L'AUTHENTIFICATION

DÉFINITIONS

- **La notion d'authentification s'oppose à celle de l'identification d'une personne physique ou morale (dirigeant et toute personne autorisée). Cette distinction est importante puisque par abus de langage, on parle d'authentification alors qu'il s'agit d'identification. Explications :**
  - **Lorsqu'une personne présente sa pièce d'identité lors d'un contrôle, elle est identifiée grâce à un document officiel, mais n'est pas authentifiée, car le lien entre la pièce d'identité et la personne n'est pas établie de façon indiscutable, irrévocable et reconnue par les tribunaux en cas de litige.**

  Par opposition,

  - **Lorsqu'une personne est authentifiée, cette authentification doit-être apportée par un tiers de confiance et par une preuve au sens juridique reconnue devant les tribunaux (ex: la signature électronique de la carte bancaire).**

EXEMPLE DU COMPTE D'ACCÈS À UN SI

- **L'identification est une phase qui consiste à établir l'identité de l'utilisateur. Elle permet répondre à la question : "Qui êtes vous ?". L'utilisateur utilise un identifiant (que l'on nomme "Compte d'accès", "Nom d'utilisateur" ou "Login" en anglais) qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.**
- **L'authentification est une phase qui permet à l'utilisateur d'apporter la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connait.**

- **En synthèse, la charge de la preuve émanant d'un tiers de confiance distingue l'identification de l'authentification en cas de litige ou de contestation.**

FACTEURS D'AUTHENTIFICATION *(PREUVES)*

- **Dans le cas d'un individu, l'authentification consiste, en général, à vérifier que celui-ci possède une preuve de son identité ou de son statut, sous l'une des formes (éventuellement combinées) suivantes :**
  - **Ce qu'il sait (mot de passe, numéro d'identification personnel (PIN), une phrase secrète …).**
  - **Ce qu'il détient (acte de naissance, certificat d'immatriculation, carte à puce, droit de propriété, certificat électronique, diplôme, passeport, Token OTP, Carte OTP, Téléphone portable, PDA, etc.).**
  - **Ce qu'il est, soit une personne physique (empreinte digitale, empreinte rétinienne, structure de la main, structure osseuse du visage ou tout autre élément biométrique)**
  - **Ce qu'il sait faire ou fait, soit une personne physique (biométrie comportementale tel que signature manuscrite, reconnaissance de la voix, un type de calcul connu de lui seul, un comportement, etc.)**
  - **Où l'entité est, soit un endroit d'où, suite à une identification et authentification réussie, elle est autorisée (accéder à un système logique d'un endroit prescrit)**

REMARQUE

- **L'entité authentifié peut être:**
  - **Dans la majorité des cas, une personne physique - individu - personne morale**
  - **un objet comme, par exemple, une application web utilisant le protocole SSL, un serveur SSH, un objet de luxe, une marchandise, un animal, etc.**

POURQUOI S'AUTHENTIFIER

- **On peut considérer que l'authentification forte est une des fondations essentielles pour garantir :**
  - **L'autorisation ou contrôle d'accès (qui peut y avoir accès)**
  - **La confidentialité (qui peut le voir)**
  - **L'intégrité (qui peut le modifier)**
  - **La traçabilité (qui l'a fait)**
  - **L'irrévocabilité (qui peut le prouver)**

Cette approche est toutefois modulée par l'ANSSI dans son référentiel général de sécurité

MÉTHODES DE VÉRIFICATION

- **La phase de vérification fait intervenir un protocole d'authentification. On en distingue trois sortes « familles » :**
  - **L'authentification simple**
  - **L'authentification forte**
  - **L'Authentification unique**

L'AUTHENTIFICATION SIMPLE

- **l'authentification ne repose que sur un seul élément ou « facteur » . C'est le cas de la plupart des systèmes d'authentification courants**
- **Le facteur le plus utilisé est le mot de passe, dans ce cas, il est important que la politique de mot de passe renforce sa sécurité.**

Facteur d'authentification	Exemple d'authentification simple
Ce que l'on sait	Mot de passe
Ce que l'on possède	Radio-identification
Ce que l'on est	Empreinte digitale

L'AUTHENTIFICATION FORTE

L'AUTHENTIFICATION FORTE

- **L'authentification forte est, en sécurité des systèmes d'information, une procédure d'identification qui requiert la concaténation d'au moins deux facteurs d'authentification.**
- **Il est recommandé d'utiliser plusieurs facteurs de nature distincte afin de rendre la tâche plus compliquée à un éventuel attaquant.**
- **La Norme FIDO fixe la référence en la matière. D'ailleurs Windows 10 intègre un mécanisme d'authentification FIDO compatible. Il s'agit de suivre une authentification à plusieurs étapes grâce à des mots de passe, une empreinte digitale, le scan de l'œil, la reconnaissance vocale ou plus simplement grâce à une clé USB de sécurité dédiée.**

PRINCIPE DE L'AUTHENTIFICATION FORTE

« Authentifieur »

Quelque chose
que l'on possède

Secret

Quelque chose
que l'on connaît

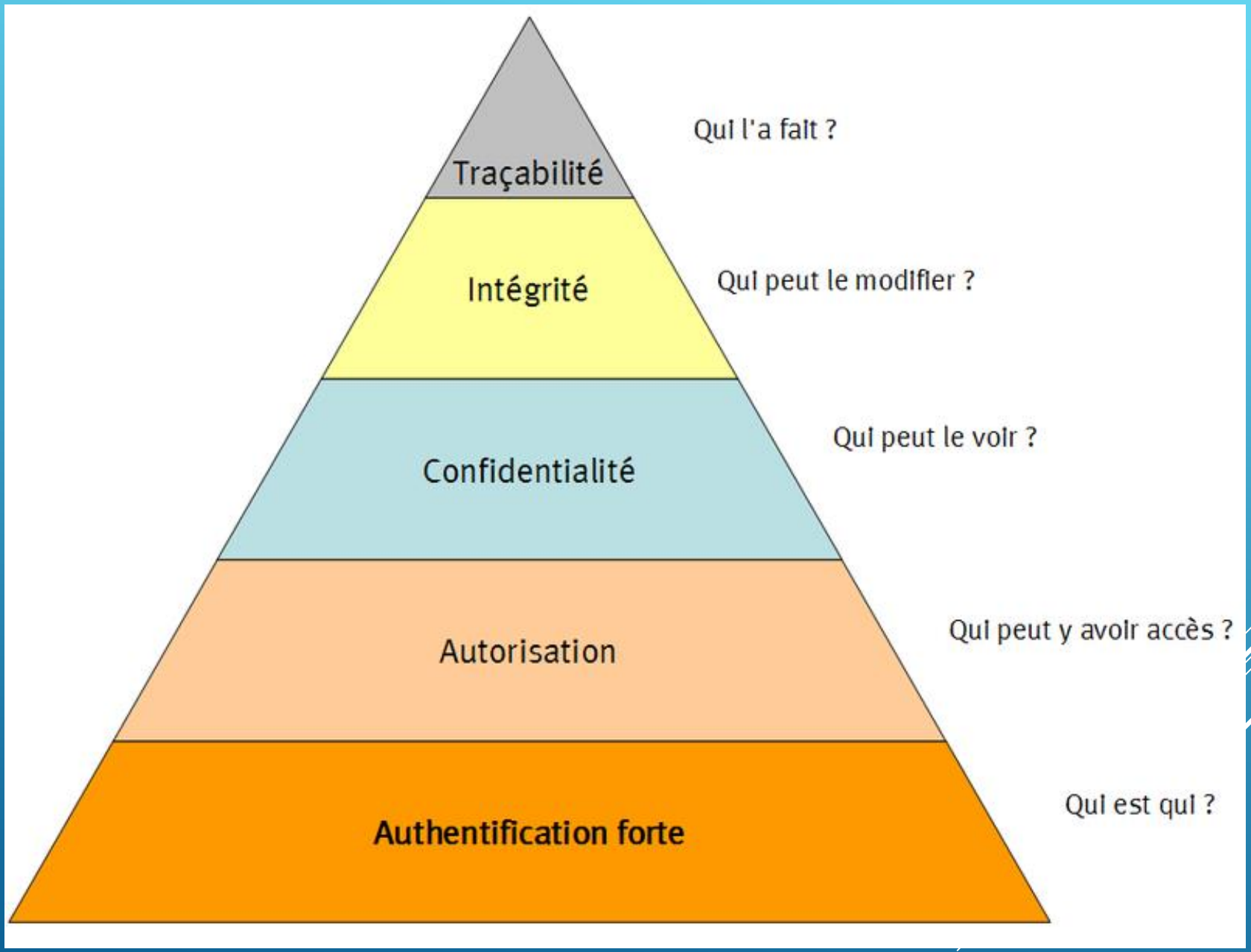
H34ff34QF

PIN Code

Authentification
forte

Biométrie

Quelque chose
que l'on est ou fait


Traçabilité
Qui l'a fait ?
Intégrité
Qui peut le modifier ?
Confidentialité
Qui peut le voir ?
Autorisation
Qui peut y avoir accès ?
Authentification forte
Qui est qui ?

POURQUOI L'AUTHENTIFICATION FORTE ?

- **Le mot de passe est actuellement le système le plus couramment utilisé pour authentifier un utilisateur. Il n'offre plus le niveau de sécurité requis pour assurer la protection de biens informatiques sensibles, car différentes techniques d'attaque permettent de le trouver facilement.**
- **On recense plusieurs catégories d'attaques informatiques pour obtenir un mot de passe :**
  - **Attaque par force brute**
  - **Attaque par dictionnaire**
  - **Écoute du clavier informatique (keylogger), par voie logicielle (cheval de troie...), ou par écoute distante (champ électrique des claviers filaires, ou ondes radio faiblement chiffrées pour les claviers sans fils)**
  - **Écoute du réseau (password sniffer) : plus facilement avec les protocoles réseau sans chiffrement, comme HTTP, Telnet, FTP, LDAP, etc.**
  - **Hameçonnage (ou filoutage), appelé en anglais phishing**
  - **Attaque de l'homme du milieu ou Man In The Middle attack (MITM) : par exemple avec les protocoles SSL ou SSH**
  - **Ingénierie sociale (faille humaines)**
  - **Extraction d'informations par torture, chantage ou menaces**

FAMILLES TECHNOLOGIQUES POUR L'AUTHENTIFICATION FORTE

- **On dénombre actuellement quatre familles :**
  - **One Time Password (OTP) / Mot de passe à usage unique.**
  - **Certificat numérique**
  - **Biométrie**

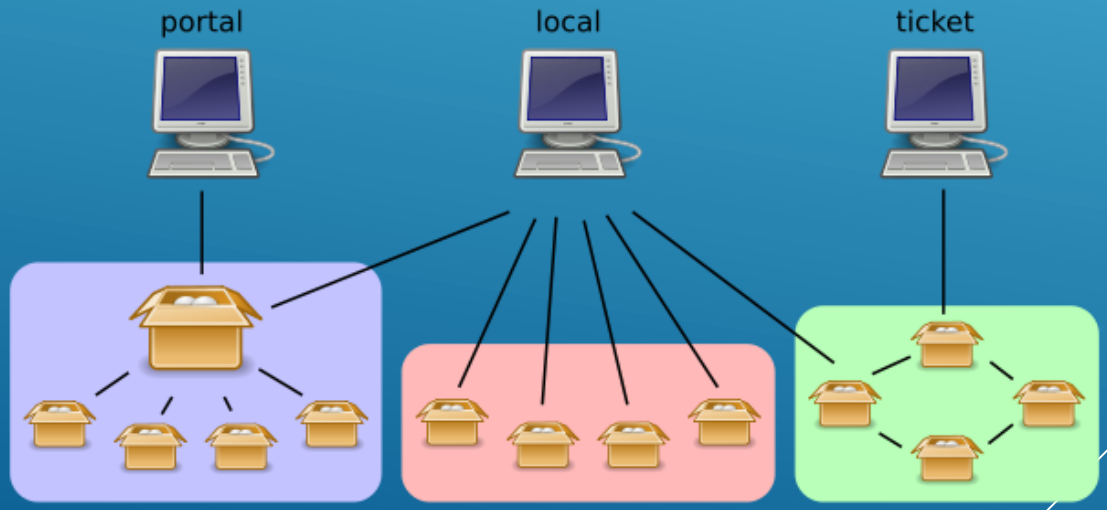
SOLUTIONS D'AUTHENTIFICATION FORTE

- OTP
  - RSA SecureID
  - Safenet
  - UniOTP distribué en France par CodeAndSoft
  - privacyIDEA Open Source Two Factor Authentication System
- Carte à puce, token pki
  - Safenet
  - Feitian
- Authentifieur USB
  - UniKey de Iolock
  - DinkeyWEB de APLIKA
  - VeriSign
- BIOMETRIE
  - UBKEY scan de l'iris distribué en France par CodeAndSoft
  - Myiris de EYELock
  - TouchID de Apple empreinte digitale
  - 3D Intel real sense reconnaissance faciale
  - NUANCE reconnaissance Vocale

L'AUTHENTIFICATION UNIQUE

DÉFINITION

- **Ou identification unique ; en anglais Single Sign-On ou SSO):**
  - **est une méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques (ou sites internet sécurisés).**



Trois approches d'authentification unique

PROTOCOLES D'AUTHENTIFICATION

EXEMPLES DE PROTOCOLES D'AUTHENTIFICATION

- **De façon appliquée, voici quelques exemples de protocoles d'authentification :**
  - **802.1x mécanisme standard de contrôle de port et d'authentification.**
  - **TLS/~~SSL~~ (qui peut également fournir du chiffrement)**
  - **NTLM (utilisé dans les réseaux de Microsoft Windows)**
  - **Kerberos (standard utilisé par Windows et bien d'autres systèmes)**
  - **Central Authentication Service (CAS) Mécanisme d'authentification et de SSO, libre et gratuit développé par l'Université Yale**
  - **Needham-Schroeder Authentication Protocol**

IEEE 802.1X

DÉFINITION

- **IEEE 802.1X est un standard lié à la sécurité des réseaux informatiques, mis au point en 2001 par l'IEEE.**
- **Il permet de contrôler l'accès physique aux équipements d'infrastructures réseau (et par ce biais, de relayer les informations liées aux dispositifs d'identification).**
- **Les réseaux ont deux exigences importantes auxquelles peut répondre cette norme :**
  - **Sécurité : Authentification et Autorisation**
  - **Flexibilité : Possibilité du Roaming**

PRINCIPE GÉNÉRAL DE FONCTIONNEMENT

- En s'appuyant sur le protocole **EAP** pour le transport des informations d'identification en mode client/serveur, et sur un serveur d'authentification (tel que **RADIUS**, **TACACS**, **CAS**, etc.) le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des **réseaux câblés** et **sans fil**.
- Si un équipement réseau actif, tel qu'un commutateur réseau ou une borne Wi-Fi est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (**PAE**).
- Indépendamment du type de connexion, chaque **port** se comporte alors comme une bascule à **deux états** : un état **contrôlé** en cas de succès d'identification et un état **non contrôlé** en cas d'échec.

PRINCIPE DE MISE EN ŒUVRE

- **La mise en œuvre d'un contrôle d'accès par port 802.1X nécessite l'activation du standard IEEE 802.1X sur :**
  - **les commutateurs réseau ou les points d'accès sans fil (clients d'identification) ;**
  - **chaque point terminal appelé « supplicant » en EAP ordinateur hôte (et éventuellement chaque imprimante, PDA, équipement VOIP, etc.) ;**
  - **le serveur d'authentification chargé de valider l'identité de l'utilisateur du port ; la norme 802.1X ne présente qu'un seul exemple de protocole : RADIUS, par exemple.**

COMPATIBILITÉ ET IMPLÉMENTATION

- **Tous les matériels n'intègrent pas forcément le standard 802.1x sur leurs équipements. Cependant, les grands fabricants informatiques l'intègrent depuis plusieurs années dans leurs modèles.**
- **Les serveurs RADIUS récents gèrent le 802.1X, avec des variations sur les protocoles EAP acceptés.**
- **Les systèmes d'exploitation récents disposent d'un « supplicant » 802.1X : Windows depuis Windows 2000, distributions Linux, Mac OS ; là aussi des variations sur les protocoles EAP pris en charge.**

CONTEXTE

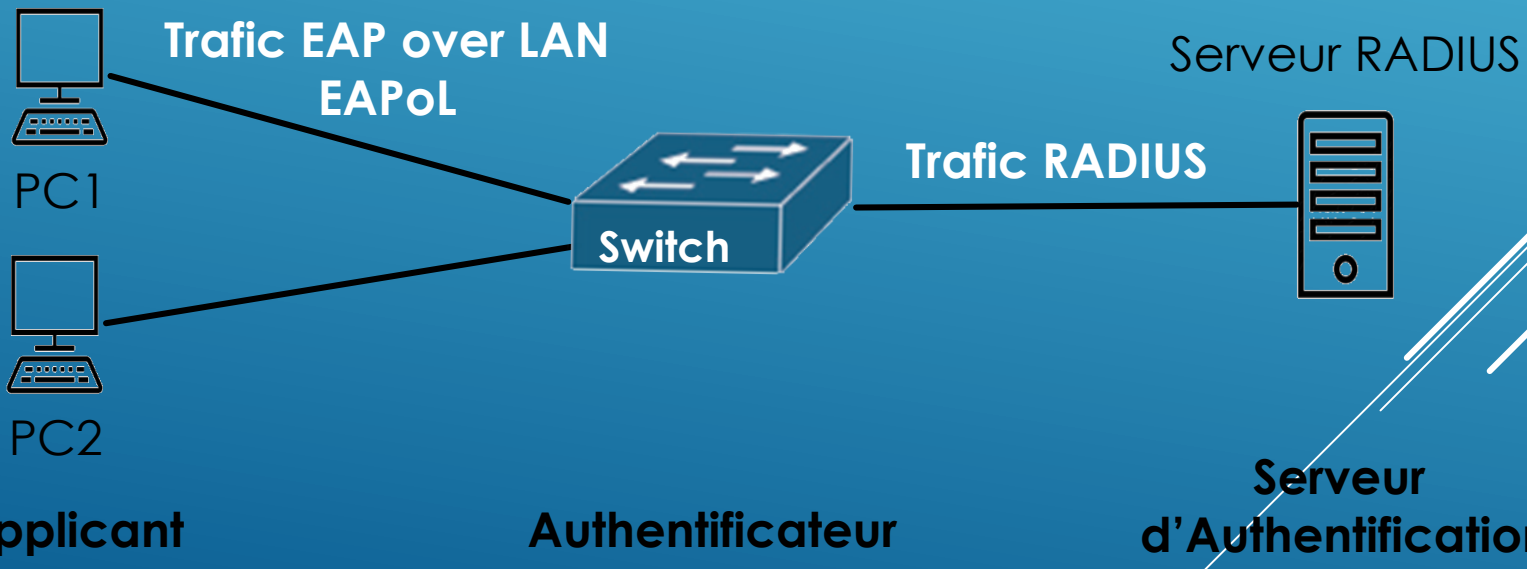
- **Besoin de s'authentifier dès l'accès physique au réseau.**
- **Standardiser un mécanisme de relais d'authentification de niveau 2 par l'IEEE.**
- **Inefficacité des mécanismes d'authentification (clé statique)**
- **Vulnérabilités des mécanismes de chiffrement des données**
  - **implémentation défaillante de l'algorithme RC4**
  - **cas du WiFi, faiblesse du protocole WEP.**

OBJECTIFS

- **Simplement contrôler l'accès physique à un réseau local**
- **Une phase d'authentification indépendante du système de transmission utilisé, basé sur des systèmes existants**
- **Simplifier l'administration du réseau (affectation dynamique des VLAN en fonction des caractéristiques de cette authentification…)**
- **développé pour les commutateurs LAN (prises Ethernet, …)**
- **En Wifi doit permettre l'authentification du demandeur, le contrôle d'accès aux bornes et la distribution des clés WEP**

LES ÉQUIPEMENTS

- **Supplicant, client du réseau**
- **Authenticator, équipement de niveau 2**
- **Authentication Server, serveur validant l'accès, RADIUS (Remote Authentication Dial-In User Service)**

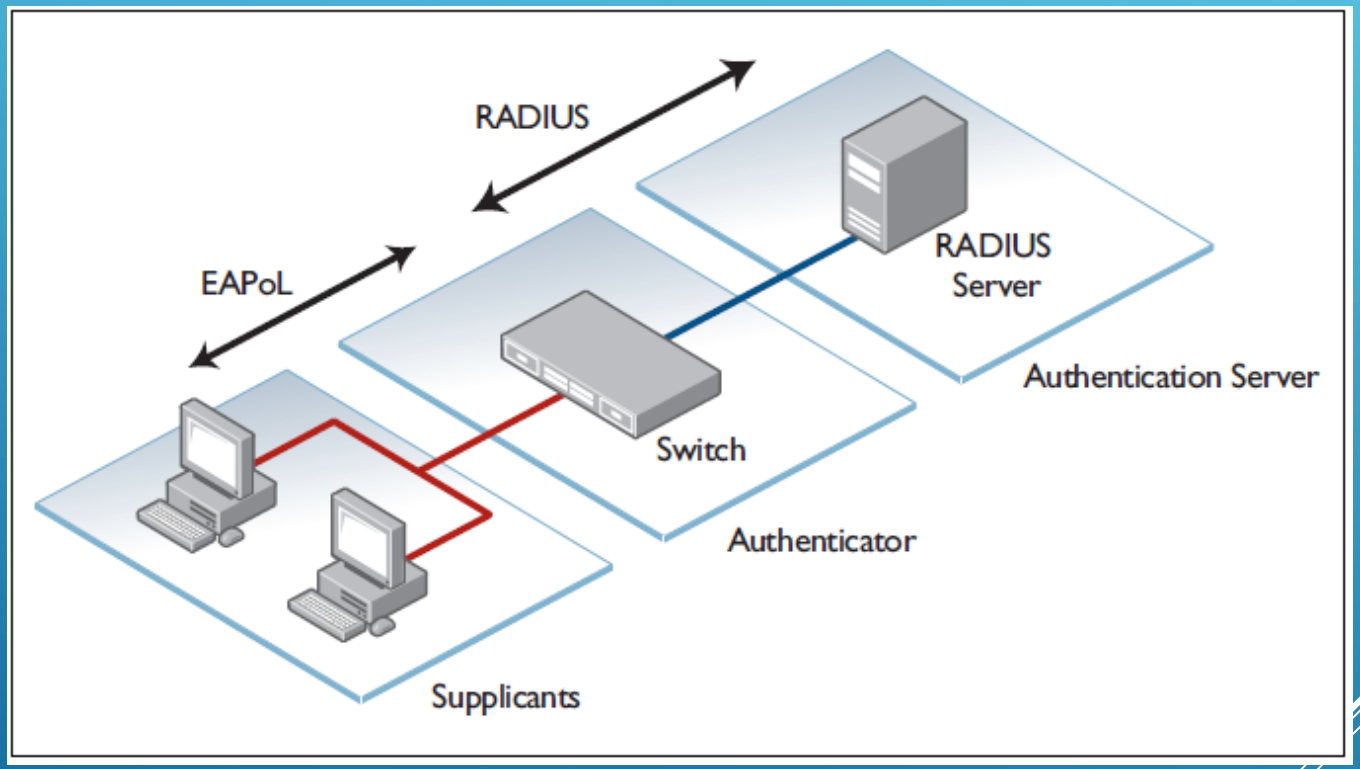


CONCEPTS STANDARDS

- **Le système authentificateur contrôle une ressource disponible via le point d'accès physique au réseau, nommé PAE (Port Access Entity).**
- **Le système à authentifier souhaite accéder à cette ressource, il doit donc pour cela s'authentifier.**
- **protocole particulier : l'EAP (Extensible Authentification Protocol).**
- **s'appuie sur des mécanismes d'authentification existants**

CONCEPTS STANDARDS

- **La norme 802.1X norme fait intervenir 3 entités**



Remarques: ce modèle est indépendant de la nature physique de la connexion.

LE CAS CLASSIQUE

- **Le système à authentifier est un poste de travail ou un serveur.**
- **Le serveur d'authentification est typiquement un serveur Radius, ou tout autre équipement capable de faire de l'authentification.**
- **On a un contrôle d'accès uniquement basé sur la valeur de l'adresse MAC/Ethernet**

PARTICULARITÉ DU 802.1X

- **Durant la phase d'authentification 802.1X, le système authentificateur se comporte comme un mandataire (proxy) entre le système à authentifier et le serveur d'authentification .**
- **Le supplicant souhaite accéder aux ressources du réseau. Mais pour cela il va devoir s'authentifier.**
- **Le système authentificateur gère cet accès via le PAE.**
- **Le supplicant va dialoguer indirectement avec le serveur via le relais (Switch), grâce au protocole EAP.**

PARTICULARITÉ DU 802.1X

- **La structure du 802.1x s'appuie donc sur 4 couches :**
- **couche média : Token Ring, Ethernet, ..**
- **couche protocole : EAP, protocole d'identification**
- **couche méthode d'authentification : elle s'appuie sur les mots de passe, les certificats, …**
- **couche infrastructures qui comporte le matériel d'authentification comme le serveur Radius, …**

PARTICULARITÉ DU 802.1X

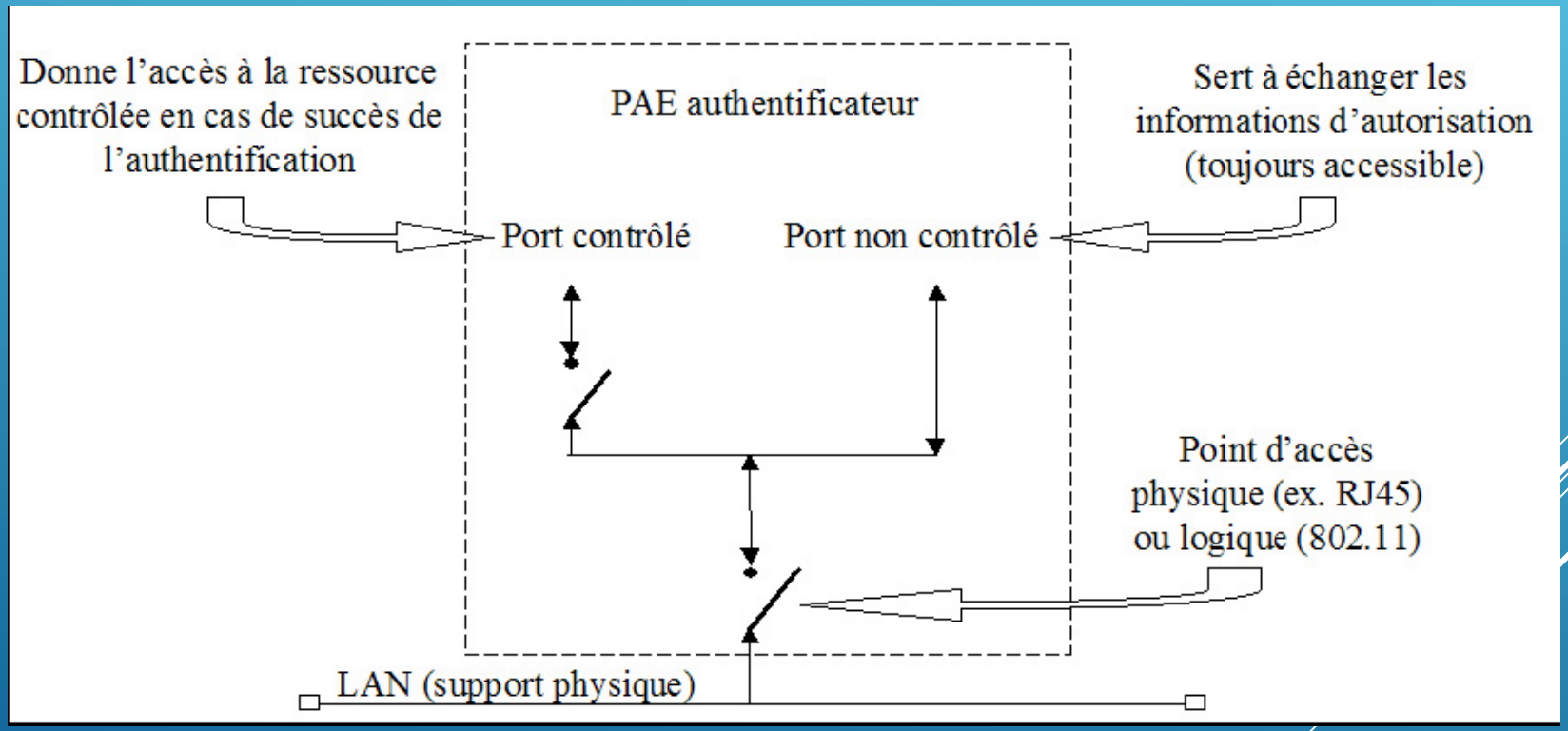
- 802.1x consiste à scinder le port d'accès physique au réseau en deux ports logiques, qui sont connectés en parallèle sur le port physique.
- Le premier port logique est dit « contrôlé »
  - ouvert
  - fermé
- Le deuxième port logique est, lui, toujours accessible mais il ne gère que les trames spécifiques à 802.1X.

LES ÉTATS DU PORTS

- **Par défaut en mode unauthorized**
- **Connexion, requête d'authentification**
  - **Port en mode authorized si valide**
  - **Port en mode unauthorized sinon**
- **Déconnexion, port en mode unauthorized**
- **Client ne supportant pas le 802.1x, port en mode unauthorized, possibilité d'activé le port avec un accès restreint.**
- **Expiration des timers de session, port en mode unauthorized**

FONCTIONNEMENT

- **Le point d'accès au réseau (PAE)**

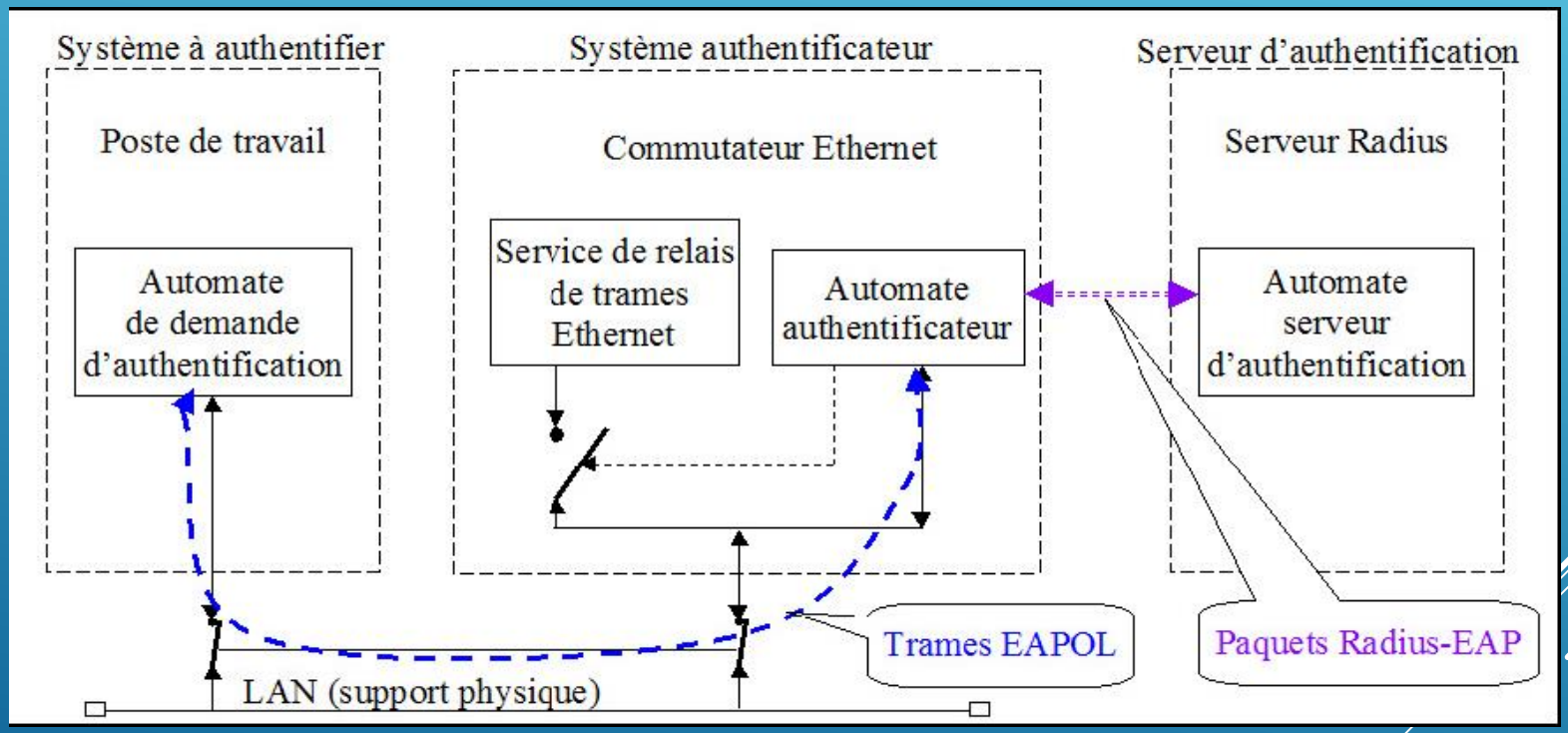


FONCTIONNEMENT

- La norme 802.1X s'appuie sur les standards existants.
- Le dialogue entre le système authentificateur et le système à authentifier se fait en utilisant le protocole EAP (PPP Extensible Authentication Protocol).
- Les paquets EAP sont transportés dans des trames Ethernet spécifiques EAPoL (EAP Over Lan) qui sont marquées avec le numéro de type (Ethertype) égal à 88FE.
- Le dialogue entre le système authentificateur et serveur d'authentification se fait par une simple « ré-encapsulation » des paquets EAP dans un format qui convient au serveur d'authentification, sans modification du contenu du paquet par le système authentificateur.
- Ce dernier effectue cependant une lecture des informations contenues dans les paquets EAPoL afin d'effectuer les actions nécessaires sur le port contrôlé (blocage ou déblocage).

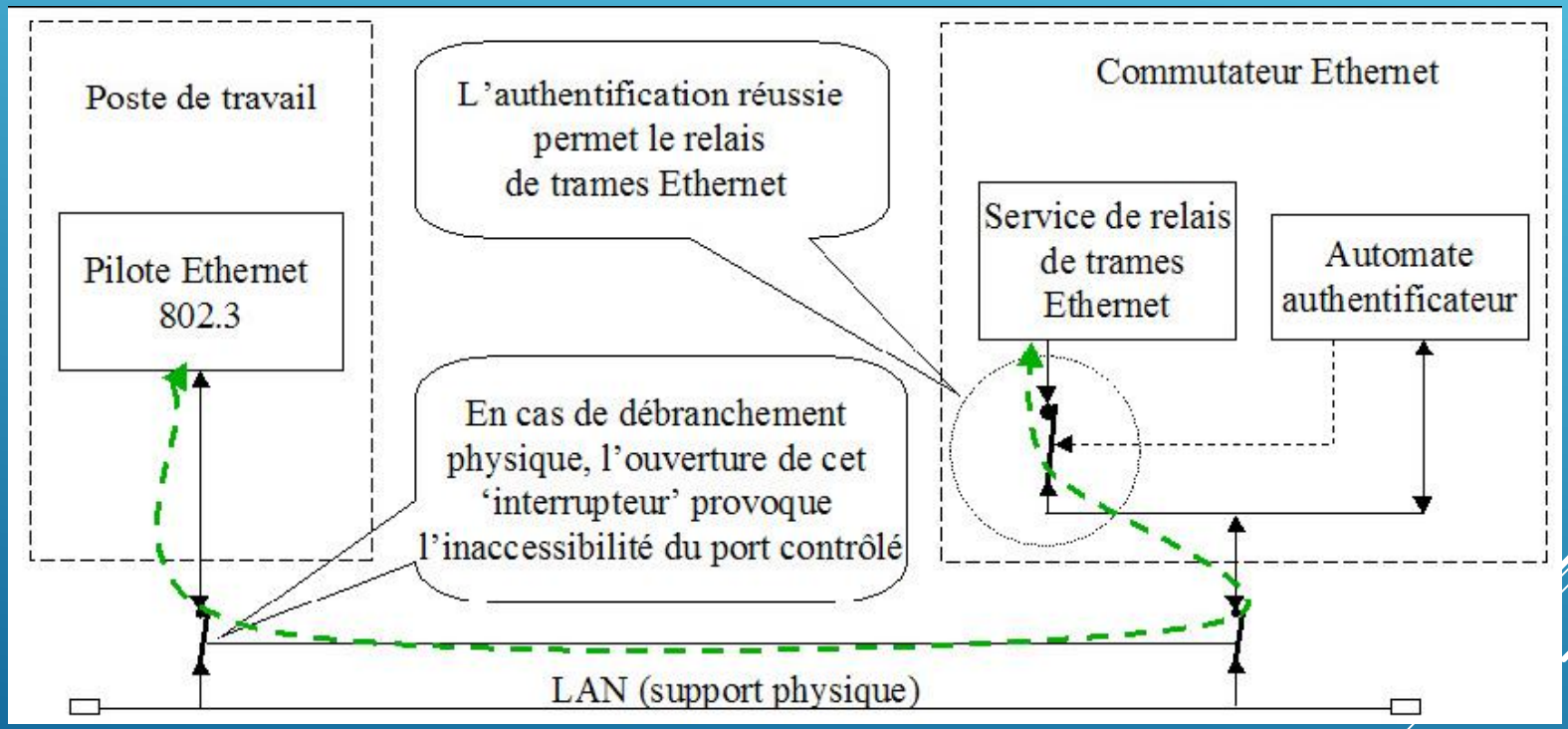
FONCTIONNEMENT

- **Circulation des paquets d'authentification**



FONCTIONNEMENT

- **trafic Ethernet après authentification**



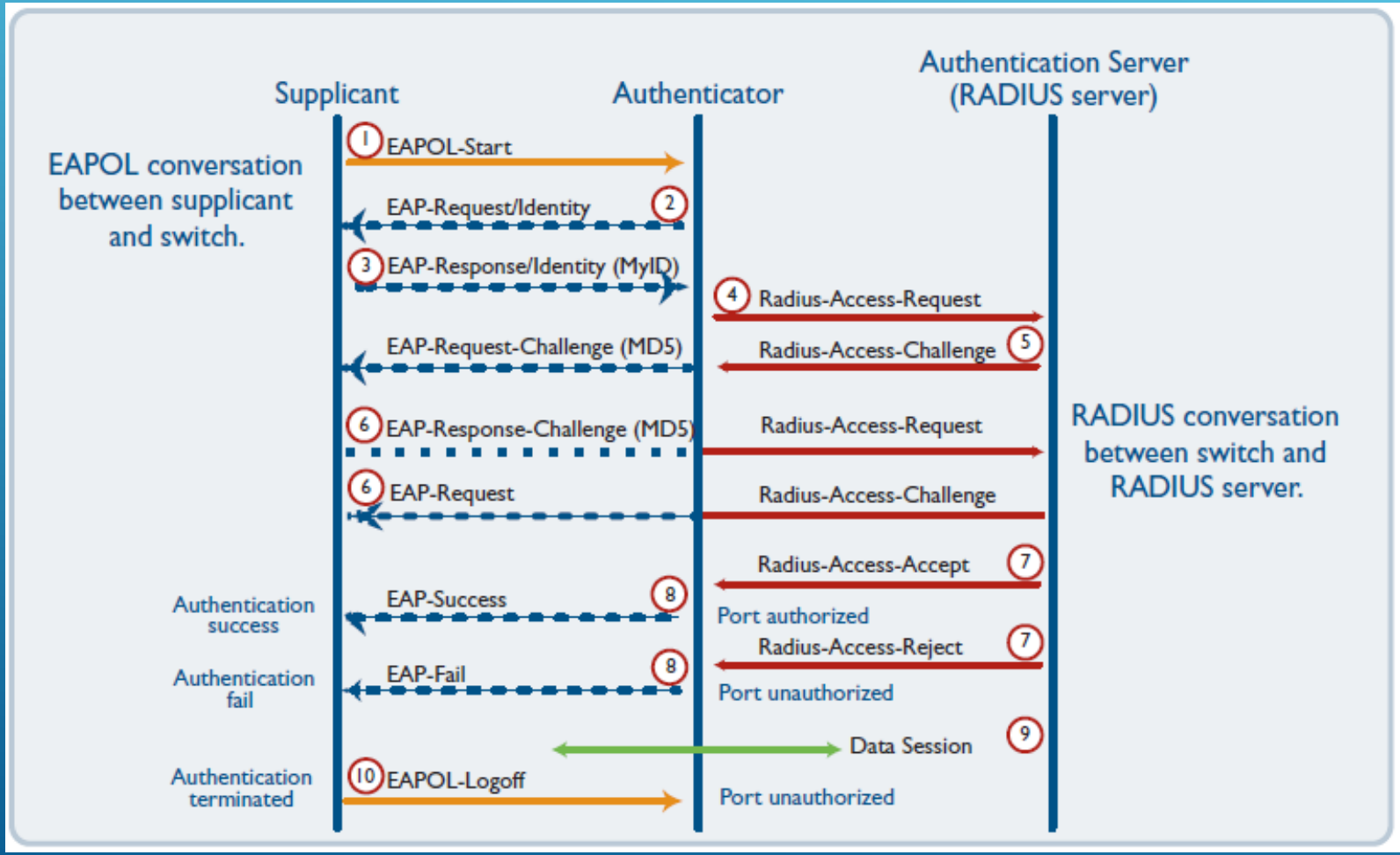
FONCTIONNEMENT

Exemple de session 802.1X/EAP

- **Avant la connexion du système à authentifier au port physique du PAE du système authentificateur, le port contrôlé de ce dernier est bloqué, et seul le port non contrôlé est accessible.**
- **Lorsque le système à authentifier se connecte au port physique du système authentificateur, il reçoit un paquet EAP l'invitant à s'authentifier. Sa réponse est reçue sur le port non contrôlé du système authentificateur, puis est retransmise au serveur d'authentification par ce dernier.**

FONCTIONNEMENT

- **Exemple: Diagramme de séquence d'une Session EAPoL**



LES FAIBLESSES DE 802.1X

- **La principale faiblesse de 802.1X vient de ce qu'il a été conçu au départ dans un contexte de connexion physique (type accès PPP sur RTC).**
- **Rien n'empêche en effet un utilisateur d'insérer un hub (transparent à 802.1X) et de faire bénéficier d'autres utilisateurs de l'ouverture du port Ethernet d'un commutateur.**
- **Les attaques par écoute et rejeu sont aussi possibles, ainsi que le vol de session. Les attaques sur 802.1X sont, de plus, facilitées dans le cas de l'Ethernet sans fil.**
- **attention, il faut que le 802.1x soit bien implémenté sur les différentes machines.**
- **Le 802.1x est maintenant intégré par défaut dans les différents systèmes d'exploitation.**

EVOLUTIONS

- La révision du standard 802.1X se fait par l'addendum 802.1aa, dont le dernier draft (numéro 5) a été publié en février 2003.
- Les principales modifications introduites concernent le non rejeu des échanges, l'authentification mutuelle, et la gestion des clés.
- L'authentification mutuelle est une amélioration importante, car elle permet de résoudre le cas où le client est lui-même un fournisseur de service réseau, et a besoin d'être sûr qu'il s'adresse bien à un port 802.1X de confiance.

MISE EN PLACE

- **Le Supplicant**
  - **Activation de 802.1x**
  - **Choix de la méthode EAP**
- **L'Authenticator**
  - **Activation du 802.1x sur les ports**
  - **Redirection vers l'Authentication Server**
  - **Règle de sécurité sur le port ou la borne**
- **L'Authentication Server**
  - **Création des profils**
  - **Mise en place des règles de sécurités sur les profils**
  - **Liens externes (LDAP, DHCP)**

CONCLUSION

- Adaptable aux réseaux câblés ou sans fil
- Sécurité en amont, pas de congestion totale du réseau
- Modularité selon la méthode EAP choisie
- Gestion dynamique de la configuration de l'équipement d'extrémité en fonction du compte utilisateur
- Possibilité de connexion avec annuaire LDAP

KERBEROS

- **Problème**

- **Composantes de Kerberos**
  - **Key Distribution Center (KDC) : Représente le tiers de confiance des autres entités**
  - **Client (demandeur de service)**
  - **Serveur (fournisseur de services)**

VUE GLOBALE DU FONCTIONNEMENT DE KERBEROS

- **Client s'authentifie au KDC!**
  - **Obtient un TGT (Ticket-Granting Ticket)**
- **Le client demande un ticket pour un service spécifique (en utilisant son TGT).**
  - **Obtient un Ticket de service**
- **Le client envoi le Ticket de service au Serveur**
  - **Le serveur valide le Ticket de Service**

REMARQUES IMPORTANTES SUR LES CLÉS

- **Dans les processus Kerberos, les clés ne sont jamais transmissent via le réseau.**
- **Ces clés sont utilisées pour crypter au niveau des différentes composantes.**
- **Étant capable de décrypter les données reçues, prouvent qu'on connait les données d'authentification (ID/Clé).**
- **Deux types de clés :**
  - **Clés long terme : TGS/Service/Client**
  - **Clés de Session : Service/TGS**

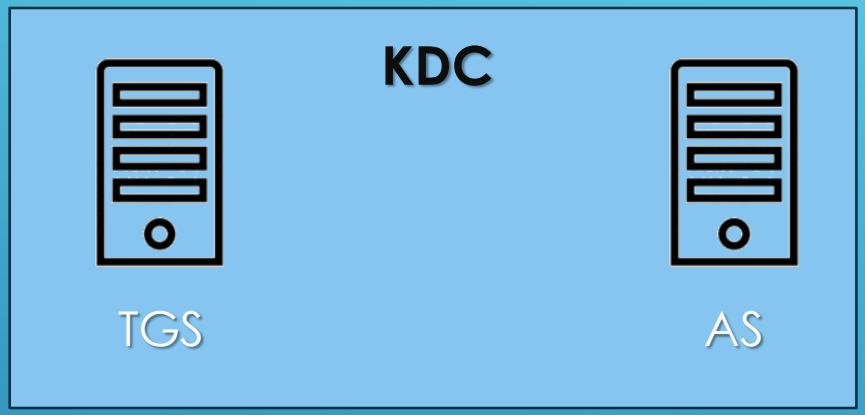
DEMANDE DE SERVICE COTÉ CLIENT

- **Le client doit identifier le service de manière unique**
- **Les identifiants sont spécifiés grâce au SPN (Service Principal Names)**
  - **Fournie des nomes identifiant une instance d'un services.**
  - **Plusieurs instance du même service ont des identifiants « noms » différents.**
  - **Chaque service peut avoir plusieurs SPN (s'il y a plusieurs noms que le client pourra utiliser pour l'authentification) .**
    - **Le SPN inclut le nome de l'ordinateur Hôts.**
- **Le SPN doit être enregistré avant son utilisation.**
- **Format du SPN**
  - **Windows « Service class »/« Hôte » : (Hote : est le nom DNS de l'hôte du service.**
  - **MIT kerberos :**
    - **User Principal Names : user@REALM**
    - **Service Principal Names : « Service class »/hostname@REALM**

PRÉREQUIS

- **KDC avec des utilisateurs et services enregistrés.**
- **Client capable d'accéder au KDC**
  - **S'authentifier (obtenir un TGT)**
  - **Demander l'accès à un service (obtenir un ST « Service Ticket » pour un SPN donnée.**
  - **Un Service capable de valider la ST.**

ARCHITECTURE



Serveur

Processus

Client

Utilisateur

MESSAGES KERBEROS

- **Demande d'authentification au service:**
  - **KRB_AS_REQ**
  - **Client ➔ Serveur**
  - **Utilise une clé long terme client.**
  - **Message partiellement crypté par le client**
    - **Authentificateur : Time Stamp (crypté)**
    - **UserID, @IP client, service SPN (en clair)**
  - **Le sucée du décryptage (par le AS) constitue une validation de l'identité du client.**

MESSAGES KERBEROS

- **Réponse d'authentification au service:**
  - **KRB_AS_REP**
  - **AS ➔ Client**
  - **Contient deux parties:**
    - **Clé de session TGS crypté par l'AS à l'aide de la clé du client. Ainsi décrypté par le client.**
    - **Le TGT qui inclue (ID Client, @IP Client, Validité du ticket et la clé de session du TGS) crypté par l'AS à l'aide de la clé du TGS. Ainsi décrypté par le TGS.**

- **Demande du Ticket-Granting Service:**
  - **KRB_TGS_REQ**
  - **Client ➔ TGS**
  - **Contient deux parties:**
    - **Authentificateur : Time Stamp (crypté par la clé de session du TGS)**
    - **Une copie du TGT (même que celui reçu par le client dan l'étape précédente).**

- **Réponse du Ticket-Granting Service:**
  - **KRB_TGS_REP**
  - **TGS ➔ Client**
  - **Contient deux parties:**
    - **Clé de session du service crypté a l'aide de la clé de session TGS. (décrypté par le client)**
    - **Le TS (Service Ticket) qui inclue (ID Client, @IP Client, Validité du ticket et la clé de session du Service) crypté par l'AS à l'aide de la clé du Service. Ainsi décrypté par le Serveur.**

- Demande d'authentification Client/serveur
  - KRB_AP_REQ
  - Client ➔ Serveur
  - Contient deux parties:
    - Authentificateur : Time Stamp (crypté avec la clé de session du service)
    - Une copie du ST (même que celui reçu par le client dan l'étape précédente).
  - Tout décrypté par le serveur

- **Réponse d'authentification Client/serveur (Optionnelle pour l'authentification mutuelle)**
  - **KRB_AP_REP**
  - **Serveur ➔ Client**
  - **Authentificateur : Time Stamp (crypté avec la clé de session du service)**