =
AS
User ID
KDC
Annuaire
AS/TGS
HASH (pwd) =
clt/tgs
+
TGT
TGS
ID
TGT
Annuaire
AS/TGS
Service
+
ID
+
clt/srv
clt/srv

Kerberos



Kerberos

- **Faiblesses**
  - 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

SESAME

- **S**ecure **E**uropean **S**ystem for **A**pplications in a **M**ulti-vendor **E**nvironment

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

SESAME

- **Concepts**
  - **AS:** Authentication serveur

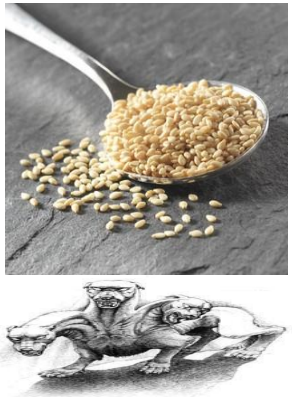
    Authentifier l'utilisateur et fournisseur de jetons pour communiquer avec le PAS

  - **PAS:** Privilège Attribut Service

    Fournisseur de PAC permettant d'accéder aux ressources

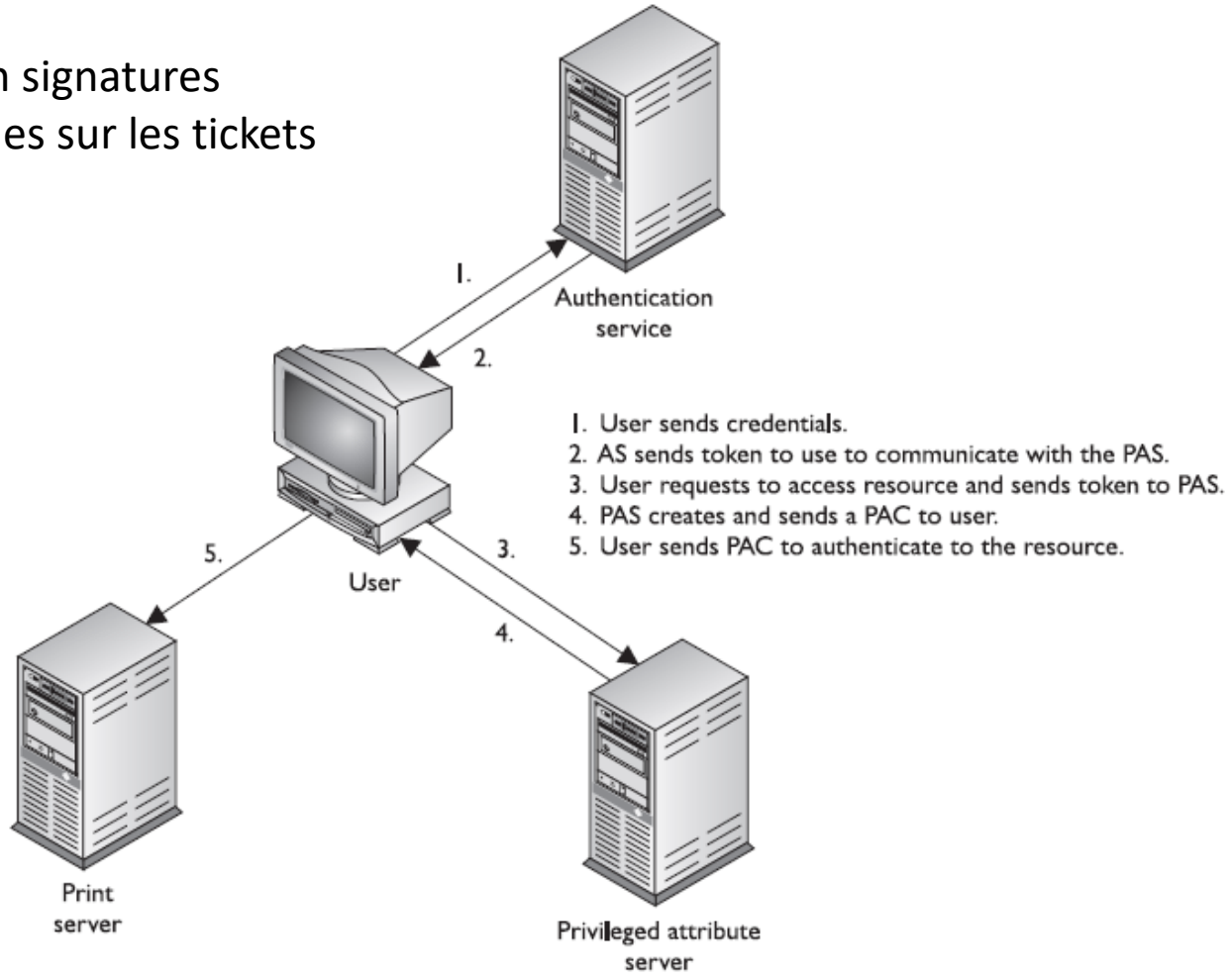
  - **PAC**: Privilège Attribut Certificate

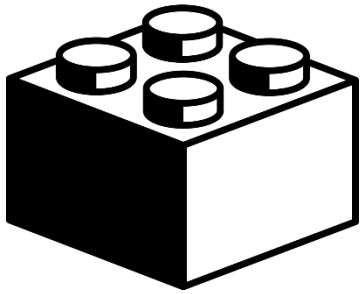
    Ticket permettant d'accéder aux ressources



SESAME

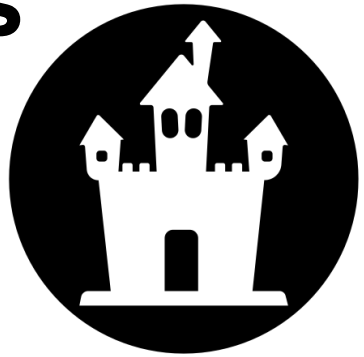
Utilisation signatures numériques sur les tickets





Modèles de contrôle d'accès

Modèles de contrôle d'accès

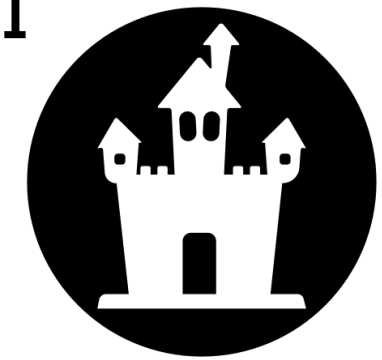


- **Définition**

  Framework définissant comment les sujets ont accès aux objets.

- **Principaux Modèles**
  - **DAC** – **D**iscretionary **A**ccess **C**ontrol
  - **MAC** – Mandatory **A**ccess **C**ontrol
  - **RBAC** – **R**ole **B**ased **A**ccess **C**ontrol

DAC – Discretionary Access Control



❑ Histoire

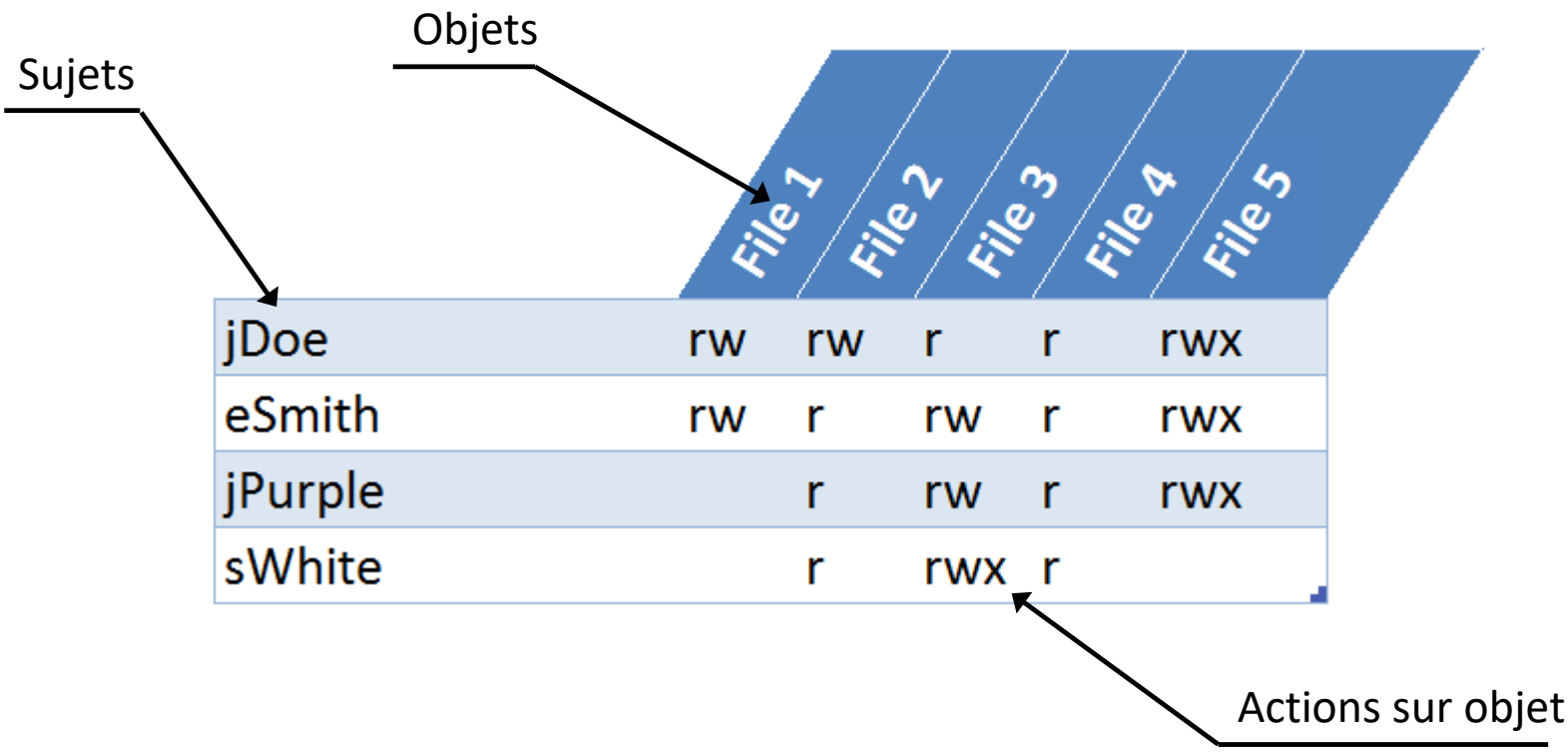
Modèles discrétionnaires (Trusted Computer System Evaluation Criteria, DOD, 1985)

…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

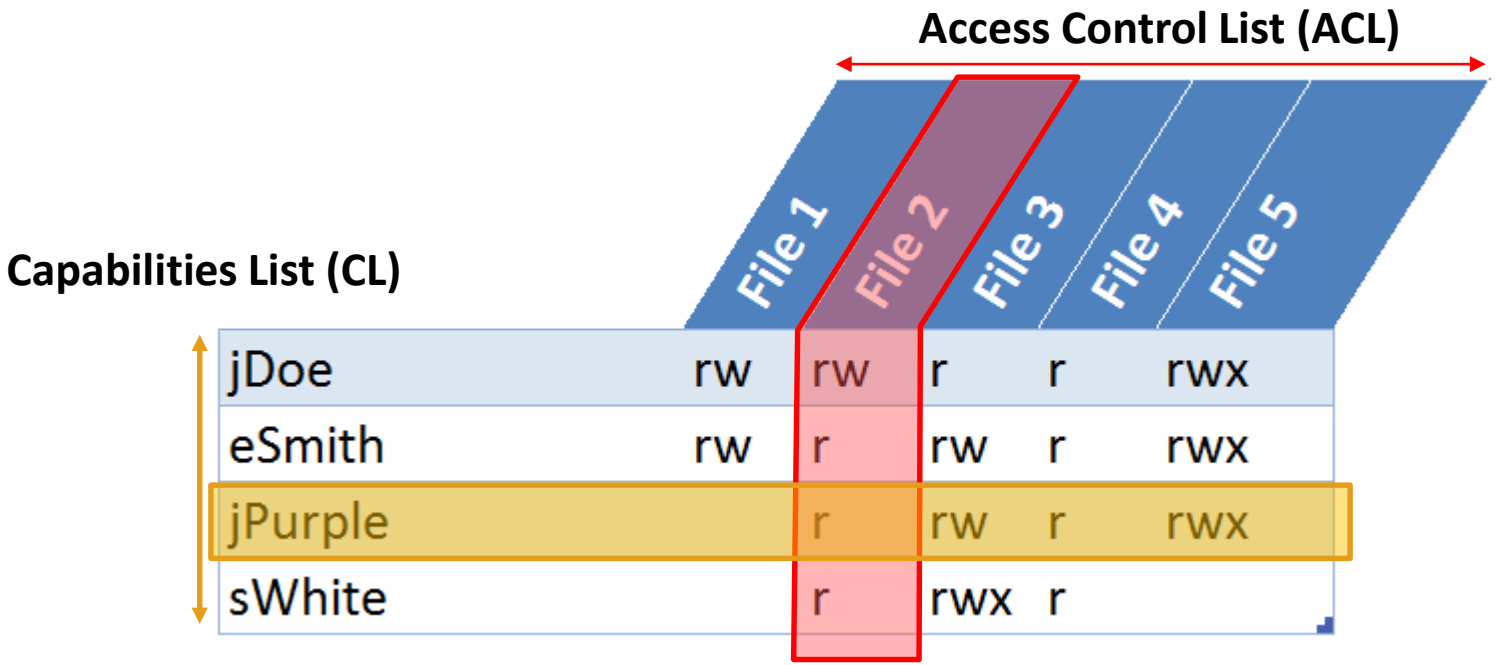
- Les droits sont organisés en matrice
- La définition des droits est laissée à la discrétion des propriétaires des objets.

DAC – Discretionary Access Control

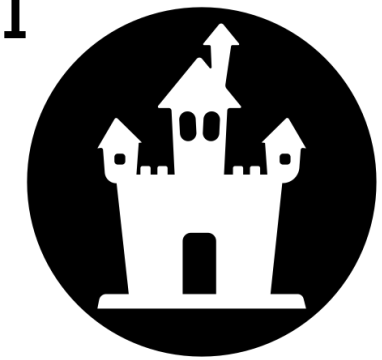


Droits UNIX/LINUX

DAC – Discretionary Access Control



DAC – Discretionary Access Control



- **Limites**
  - Fastidieux
  - Pas de structuration
  - Fastidieux -> erreurs
  - Pas d'assurance que le sytème 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

MAC – Mandatory Access Control

- 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")

CPE LYON

MAC – Mandatory Access Control

2 règles de base pour la dérivation des autorisations

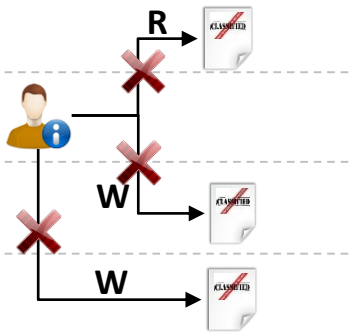
NO READ UP	Un sujet accrédité d'un niveau n ne peut pas accéder en lecture à un niveau n+1,n+2,…n+i
NO WRITE DOWN	Un sujet accrédité d'un niveau n ne peut pas accéder en écriture à des objets de classification n-1,n-2,…n-j

Très secret défense

Secret défense

Confidentiel Défense

Non Classé



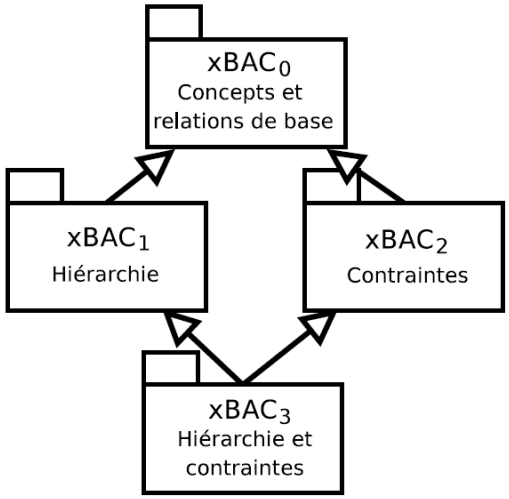
RBAC – Role Base Access Control

Définition

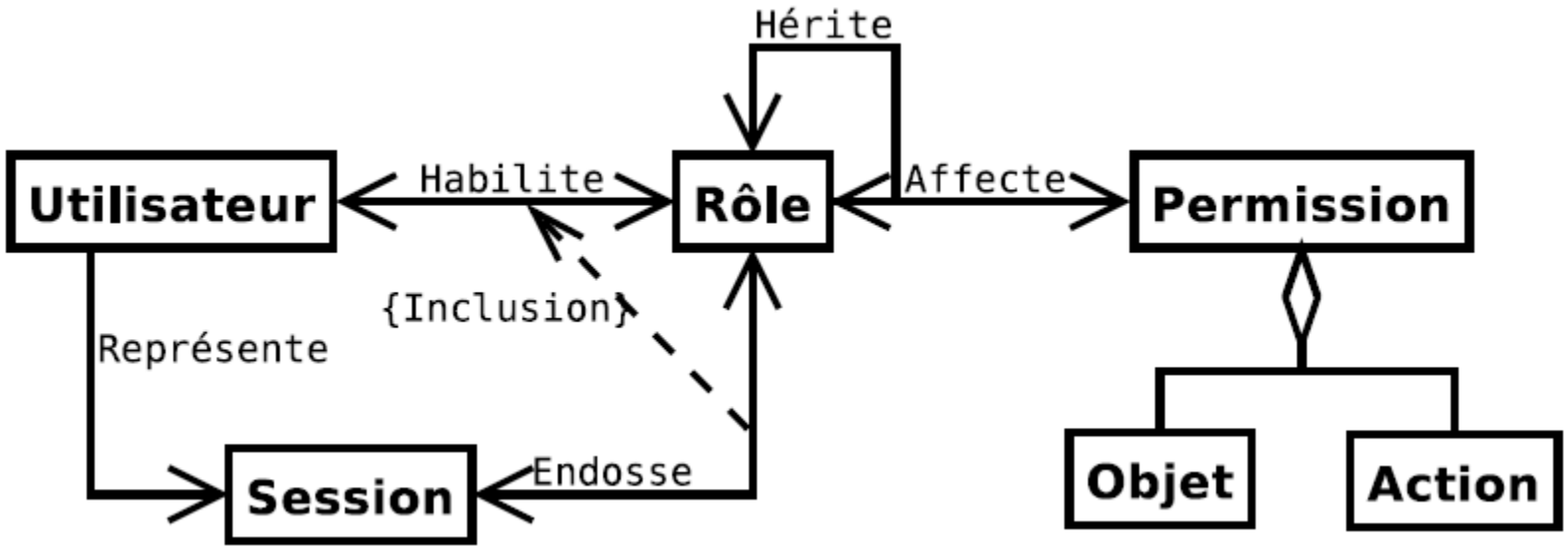
RBAC ou nondiscretionary access control utilise un système de contrôle centralisé déterminant le type d'accès d'un sujet à un objet en fonction de son rôle (job, fonction)

Propriétés

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



$RBAC_0$ – Role Base Access Control



$RBAC_0$ – Role Base Access Control

URA

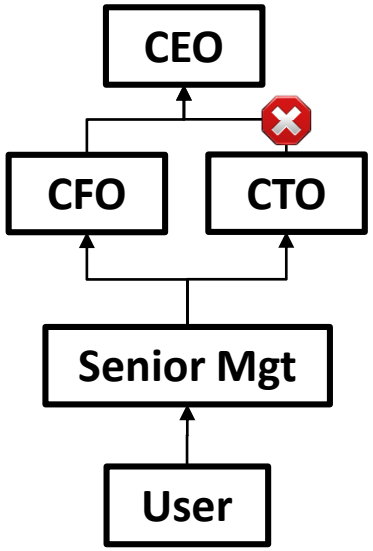
	CEO	CFO	CTO	Senior Mgt	User
jDoe	X				X
eSmith		X		X	X
jPurple			X	X	X
sWhite					X

PRA

	File 1			File 1			File 1			File 1			File 1			File 1		
	R	W	X	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

$RBAC_1$ – Role Base Access Control

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
CFO	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
Senior Mgt										X	X	X	X	X	X	X	X	X
User													X	X	X	X	X	X

$RBAC_2$ – Role Base Access Control

URA

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

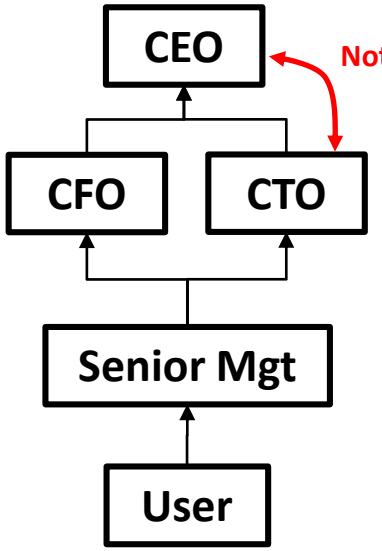
Contraintes
- Acceptable, Non-Acceptable
- Exclusion mutuelle, cardinalité, rôle prérequis

PRA

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

$RBAC_3$ – Role Base Access Control

Contraintes & Hiérarchie

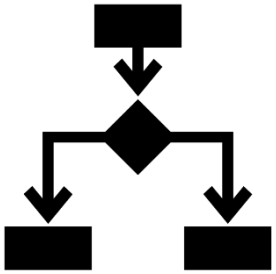


	File 1			File 1			File 1			File 1			File 1			File 1		
	R	W	X	R	W	X	R	W	X	R	W	X	R	W	X	R	W	X
CEO	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X	X
CFO	X			X	X	X	X			X	X	X	X	X	X	X	X	X
CTO	X									X	X	X	X	X	X	X	X	X
Senior Mgt										X	X	X	X	X	X	X	X	X
User													X	X	X	X	X	X

Not acceptable

RBAC – Role Base Access Control

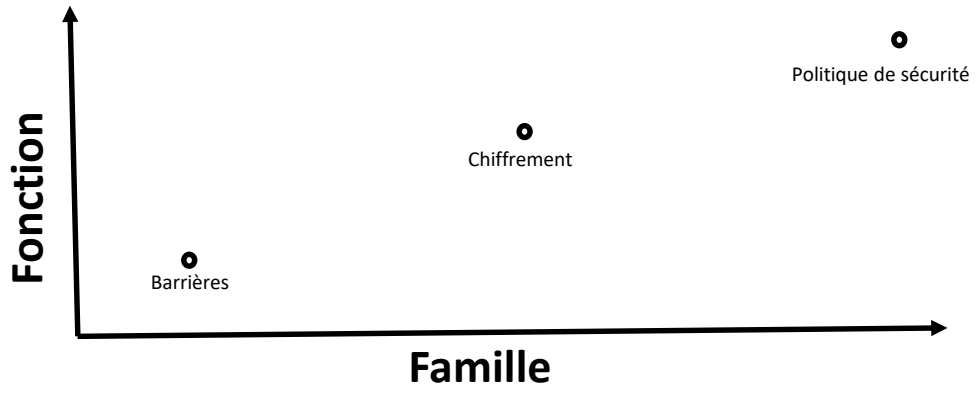
- **Avantages**
  - Passage à l'échelle
  - S'adapte facilement aux organisations:
    - Organisation flexible
    - Turn over
  - Customisation des droits (contraintes et hiérarchies)
- **Limites**
  - Difficile à mettre en œuvre si la hiérarchie et les rôles sont faiblement documenté
  - Politique organisationnelle trop détaillée peut freiner la croissance de l'entreprise
- **Exemple d'utilisation**
  - Produit CISCO, OS Windows, Solaris, HP



Famille de Contrôles d'Accès

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

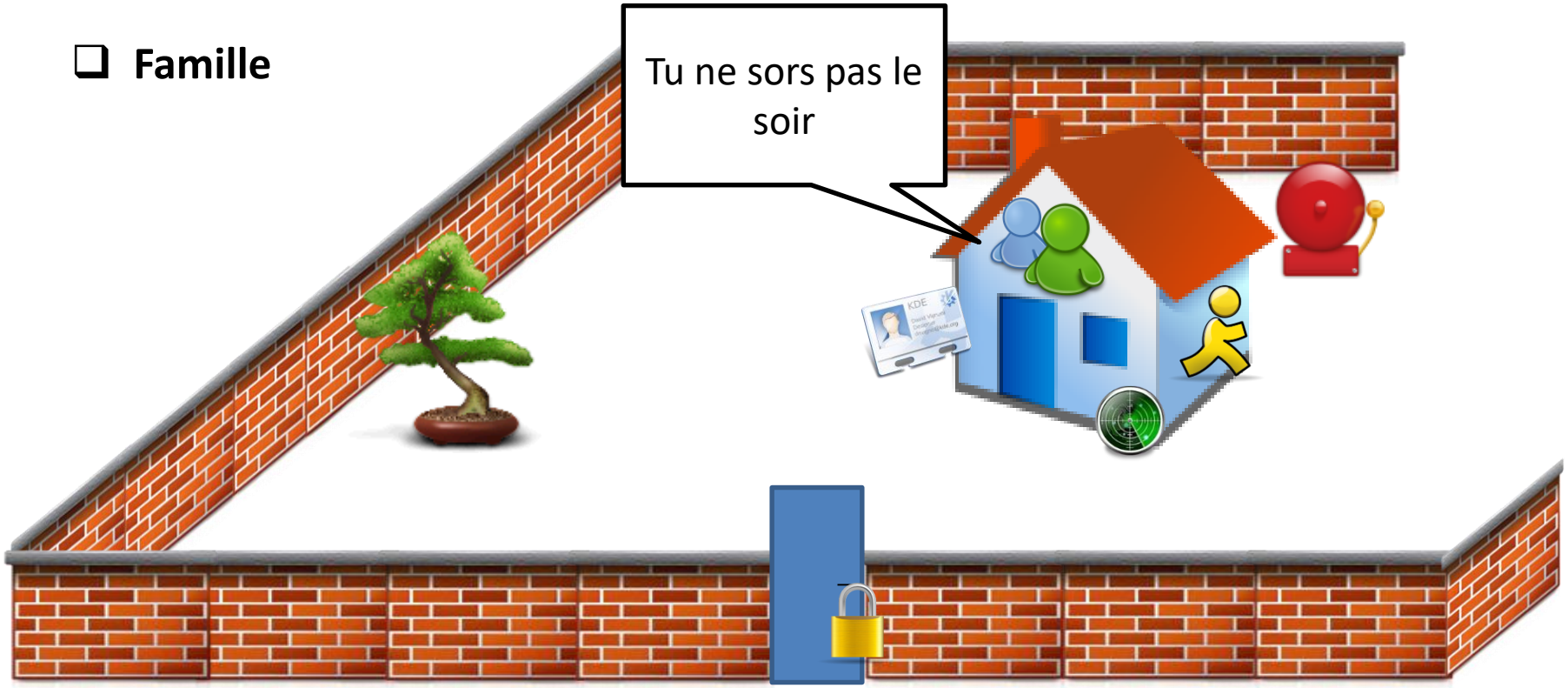


Famille de contrôle d'accès

- **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

Famille de contrôle d'accès

- Famille

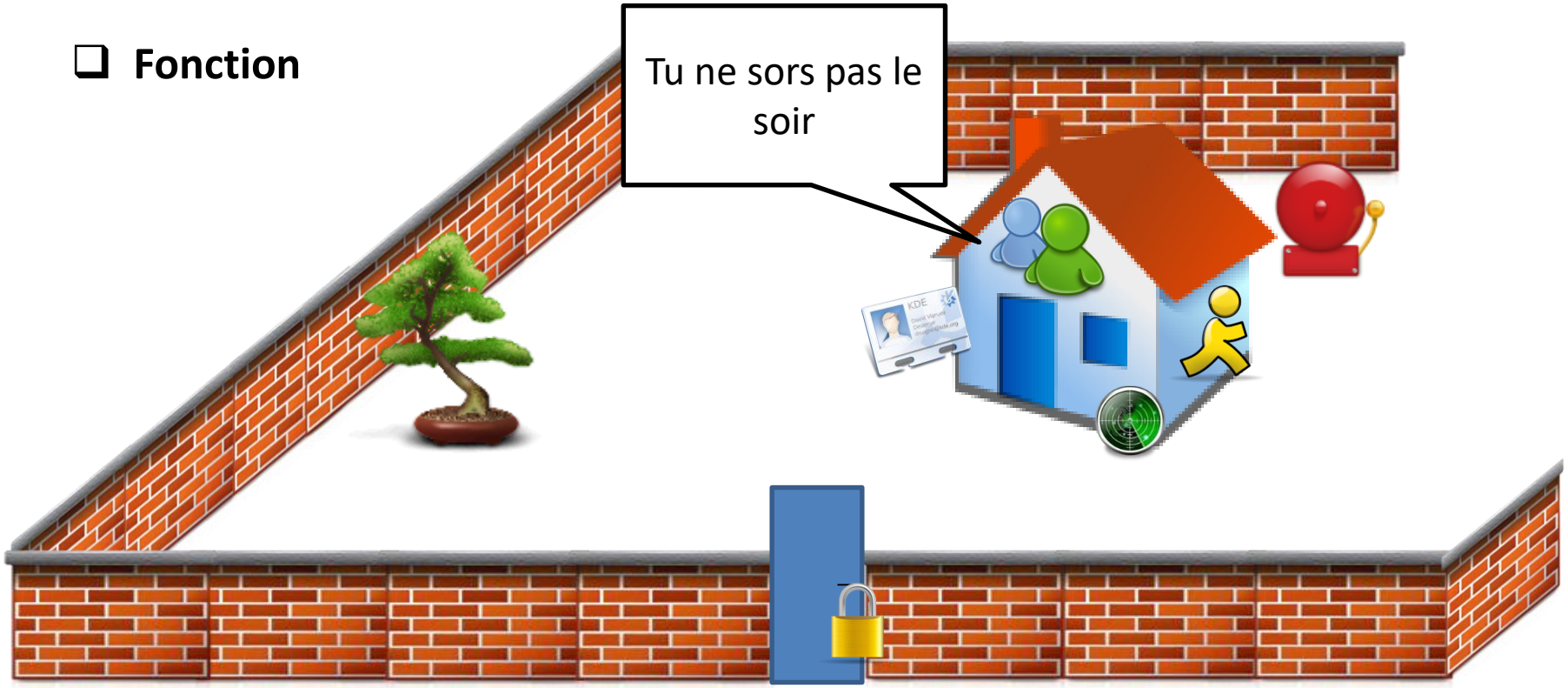


Famille de contrôle d'accès

- **Fonction**
  - **Dissuasion**: Décourage un attaquant potentiel
  - **Prévention**: Eviter un incident, une attaque
  - **Correction**: Réparer des composants ou système après ur 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

- **Fonction**



Famille de contrôle d'accès

- **Fonction**
  - **Dissuasion**: Décourage un attaquant potentiel
  - **Prévention**: Eviter un incident, une attaque
  - **Correction**: Réparer des composants ou système après ur 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

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

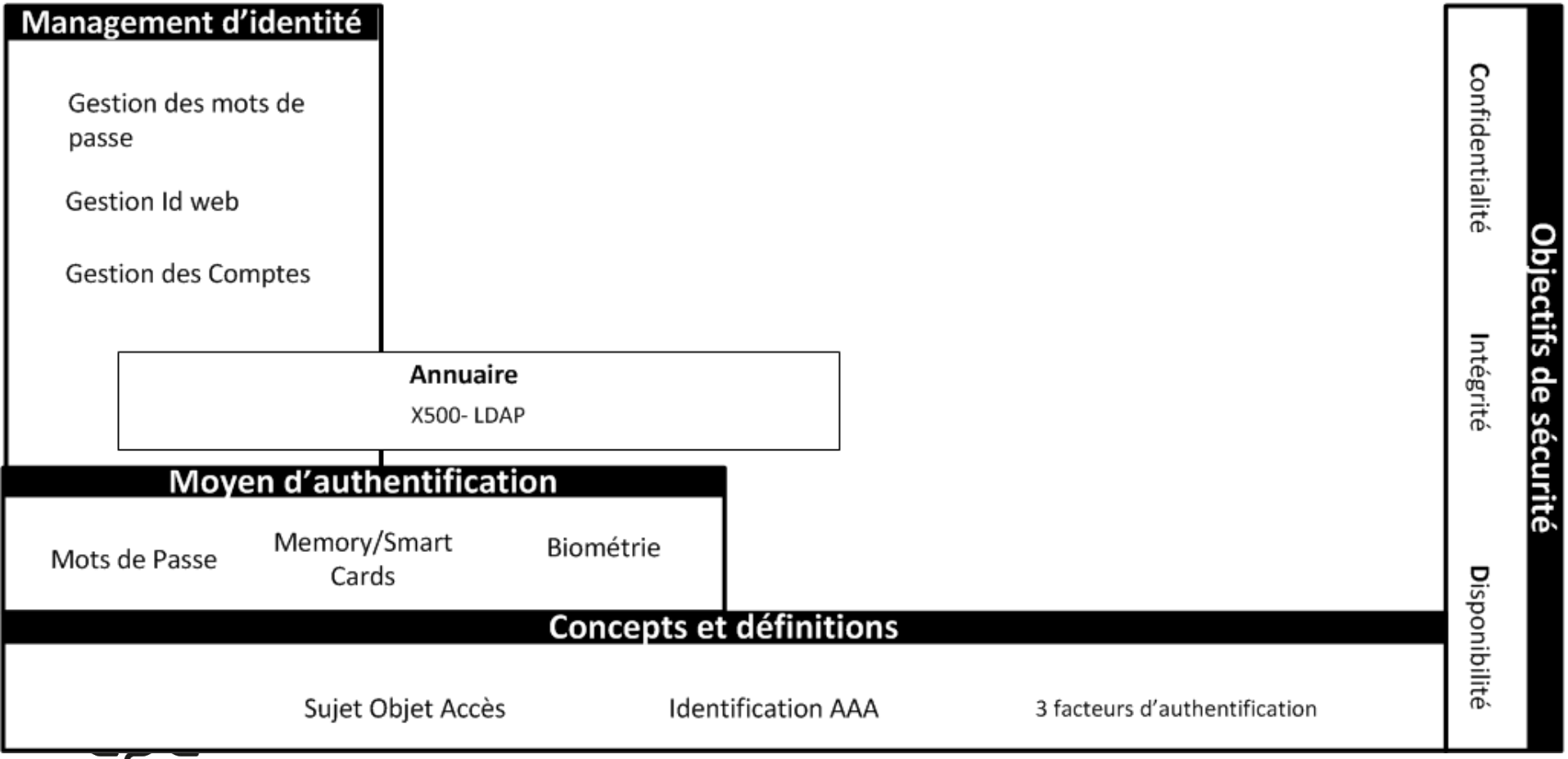
Famille de contrôle d'accès

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

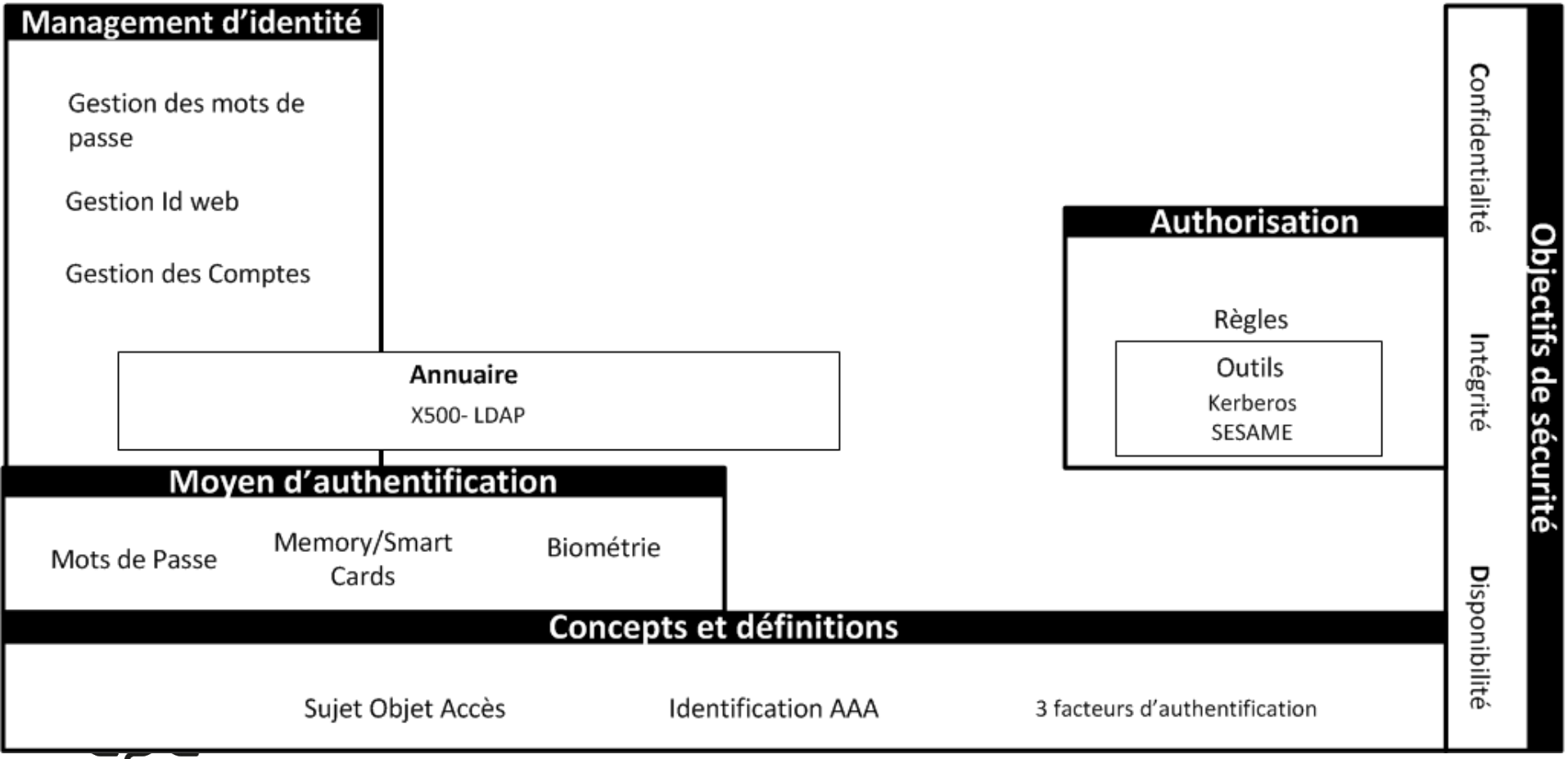
Conclusion

Conclusion

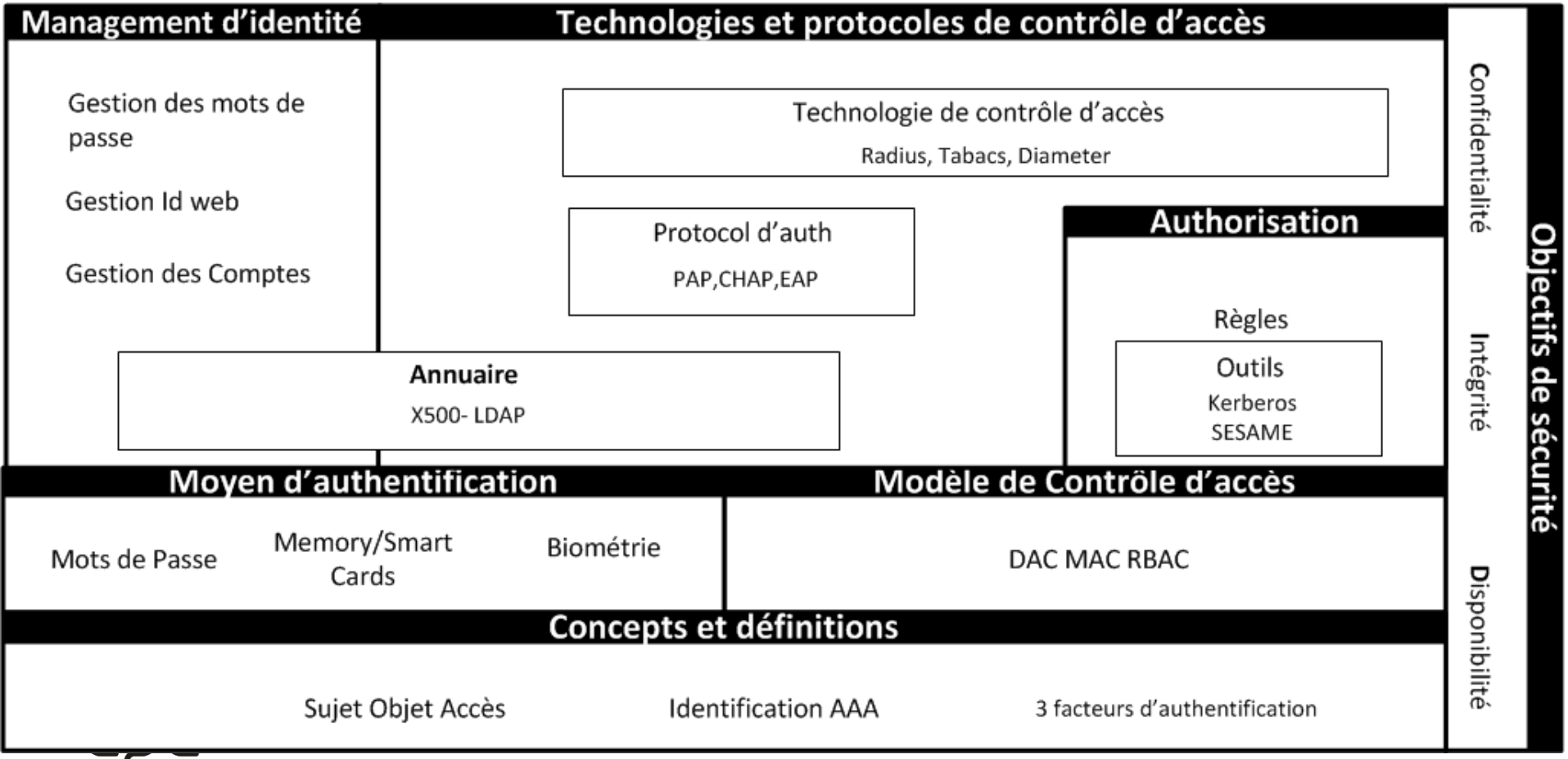
Conclusion



Conclusion



Conclusion



Questions ?

Jacques Saraydaryan

Jacques.saraydaryan@cpe.fr