

Déploiement PKI

Enseignements du déploiement interne Microsoft

Cyril VOISIN
Chef de programme Sécurité
Microsoft France

Sommaire

- Réseau sans fil 802.1x
- Carte à puce pour accès RAS / VPN
(EAP-TLS, Radius IAS, Active Directory)
- Messagerie S/MIME (signature,
chiffrement)

Réseau sans fil 802.1x

Déploiement WLAN chez Microsoft

802.11b/802.1x chez Microsoft

- Situation actuelle
 - 3200 points d'accès déployés
 - 32000+ cartes WiFi depuis 1999
 - Les configurations standards ont le WiFi intégré
 - Ordinateurs portables, tablet PC
- Déployé largement sur 4 continents et 10 pays
 - Puget Sound – 72 batiments
 - Amériques (du sud et du nord) – 46 sites
 - EMEA – 42 sites
 - Extrême Orient – 23 sites
- 17 serveurs IAS Windows Server 2003 déployés (RADIUS)

802.11b/802.1x chez Microsoft

- Pourquoi avoir déployé le 802.11?
 - Décision au niveau exécutif en 1999
 - Supporte de nouveaux scénarios de mobilité
 - Gain de 1h30 de connectivité en moyenne sur le campus
 - 24% des employés utilisent le WLAN plus de 6 heures par jour
 - Gains de productivité
 - 30 à 90 minutes de gain de productivité par jour
 - Très bonne acceptation par les utilisateurs.
Ex : les participants aux projets pilotes ne voulaient pas rendre les matériels
 - Déploiements de postes plus rapides et plus économiques
 - ~\$500 par bureau câblé, ~\$180 par utilisateur Wireless (estimation interne – Campus)

802.11b/802.1x chez Microsoft

- Pourquoi avoir déployé le 802.1x ?
 - Utilisation d'une seule clé statique pour chaque client et points d'accès (PA)
 - Faiblesse de WEP / facilité des attaques
 - Technologies d'antennes au point
 - Le choix : arrêter le WiFi ou implémenter une sécurisation forte

Problèmes de sécurité liés au 802.11

- Wired Equivalent Privacy (WEP) : faible
 - Une clé WEP 128 bit peut être cassée en 2 heures avec des outils PC et une carte WiFi.
 - Les clés WEP ne sont pas changées dynamiquement et sont donc vulnérables aux attaques.
 - Une carte WiFi volée ou perdue peut donner LA clé (*B.O.R.E.*)
 - Comment apporter les clés WEP aux clients de façon sécurisée ?
- Filtrage d'adresse MAC : pas un moyen de sécurité
 - Montée en charge – doit être administrée et propagée à tous les Points d'Accès (PA). Les listes ont une taille limitée.
 - Pas de moyen d'associer une adresse MAC à un utilisateur
 - Carte volée, perdue et non déclarée ?
 - Spoofing d'adresses MAC (après écoute du trafic)

Solutions de sécurisation du WiFi

- Connectivité VPN
 - PPTP, L2TP, Tierce
 - Problèmes :
 - nécessite un logon RAS
 - le serveur VPN est un goulot d'étranglement
- IPSec
 - Solutions du marché
 - Problèmes :
 - Authentification niveau machine seulement
 - Gestion des certificats

Solutions de sécurisation du WiFi

- Authentification par mot de passe au niveau 2
 - Cisco LEAP, RSA/Secure ID
 - Inconvénient : cible pour les attaques de type dictionnaire
- Authentification par certificat au niveau 2 (PKI)
 - IEEE 802.1x EAP/TLS
 - Solution retenue en interne – déployée à l'été 2001

Problèmes liés au déploiement de 802.11/802.1x

- Nécessite des clients 802.1x
 - Windows XP en standard (PEAP via le SP1)
 - Windows 2000 depuis 11/2002
 - Windows NT4 Workstation, Windows 98 et Millennium : via des contrats de support Microsoft Premier et Alliance
 - Pocket PC : code fourni aux OEM en octobre 2002
- Outils clients nécessaires (obtention et installation des certificats)

Problèmes liés au déploiement de 802.11/802.1x

- Choix du matériel
 - pour les PA : pas de partie amovible, administration à distance sécurisée
 - pour les cartes réseau : compatibilité
- Timeout client DHCP (Windows XP sans SP1)
- Diagnostics des problèmes RF
 - Interférence : co-channel (recouvrement), PA intrus, ad hoc
 - Zones d'ombres RF

Problèmes liés au déploiement de 802.11/802.1x

- Contrôler/détecter les installation sauvages de point d'accès
- Diagnostic de problèmes 802.1x :
 - Ressources cross-organisationnelles requises (PKI, Radius, Active Directory, point d'accès, carte WiFi)
- Mise à jour distante des points d'accès
- Dimensionnement du serveur RADIUS :
 - Doit supporter bien plus d'authentifications qu'un serveur RAS
- Gestion de la révocation - Certificate Revocation Lists (CRL)

802.1x en pratique

- Utiliser EAP/TLS et les clés WEP 128 bits.
- Choisir un intervalle de renouvellement des clés WEP qui évite le craquage mais ne surcharge pas inutilement les serveurs
- Paramétrer les clients pour forcer l'authentification utilisateur et machine

`HKLM\SW\MS\EAPOL\Parameters\General\Global\AuthMode = 1`

802.1x en pratique

- Développer une méthode pour gérer les points d'accès indésirables
 - Développement ou solution du marché pour la détection
 - Procédure pour élimination
- Concernant les points d'accès
 - Paramétrer un mot de passe administrateur fort pour les points d'accès
 - Ils doivent supporter 802.1x EAP/TLS, WEP 128 bits
- Utiliser plusieurs canaux de séparation pour minimiser les échos
 - Exemple : Canaux 1, 6 et 11 (Europe jusqu'à 13 possible mais non utilisé chez Microsoft)

802.1x en pratique : les clients

- Cartes WiFi :
 - Interopérabilité avec les points d'accès (dont les WLAN personnels)
 - Support WEP 128 bits
 - Disponibilité d'un pilote certifié pour la plateforme visée
- Logiciel :
 - Développer une méthode automatisée pour fournir les certificats
 - Dans un futur proche : WZCTOOL de Windows Server 2003 (Wireless Zero Configuration wizard)

802.1x en pratique : Active Directory

- Utiliser les groupes globaux/universels pour organiser les comptes *wireless*
- Contrôler les permissions d'accès au travers de *Remote Access Policy*
- Mettre en oeuvre l'*auto-enrollment* sur les comptes machines, en configurant la stratégie de groupe « *Automatic Certificate Request Settings* »

802.1x en pratique :

Serveurs Radius et points d'accès

- Sécuriser le trafic entre points d'accès et serveurs RADIUS via IPSec
- Utiliser les mots de passe forts pour les secrets partagés RADIUS
- Utiliser autant de secrets partagés RADIUS que possible
- Utiliser des proxies Radius quand en multi-domaine
 - Permet de relayer les authentications sur le serveur RADIUS du domaine d'appartenance
 - Gain en évolutivité et administration
- Ne pas prévoir plus de 20-50 connexions clients simultanées par points d'accès,
 - Partage de bande passante par point d'accès !

802.1x en pratique :

Serveurs Radius et points d'accès

- Pour des environnements à haute densité de clients, utiliser plus de points d'accès, à puissance de transmission réduite
- Mise à jour des firmwares des points d'accès existants
- Les fréquences autorisées varient d'un pays à l'autre
- Attention à respecter les règles de sécurité des biens et des personnes en installant les points d'accès (prévention anti-incendie, utilisation d'une alimentation centralisée basse tension sauvegardée)
- Câble universel :
alimentation + réseau, personnalisation : accès console

Carte à puce pour l'accès à distance

Authentification à 2 facteurs pour le RAS chez Microsoft

Aperçu de la solution

- Amélioration de la sécurité (carte + PIN)
- Flexibilité (stockage sécurisé)
- Simplicité
- Capitalisation sur une infrastructure déjà existante : Windows 2000, Active Directory, Certificate Services



"The use of Smart Cards will significantly increase the security of our corporate network by improving our ability to authenticate each employee and business partner as they remotely connect to Microsoft."

Greg Wood, General Manager, Corporate Security, Microsoft Corporation

Le RAS chez Microsoft

- Le groupe informatique interne chez Microsoft :
OTG – Operations and Technology Group
 - En charge des réseaux internes, des télécommunications, des applications métier, des serveurs d'infrastructure
 - En particulier, gère les risques sécurité des accès distants (RAS, Remote Access Services)
- Quelques chiffres
 - Environ 58000 employés et sous-traitants utilisent les accès RAS
 - 400 sites dans le monde, 175 points d'accès (directement par modem ou carte RNIS, ou bien par connexion à un FAI puis VPN, PPTP ou L2TP)
 - Environ 250 000 connexions par semaine

Le RAS chez Microsoft

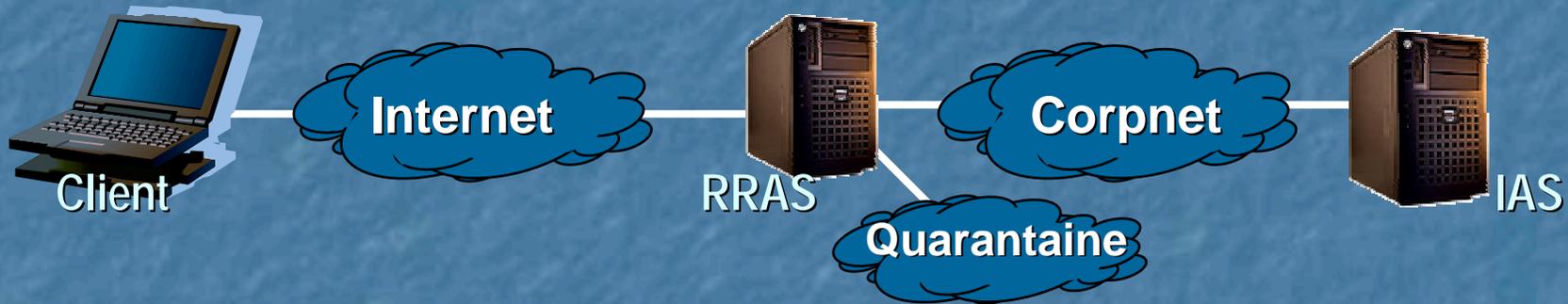
- La problématique de l'authentification pour le RAS
 - Validation du nom et du mot de passe associé (insuffisant)
 - Authentification à deux niveaux (correct)
 - Quelque chose que l'on a (la carte à puce) et
 - quelque chose que l'on sait (le code d'accès - Personal Identification Number - PIN)
 - Volonté de pallier certaines vulnérabilités sur les ordinateurs non gérés (à la maison en particulier)
 - Virus, chevaux de Troie, vers
 - Connexion permanente (ADSL) à l'Internet qui augmente les menaces
- La carte à puce a été choisie par rapport à d'autres technologies alternatives en raison de son coût, de sa fiabilité, de ses fonctionnalités et de sa mobilité

Menaces / contre mesures

- **Personne mal intentionnée (hacker)**
 - Authentification à 2 facteurs : Carte à puce + PIN
 - Stratégie de mots de passe forts
- **Logiciel malveillant**
 - Vérification de la configuration minimum requise :
 - *Connection Manager*
 - Antivirus
 - Windows XP avec parefeu activé
 - *RAS Quarantine*

Infrastructure plus sécurisable

Mise en quarantaine



Configuration client
non contrôlée :

- Version d'OS supportée ?
- Routage ?
- Firewall ?
- Signature A/V à jour ?
- Correctifs appliqués ?

Concept :

- Isoler
- Tester
- Configurer
- Autoriser / bloquer l'accès

La carte à puce chez Microsoft

- Difficile à suborner
 - Il faut
 - Un lecteur de carte à puce
 - Un PIN
- Tire parti des technologies présentes en standard au sein des serveurs Windows 2000 Server / Windows Server 2003
 - Fonctionnalité des services de certificats
 - Sécurité d'une *Public Key Infrastructure* (PKI)
 - *Cryptographic Service Provider* (CSP)
 - Sécurité *Extensible Authentication Protocol/Transport Layer* (EAP/TLS)

La carte à puce chez Microsoft

- Fonctions utilisateur disponibles actuellement
 - Visualisation du contenu de la carte, reset du PIN, ajout de données personnelles
- Fonctions utilisateur disponibles dans le futur
 - Ajout de nouveaux certificats pour différentes applications
- Remplacement des badges d'accès aux bâtiments (avec photos) pour tous les employés de Microsoft (aux USA – en Europe, 2 badges)
 - Ceux-ci comprennent maintenant un processeur de chiffrement embarqué disposant de 32 Ko

Architecture

- Besoins sur le poste client
 - Windows XP Professionnel
 - Lecteur de carte à puce avec le connecteur approprié
 - Application antivirus
 - Autres logiciels additionnels
 - Différents outils OEM pour la carte à puce
 - Version pré-configurée du Connection Manager qui standardise toutes les options de configuration de la carte à puce lors de l'installation
 - Développements personnalisés
 - Extension des scripts du Connection Manager pour vérifier toute les éléments de sécurité du poste client en connexion RAS. Si cette vérification de la configuration minimale du poste client échoue, mise en quarantaine (RAS Quarantine Service de Windows Server 2003)

Déploiement

- Acquisition d'un processeur de chiffrement 32 Ko et intégration dans des cartes à puce au format standard (RFID)
- Formation d'un card management team centralisé
 - Personnalisation, émission et gestion de la distribution, support utilisateur de deuxième niveau
- Les Smart Card Security Officers distribuent les cartes
 - Vérification de l'identité
 - Échange des anciens badges d'accès aux bâtiments et remplacement par les nouveaux badges carte à puce
 - L'utilisateur doit changer son PIN initial avant de se connecter à distance sur le réseau
 - PIN obligatoirement alphanumérique, 5 à 15 caractères

Déploiement

- Utilisation de l'infrastructure de PKI pour créer les certificats de logon stockés dans les cartes à puce et l'annuaire Active Directory, délivrés à travers les services de certificats de Windows Server
- Mise en place d'une solution de délégation pour la distribution régionale et les responsabilités administratives afin de diminuer les coûts
 - Autorisation de distribuer des cartes de remplacement après avoir obtenu l'accord de l'équipe sécurité de Redmond
 - Fourniture de cartes à puce pré-configurées dont les numéros de série sont tracés soigneusement

Les défis

- Utilisateurs mobiles
 - Les utilisateurs de PDA ne peuvent obtenir un accès RAS (pas de support du protocole EAP/TLS pour l'instant)
- RNIS
 - Le groupement de canaux RNIS n'est pas supporté (réduction des performances réseau)
- Sélection d'un produit matériel
 - Les modèles de cartes à puce évoluent rapidement ; le déploiement à l'échelle de Microsoft ne permet pas une standardisation sur un seul modèle

Les défis

- Machines à la maison
 - Les utilisateurs à la maison qui ont des machines Macintosh, UNIX et Linux ne peuvent obtenir un accès RAS (pas de support pour le protocole EAP/TLS)
 - Remarque : les machines à la maison qui ne peuvent pas mettre en place une solution carte à puce pour des raisons logicielles (Windows XP) ou matérielles (USB) peuvent accéder à leurs messageries, calendriers, contacts et aux dossiers publics via le Web en utilisant Outlook Web Access (via HTTPS). Utilisé par 30000 employés chaque mois.

Le futur

- Meilleure gestion des comptes avec des privilèges élevés
 - Utiliser le paramétrage dans Windows qui requiert l'utilisation d'une carte à puce pour l'utilisation d'un compte hautement privilégié (but : minimiser les éventuelles compromissions et améliorer la traçabilité)
- Signatures numériques (messagerie)
- Extension du support applicatifs
 - Signature des dotations en stock options, sécurisation des données financières et DRH, signature du code source, etc.

Autres leçons apprises

- Comprendre les possibilités de la carte à puce
- Anticiper les évolutions des technologies sur les 12-24 prochains mois
- Prévoir un moyen secondaire d'accès sécurisé
- Outils d'administration des cartes à puce pas encore matures (augmentation de l'administration requise)

Autres leçons apprises

- S'assurer que les équipes sont correctement formées sur les technologies de PKI
- Ce n'est pas une solution permettant de couvrir 100 % de la population de utilisateurs
 - Comprendre les impacts de l'utilisation de postes client non standards
- Pénalisation en termes de performance lors du logon initial : ajout d'environ 30 secondes au processus de logon
 - L'augmentation de la sécurité du réseau justifie pleinement cette pénalisation

Messagerie sécurisée S/MIME

Signature et confidentialité des méls chez Microsoft

Composants

- Avant
 - Outlook 2002
 - KMS / Exchange 2000 / Active Directory
- Maintenant
 - Outlook 2003 beta 2
 - Exchange 2003 beta / Windows Server 2003
- Usages : signature (authentification, intégrité), chiffrement (confidentialité)
- Certificats :
 - du stockage logiciel... (maintenant)
 - vers les cartes à puce (avenir proche)

En résumé

- Microsoft a cherché à mettre en œuvre en interne une solution sécurisée permettant l'accès au réseau quel que soit l'endroit d'où travaillent les Microsoftees.
- La mise en œuvre d'une authentification à deux niveaux pour le RAS et du 802.1x en font partie
- En tout état de cause, il faut planifier attentivement une telle mise en oeuvre

Microsoft®

Annexes

Plus d'informations

- <http://www.microsoft.com/technet/itshowcase>
- <http://www.microsoft.com/wifi>
- <http://www.microsoft.com/wireless>
- <http://www.microsoft.com/hwdev/tech/network/wireless>
- <http://www.ieee.org>
- <http://standards.ieee.org/wireless/>
- <http://www.ieee802.org/1/pages/802.1x.html>
- <http://www.wi-fi.org>
- Il est possible de trouver des informations additionnelles sur les technologies de cartes à puce et de mise en place d'infrastructure de PKI en
 - <http://msdn.microsoft.com/library/?url=/library/en-us/dnscard/html/smartcardcspcook.asp>
 - http://www.microsoft.com/seminar/includes/seminar.asp?url=/Seminar/en/Windows/20000727_WIN2K_PublicKey1/Portal.xml
 - http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/deploy/dgch_pki_ODBG.asp

Glossaire

- IAS: Internet Authentication Server
- EAP: Extensible Authentication Protocol
- PEAP : Protected Extensible Authentication Protocol
- TLS: Transport Layer Security
- WiFi : Wireless Fidelity (802.11)
- CRL: Certificate Revocation Lists
- WEP : Wired Equivalent Privacy
- TKIP : Temporal Key Integrity Protocol
- AES: Advanced Encryption Standard
- RADIUS : Remote Authentication Dial-In User Service
- GP : Group Policy
- WLAN : Wireless Local Area Network
- VPN : Virtual Private Network
- PKI: Public Key Infrastructure
- PPTP : Point to Point Tunneling Protocol
- L2TP: Layer Two Tunneling Protocol
- IEEE: Institute of Electrical and Electronics Engineers

Processus d'authentification 802.1x

1. Client forms an 802.11b association with an access point.
2. The access point sends the client an EAP "identity request".
3. The client responds by sending its EAP "identity" to the access point. The identity consists of the domain username or machinename and domain, e.g. `alias@FOO.domain.microsoft.com`.
4. The access point forwards this request to the RADIUS server over its uncontrolled port.
5. After receiving the client's EAP "identity", the RADIUS server (1) requests a certificate that is associated with the identity it just received and (2) sends the server certificate through the AP to the client.
6. The client validates the server certificate it receives and sends its own domain certificate back to the RADIUS server via the access point. NOTE: The client will previously have needed to obtain the certificate over an ethernet connection to the network or some other means of connecting that does not use 802.1X.

Processus d'authentification 802.1x

8. The RADIUS Server checks with the Active Directory Domain Controller to ensure that the domain user account information in the "identity" packet is indeed associated with the domain user certificate received from the client. If not, the RADIUS server sends an authentication failure message to the access point.
9. Upon successful authentication, the RADIUS server sends a success message to the access point along with a usable WEP key for the session.
10. The access point forwards the WEP Key to the client. This WEP key is used for the current session in which the client is associated with the Access Point. NOTE: A subsequent WEP key is provided by the AP to the client if the client roams to a new AP or the WEP refresh interval passes.
11. The access point opens the controlled port to give the client access to corpnet resources.
12. The client implements the WEP key to encrypt its 802.11b link layer wireless connection to the access point and starts DHCP to obtain a corpnet IP address through the AP's controlled port.
13. After successfully receiving an IP address from the DHCP server, the client then completes a normal logon to the domain and can begin using the network.

IEEE 802.11 Task Groups (TG)

- Different 802.11 PHYs
 - 802.11 – 2Mbps DS or FH
 - 802.11b – 11Mbps DS
 - 802.11g - 22Mbps OFDM
 - 802.11a – 54 Mbps OFDM
- 802.11d – World mode
- 802.11e – 802.11 QoS based on 802.1p
- 802.11f – inter AP protocol
- 802.11h – dynamic power and freq control
- 802.11i - Advanced Encryption Standard (AES) plus .1x style authentication

Avenir de la sécurité WLAN

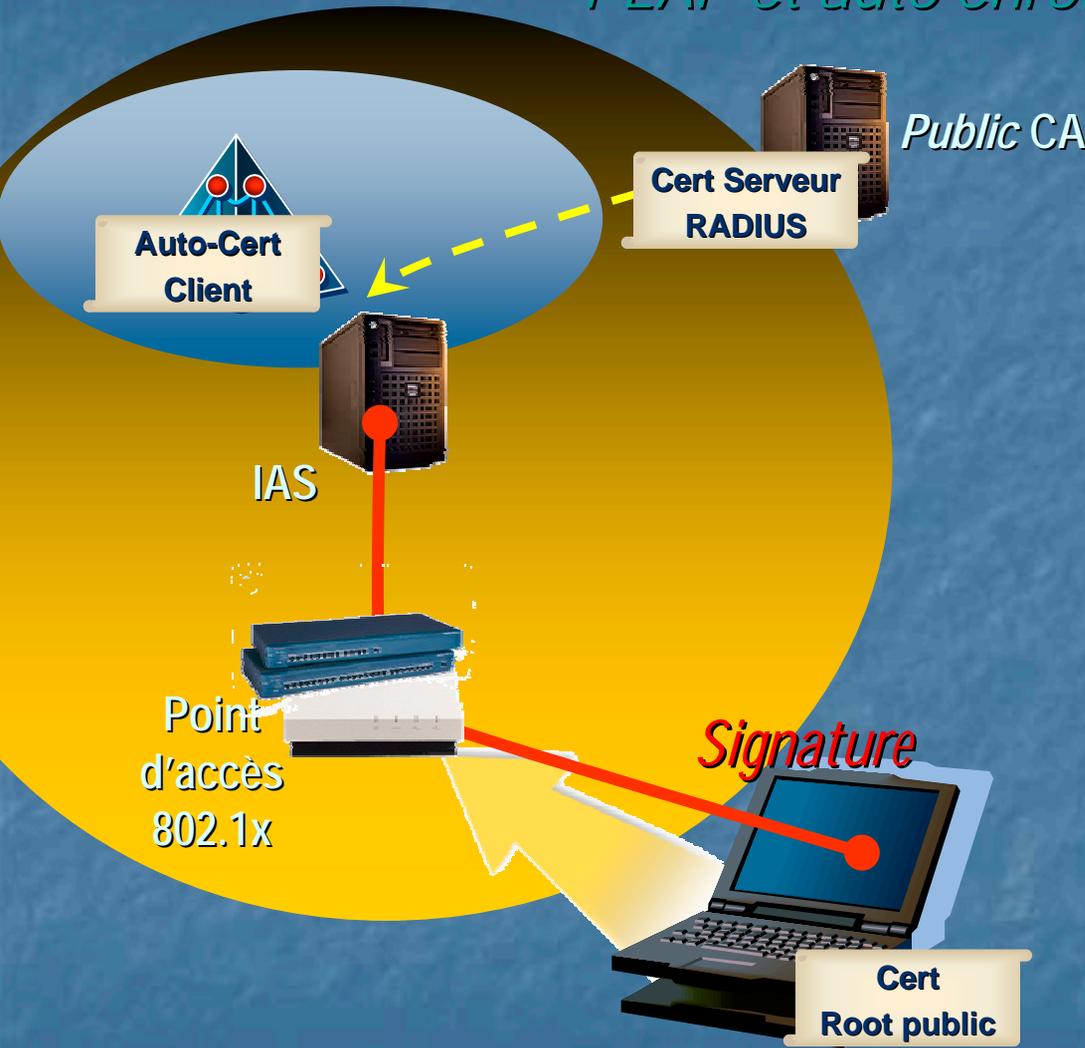
- 802.11a - 5.0 GHz
 - OFDM – Résistance aux interférences
 - Haut débit : 54 Mb/s
- 802.11i – Remplacement de WEP pour un chiffrement par paquet :
 - Temporal Key Integrity Protocol (TKIP) – Par mise à jour du Firmware
 - Advanced Encryption Standard (AES) – Nécessite la mise à jour du chipset
- Protected EAP (PEAP)
 - Négociations chiffrées de l'authentification
 - TLS ou MSCHAPV2 peuvent être utilisés
 - PEAP/TLS plus sécurisé que EAP/TLS
- Le 31/3/2003 : mise à disposition de WPA (WiFi Protected Access (plus sécurisé que WEP; ouvre la voie vers 802.11i)

Mise en oeuvre

- Stratégie de mots de passe forts
 - Accès au stockage des mots de passe restreint et audité
 - Changement tous les 70 jours
 - Interdiction du paramétrage « ce mot de passe n'expire jamais »
 - Aucune transmission de mot de passe en clair
 - Pas de mise en cache de mots de passe
 - Interdiction d'utilisation de mots de passe dans des batches
 - Les comptes homonymes doivent avoir des mots de passe significativement différents dans les domaines où ils sont présents
 - Doit suivre les règles de complexité

Infrastructure plus sécurisable

PEAP et auto enrôlement



1. Le poste client (pas dans le domaine) a le certificat racine de la CA *public*
2. Le serveur RADIUS obtient un certificat de la CA *public*
3. Tentative de connexion
4. Vérification du certificat du serveur RADIUS par le client
5. Canal EAP sécurisé en utilisant le certificat du serveur RADIUS
6. Authentification du client en utilisant le mot de passe AD
7. Le client joint le domaine et s'auto enrôle
8. Ensuite, le certificat sera utilisé pour l'authentification