
# Référentiel sur l'usage du Wi-Fi en établissement et école
# Cadre technique

**Version 1.0 Mai 2015**

# Documents de référence

## Documents Généraux

| Nom | Version | Date | Commentaires |
|---|---|---|---|
| *[Réf. 1] - note technique N° DAT-NT-005/ANSSI/SDE/NP du 30 mars 2013 précisant les « recommandations techniques de sécurité relatives au réseau Wi-Fi ». ANSSI* | | | |
| *[Réf.2] Note juridique « le Wi-Fi dans les établissements scolaires » du 2 avril 2014. Cabinet Alain Bensoussan Avocats* | | *02/04/2014* | |
| *[Réf. 3] Note technique précisant les « différents cas d'usage d'IPsec Accès distants en nomadisme ». ANSSI* | | | |
| *[Réf. 4] Circulaire N°2004-035 du 18 février 2004 - Circulaire Darcos* | | *18/02/2004* | |
| *[Réf. 5] Note technique : Recommandations de sécurité relatives aux réseaux Wi-Fi* | *1.0* | *30/03/2013* | |
| *[Réf. 6] MEN. Guide d'élaboration d'une charte d'usage des TIC. url : http://eduscol.education.fr/cid57095/guide-elaboration-des-chartes-usage.html.* | | | |
| | | | |

| **DIFFUSION** | | |
|---|---|---|
| ***Version*** | ***Pour validation*** | ***Validé le*** |
| *1.0* | | *29/05/2015* |
| | | |

# SOMMAIRE

# Table des figures

# 1 Description du cadre technique

Dans cette partie technique plusieurs points importants seront abordés, à commencer par une étude de capacité en termes de débit. En effet, la mise en place d'une infrastructure Wi-Fi entraine généralement une augmentation du nombre d'accès à Internet. Ainsi, la bande passante disponible en sortie d'établissement ou d'école se retrouve partagée entre les technologies filaires et sans fil.

La problématique des débits s'avère primordiale avant de pouvoir lancer la mise en œuvre d'une telle infrastructure.

Le processus proposé pour la mise en place technique d'une infrastructure Wi-Fi est décrit sur le schéma suivant.


Tout d'abord, une étude capacité doit être lancée afin d'évaluer les besoins applicatifs par rapport à l'infrastructure existante.

Suite à l'étude de capacité, une étude d'implantation sera conduite en tenant compte des besoins et de plusieurs aspects notamment juridique et technique.

Des résultats de cette étude d'implantation, découleront l'installation des équipements ainsi que le paramétrage associé.

Enfin, cette partie technique présentera les solutions permettant de sécuriser les accès Wi-Fi en fonction des conclusions de la partie juridique et des technologies existant à ce jour.

**CE QU'IL FAUT RETENIR**

- **La contrainte technique majeure conditionnant la mise en place d'une infrastructure Wi-Fi se situe au niveau du débit disponible en sortie d'établissement ou d'école.**
- **L'étude d'implantation des équipements doit impérativement tenir compte des contraintes juridiques et techniques.**

# 2 Etude de capacité

La problématique des débits disponibles et nécessaires est à prendre en compte dans toute mise en place d'une infrastructure réseau, qu'il s'agisse ou non de Wi-Fi.

L'objectif d'une étude de capacité sera d'évaluer la bande passante Wi-Fi nécessaire. Il s'agira de déterminer le nombre d'utilisateurs en fonction de leur répartition géographique pour savoir si l'architecture Wi-Fi prévue supportera les débits induits.

En d'autres termes, il s'agira de définir la bande passante nécessaire et suffisante d'un support de transmission susceptible de supporter un nombre déterminé x d'utilisateurs tout en leur assurant une qualité de service correcte. Pour répondre à ce besoin, l'étude doit apporter des réponses sur les points suivants :

- Obtention des informations relatives à la bande passante.
- Détermination d'une méthode de calcul permettant d'évaluer le pourcentage de la bande passante utilisé par un utilisateur
- Définition des besoins quantitatifs d'un utilisateur pour lui apporter une qualité de navigation Web définie comme acceptable (définition des critères mis en œuvre)

Par ailleurs, les débits maximum disponibles en sortie d'établissement ou d'école, ainsi que sur les portions de réseau interne, ainsi que les flux par segment de réseau sont également des paramètres à prendre en compte. Disposer d'une vision globale permettra ainsi de déterminer quels sont les goulots d'étranglement et leurs possibilités d'évolution à court et moyen terme. Il convient de noter que cette observation ne se limite pas au Wi-Fi.

## 2.1 Obtention des informations relatives à la bande passante

Il s'agit dans un premier temps d'identifier les flux les plus consommateurs de bande passante.

Les flux HTTP générés par les serveurs proxy constituent souvent la consommation essentielle de la bande passante pour des accès Internet.

Les informations dans les logs de ces serveurs concernent des volumes transférés (taille de fichiers transférés html, jpeg, pdf, etc.). Les informations relatives à la bande passante ne sont pas directement accessibles à partir de ces logs. Les équipements qui permettront de recueillir les informations sont accessibles sur des équipements de type Firewalls ou routeurs.

## 2.2 Evaluation de la bande passante utilisée par un utilisateur

L'évaluation de la bande passante ne permet pas d'obtenir une valeur exacte. En effet, il ne pourra s'agir que de valeurs moyennes basées sur des utilisations a posteriori.

Lors de l'estimation du trafic réseau nécessaire, de nombreuses variables doivent être prises en compte parmi lesquelles :

- Le nombre de terminaux clients utilisés simultanément (pc, tablette, smartphones, etc.).
- Le type d'applications exécutées par chaque utilisateur.
- Les performances des navigateurs Internet.
- La capacité des connexions réseau et des segments réseau associés.

Des outils existent et permettent d'évaluer la bande passante utilisée et sont basés sur différentes approches. Certains utilisent une approche intrusive et d'autre une approche passive.

Cette évaluation sera réalisée en fonction des usages qui auront été répertoriés.

Au niveau des matériels utilisés, l'estimation de la capacité d'un point d'accès est réalisée en fonction du nombre d'usagers et de la répartition de ces usagers.

L'évaluation de bande passante permet de s'assurer qu'en fonction des débits disponibles sur les infrastructures filaires éventuelles et en sortie d'établissement ou d'école, l'accès par le Wi-Fi ne constituera pas un goulot d'étranglement et que l'usage des services numériques pourra se faire dans de bonnes conditions.

A titre d'appréciation, il est généralement admis qu'une page web mettant plus de 3 secondes pour s'afficher est considérée comme lente.

**CE QU'IL FAUT RETENIR**

- **L'étude de capacité permet d'évaluer les besoins en termes de bande passante en fonction des usages envisagés. Elle permet d'orienter la décision d'installer une infrastructure Wi-Fi et les choix techniques subséquents.**

# 3 Etude d'implantation

## 3.1 Présentation

Cette étape est préalable au déploiement de toute infrastructure Wi-Fi, elle permet d'évaluer la faisabilité du projet en fonction de l'architecture des bâtiments de la zone à couvrir, des possibles obstacles et autres éléments pouvant créer des interférences.

L'objectif de cette étude est donc de définir l'emplacement le plus adéquat des bornes tout en tenant compte des contraintes techniques et juridiques.

**Besoin :** Déployer un *réseau sans fil* pour des applications pédagogiques ou pour des utilisateurs externes. Vérifier que la couverture radio répondra à tous les besoins de mobilité avec un PC portable, une tablette PC, un smartphone …


## 3.2 Déroulement général d'une étude d'implantation

L'étude de couverture est réalisée grâce à des outils de planification dont le but est de calculer le nombre de points Wi-Fi à mettre en place en fonction de paramètres tels que :

- éléments d'architecture :
  - la taille des murs, leur composition (briques, chaux, BA13, etc.)
  - la configuration du bâtiment
  - la présence d'éléments perturbateurs (cage d'ascenseur, installations électriques, etc.)
- aspects juridiques
  - responsabilité du chef d'établissement / directeur d'école
  - respect des normes en matière de lieux recevant du jeune public

Une fois ce premier travail réalisé, des mesures de contrôle sur site sont généralement effectuées, afin de s'assurer de la bonne cohérence de la planification.

L'étude de couverture se poursuit par l'analyse de spectre, qui vise à détecter d'éventuelles perturbations électromagnétiques susceptibles d'altérer la qualité des transmissions radio. Cette analyse permet de déterminer les canaux d'émission de chaque point d'accès Wi-Fi.

La dernière étape de l'étude de couverture concerne les câblages et l'implantation des équipements et des points d'accès Wi-Fi. Le plan de câblage existant est étudié, et complété si nécessaire (cheminement, pose de goulottes…), puis l'emplacement des baies de brassage est déterminé et, enfin, le type d'équipement en fonction de l'environnement (température, humidité …) est sélectionné.

Enfin, à l'issue de cet audit, un rapport technique contenant l'étude de couverture et un planning listant l'ensemble des prérequis techniques à réaliser avant l'installation du réseau sans fil (pose d'alimentations électriques, ouverture de lignes analogiques etc.) est fourni.

**CE QU'IL FAUT RETENIR**

- **L'étude de couverture a pour but de déterminer avec précision le type d'équipement Wi-Fi à mettre en place dans un établissement ou une école. Elle permet de répondre aux questions relatives à la mise en place d'une infrastructure Wi-Fi : faisabilité du projet, budget, emplacement et nombre d'équipements actifs, passages de câbles, contraintes techniques, technologiques et juridiques.**
- **Elle est préalable à toute installation d'infrastructure Wi-Fi.**

# 4 Installation / Paramétrage

## 4.1 Présentation de la technologie

Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer entre eux grâce à des signaux radioélectriques.

La réglementation est assurée en France par l'ARCEP (Autorité de Régulation des Communications Electroniques et de la Poste, www.arcep.fr -ex ART-) qui fixe les conditions d'utilisation sur le territoire français des réseaux radio. Dans ce document nous nous intéressons à la technologie Wi-Fi.

Le Wi-Fi est une technologie de transmission d'information sans fil, standardisée par l'IEEE (Institute of Electrical and Electronics Engineers) sous la norme 802.11 (*ISO/IEC 8802-11*). Il s'agit d'une norme internationale.

Les échanges en Wi-Fi sont basés sur des ondes **radioélectriques** sur les bandes de fréquences 2,4 GHz (de 2,4 à 2,483Ghz) et 5 GHz (de 5,150 à 5,725 GHz).

Il s'agit de bandes libres, qui ne nécessitent pas d'autorisation de la part d'un organisme de réglementation. Toutefois, tous les réseaux Wi-Fi doivent respecter les conditions techniques d'utilisation des fréquences des bandes 2,4 GHz et 5 GHz, notamment les limites de puissance d'émission (PIRE[1]) définies par l'Autorité de régulation des communications électroniques et des postes (ARCEP). Ces règles de limitation de puissance ont pour objet de permettre la coexistence des différents réseaux radioélectriques de faible puissance.

Le tableau ci-après présente un récapitulatif des différentes normes ainsi que les caractéristiques associées.

| Norme | Description |
|---|---|
| 802.11a | La norme 802.11a permet d'obtenir un haut débit (**dans un rayon de 10 mètres : 54 Mbit/s théoriques, 27 Mbit/s réels**). Elle utilise la bande de fréquences des **5 GHz** |
| 802.11b | La norme 802.11b propose un débit théorique de **11 Mbit/s (6 Mbit/s réels) avec une portée pouvant aller jusqu'à 300 mètres (en théorie)** dans un environnement dégagé. La plage de fréquences utilisée est la bande des **2,4 GHz** |
| 802.11g | La norme 802.11g offre un haut débit (**54 Mbit/s théoriques, 25 Mbit/s réels**) sur la bande de fréquences des **2,4 GHz**. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. |
| 802.11i | La norme 802.11i (WPA2) a pour but de fournir une solution de sécurisation augmentée des réseaux Wi-Fi (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les standards 802.11a, 802.11b et 802.11g. |

1 La PIRE est la puissance isotrope rayonnée équivalente d'une antenne. Exprimée en Watt, elle est égale au produit de la puissance fournie à l'antenne d'émission par le gain de l'antenne

| Norme | Description |
|---|---|
| 802.11n | La norme 802.11n est disponible depuis 2009. Le débit théorique atteint les **300 Mbit/s (débit réel de 100 Mbit/s dans un rayon de 100 mètres)** grâce aux technologies MIMO (Multiple-Input Multiple-Output) et OFDM (Orthogonal Frequency Division Multiplexing).<br>Le 802.11n a été conçu pour pouvoir utiliser les fréquences **2,4 GHz ou 5 GHz**. |
| 802.11ac | IEEE 802.11ac est un standard de transmission sans fil dans la bande des 5 GHz (5,4GHz) uniquement. Le débit théorique atteint les **450Mbps** avec la possibilité d'agréger des canaux par clients pour une augmentation du débit. Cette norme devra assurer la compatibilité avec les versions 802.11a et 802.11n mais pas avec les versions 802.11b et 802.11g. |

Actuellement, les normes les plus utilisées sont les 802.11b et 802.11g. Dans le cadre de la mise en place de cette technologie au sein du ministère de l'éducation nationale, **il conviendra d'utiliser des terminaux compatibles avec les normes 802.11g ou 802.11n.**

La portée d'un réseau Wi-Fi dépend de la puissance d'émission. Elle est généralement limitée à quelques centaines de mètres.

## 4.2 Bonnes pratiques en termes de paramétrage et d'installation

Cette section reprend les éléments de la note technique : « Recommandations de sécurité relatives aux réseaux Wi-Fi » de l'ANSSI parue le 30/03/13.

L'ANSSI estime qu'il est primordial d'appliquer une liste de 23 recommandations afin de conserver la maîtrise et le bon usage des réseaux Wi-Fi. Cependant, nous retiendrons uniquement celles qui sont en rapport avec notre sujet c'est-à-dire le Wi-Fi dans le cadre d'établissements scolaires ou d'écoles.

Lorsque les points d'accès, les terminaux et plus généralement les systèmes d'information utilisés le permettent, ces recommandations doivent être imposées techniquement. Cela concerne notamment les aspects d'authentification, de protection cryptographique et de mise à jour des terminaux.

**Sur tout type de terminaux, personnels ou professionnels :**

| | |
|---|---|
| R1 | N'activer l'interface Wi-Fi que lorsqu'elle celle-ci doit être utilisée. |

| | |
|---|---|
| *R2* | *Afin de garder le contrôle sur la connectivité du terminal, désactiver systématiquement l'association automatique aux points d'accès Wi-Fi configurés dans le terminal.* |

| | |
|---|---|
| R3 | Maintenir le système d'exploitation et les pilotes Wi-Fi du terminal en permanence à jour des correctifs de sécurité. |

| | |
|---|---|
| R4 | Éviter tant que possible de se connecter à des réseaux sans fil inconnus ou qui ne sont pas de confiance. |

| | |
|---|---|
| R5 | Bloquer, par configuration du pare-feu local, les connexions entrantes via l'interface Wi-Fi. |

**Sur les terminaux à usage professionnel :**

| | |
|---|---|
| R6 | Respecter la politique de sécurité de l'entité, en particulier s'agissant des moyens cryptographiques d'authentification ainsi que de protection en confidentialité et en intégrité qui doivent être mis en œuvre. |

| | |
|---|---|
| R7 | Ne pas brancher de bornes Wi-Fi personnelles sur le réseau de l'entité. |

| | |
|---|---|
| *R8* | *En situation de mobilité, lors de toute connexion à des points d'accès Wi-Fi qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport), préalablement à tout échange de données, utiliser systématiquement des moyens de sécurité complémentaires (VPN IPsec par exemple).* |

| | |
|---|---|
| R9 | Plus largement, lorsque des données sensibles doivent être véhiculées via un réseau Wi-Fi, l'utilisation d'un protocole de sécurité spécifique, tel que TLS ou IPsec, doit être mis en œuvre. |

**Sur les points d'accès Wi-Fi :**

| | |
|---|---|
| R10 | Configurer le point d'accès pour utiliser un chiffrement robuste. le mode WPA2 avec l'algorithme de chiffrement AES-CCMP est fortement recommandé. Pour les points d'accès personnels, utiliser le mode d'authentification WPA-PSK (WPA-Personnel) avec un mot de passe long (une vingtaine de caractères par exemple) et complexe, d'autant plus que ce dernier est enregistré et n'a pas besoin d'être mémorisé par l'utilisateur |

Note : L'utilisation d'un mot de passe faible peut réduire à néant la sécurité du réseau Wi-Fi. La notion de complexité d'un mot de passe est abordée dans les recommandations de sécurité relatives aux mots de passe.

| | |
|---|---|
| R11 | Lorsque l'accès au réseau Wi-Fi n'est protégé que par un mot de passe (WPA-PSK), il est primordial de changer régulièrement ce dernier mais également de contrôler sa diffusion. En particulier, il convient de :<br><br>– ne pas communiquer le mot de passe à des tiers non autorisés (prestataires de services par exemple);<br><br>– ne pas écrire le mot de passe sur un support qui pourrait être vu par un tiers non autorisé;<br><br>– changer le mot de passe régulièrement et lorsqu'il a été compromis. |

| | |
|---|---|
| R12 | Pour les réseaux Wi-Fi en environnement professionnel, mettre en œuvre WPA2 avec une infrastructure d'authentification centralisée en s'appuyant sur WPA-Entreprise (standard 802.1X et protocole EAP), ainsi que des méthodes d'authentification robustes. |

Note : Un abonné à un réseau Wi-Fi protégé par WPA-PSK peut très simplement intercepter les données échangées par un autre abonné de ce même réseau. L'utilisation de WPA-PSK ne permet donc pas de garantir la confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi. En environnement professionnel, EAP reste alors à privilégier. Différentes méthodes d'authentification basées sur le protocole EAP peuvent être utilisées, mais certaines sont à éviter car elles peuvent présenter des vulnérabilités. Parmi les méthodes d'authentification EAP les plus robustes associées au label WPA-Entreprise, EAP-TLS est à privilégier. Elle exige toutefois une Infrastructure de Gestion de Clés (IGC), avec clé privée et certificat à déployer auprès de chaque utilisateur. Lorsqu'EAP est utilisé, il convient par ailleurs que les clients vérifient l'authenticité du serveur d'authentification

| | |
|---|---|
| R13 | Configurer le Private VLAN invité en mode isolated lorsque que le point d'accès Wi-Fi prend en charge cette fonctionnalité. |

Note : La fonction de Private VLAN contribue à la protection en confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi

| | |
|---|---|
| R14 | Ne pas conserver un nom de réseau (SSID) générique et proposé par défaut. Le SSID retenu ne doit pas être trop explicite par rapport à une activité professionnelle ou une information personnelle |

| | |
|---|---|
| R15 | Désactiver systématiquement la fonction WPS (Wi-Fi Protected Setup) des points d'accès. |

Note : WPS simplifie l'authentification d'un terminal sur un réseau WPA2 (par code PIN par exemple) mais réintroduit une vulnérabilité importante qui en réduit fortement l'intérêt du point de vue de la sécurité. Cette fonctionnalité est détaillée en annexe.

| | |
|---|---|
| R16 | Sécuriser l'administration du point d'accès Wi-Fi, en :<br><br>– utilisant des protocoles d'administration sécurisés (HTTPS par exemple);<br><br>– connectant l'interface d'administration à un réseau filaire d'administration sécurisé, à minima<br><br>en y empêchant l'accès aux utilisateurs Wi-Fi;<br><br>– utilisant des mots de passe d'administration robustes |

| | |
|---|---|
| R17 | Configurer le point d'accès pour que les évènements de sécurité puissent être supervisés. En environnement professionnel, il est préférable de rediriger l'ensemble des évènements générés par les points d'accès vers une infrastructure centrale de supervision. |

| | |
|---|---|
| R18 | Maintenir le microgiciel des points d'accès à jour |

**Concernant l'architecture réseau :**

| | |
|---|---|
| R19 | Ne jamais sous-estimer la zone de couverture d'un réseau Wi-Fi. Ne jamais penser être à l'abri de tout risque du fait de l'isolement géographique du point d'accès Wi-Fi. |

| | |
|---|---|
| R20 | En environnement professionnel, isoler le réseau Wi-Fi du réseau filaire et mettre en place des équipements de filtrage réseau permettant l'application de règles strictes et en adéquation avec les objectifs de sécurité de l'organisme. Comme pour le point d'accès, l'équipement de filtrage doit être paramétré pour que puissent être supervisés les évènements de sécurité |

| | |
|---|---|
| R21 | Si un réseau Wi-Fi "visiteurs" doit être mis en place, il est recommandé de déployer une infrastructure dédiée à cet usage, isolée des autres et ne donnant accès à aucune ressource du réseau interne. Ce réseau doit par ailleurs avoir sa propre politique de sécurité beaucoup plus restrictive |

**En environnement Active Directory :**

| | |
|---|---|
| R22 | Mettre en œuvre les GPO nécessaires à l'application de stratégies de sécurité verrouillant les configurations Wi-Fi des postes clients Windows, de manière à appliquer techniquement différentes recommandations indiquées dans ce document |

| | |
|---|---|
| R23 | Afin de ne pas les communiquer aux utilisateurs, déployer sur les postes Windows les informations de connexion au Wi-Fi par GPO (nom de réseau, clé d'accès, certificats éventuels si la méthode EAP le nécessite, etc.) |

# 5 Sécurisation des accès

Préalablement à la sécurisation des accès, une présentation des différents concepts et des protocoles de sécurisation de données sera proposée.

## 5.1 Concepts

**L'identification** est le procédé consistant à associer un moyen de reconnaissance unique (identifiant) à une entité qui peut être une personne, un matériel ou un processus.

Ce terme désigne également l'opération qui consiste à déterminer l'entité qui se trouve à l'origine d'une action.

**L'authentification** est le processus qui consiste à vérifier que l'identité revendiquée par une entité l'est de façon légitime.

Elle est basée sur un ou plusieurs mécanismes de reconnaissance :

- Quelque chose que l'entité connaît comme par exemple un mot de passe ou un numéro personnel d'identification (code PIN) ;
- Quelque chose que l'entité possède, telle qu'une carte ou une clé ;
- Une caractéristique physique telle qu'une empreinte digitale ou rétinienne.

**L'authentification** est plus sûre si plusieurs techniques sont utilisées conjointement, on parle alors d'authentification forte.

On parle d'authentification mutuelle lorsque deux entités s'identifient l'une auprès de l'autre. Dans le cadre du Wi-Fi il s'agit de vérifier l'identité de la personne ou de la machine qui veut se connecter au réseau ET de vérifier l'identité de la machine qui donne accès au réseau (afin d'être certain se connecter au bon réseau).

**L'autorisation** consiste à définir ce qu'une identité a le droit de faire avec une ressource mise à sa disposition.

**Le contrôle d'accès** consiste à vérifier si une entité a l'autorisation d'effectuer une action sur une ressource. Si le moyen d'authentifier une identité n'est pas sûr, alors il n'est pas possible de garantir que l'accès soit accordé à la bonne entité.

**La « journalisation »**, est le processus qui vise à enregistrer l'historique des événements concernant un processus informatique. Ces historiques sont conservés dans des fichiers appelés journaux. Un journal de connexion peut contenir plusieurs données liées à une connexion, comme la date et l'heure, l'adresse MAC de l'adaptateur réseau du client final, l'adresse IP d'un équipement, l'identifiant d'un abonné...

Si le moyen d'authentifier une identité n'est pas sûr, alors il n'est pas possible de garantir que les actions enregistrées dans le journal ont été imputées à la bonne entité.

## 5.2 Normes de sécurité Wi-Fi ou applicables au réseau WI-FI

| Nom | Norme | Description | Remarque |
|---|---|---|---|
| WEP | 802.11 | Chiffrement optionnel proposé dans la norme 802.11 | Obsolète |
| WPA | 802.11i | Wi-Fi protected access repris dans la norme 802.11i<br><br>Chiffrement : TKIP.<br><br>Deux modes d'authentification :<br><br>1) WPA-PSK mode (secret partagé) ;<br>2) WPA Enterprise Mode (serveur RADIUS). | Déprécié |
| WPA2 | 802.11i | Chiffrement AES (WRAP et CCMP) | Recommandé (CCMP) |
| Port Based Network Access Control | 802.1X | Contrôle d'accès des équipements aux réseaux filaires et non filaires.<br><br>Non spécifique à Wi-Fi, incluse dans 802.11i. | Recommandé |
| WPS | Ss objet | Wi-Fi protected setup | Déconseillé |

**CE QU'IL FAUT RETENIR**

- **Le protocole WEP NE DOIT PAS être utilisé.**
- **Le protocole WPA NE DEVRAIT PAS être utilisé.**
- **Le protocole WAP2 ou un protocole de niveau de sécurité supérieur DEVRAIT être utilisé.**
- **WPS NE DEVRAIT PAS être utilisé.**

## 5.3 802.1X (EAPOL) EAP OVER LAN

### 5.3.1 Introduction

Le protocole 802.1X est un standard mis au point par l'IEEE dans le but de contrôler les accès physiques à un réseau local filaire ou sans fil pour établir des connexions sécurisées. Il s'appuie sur EAP (Extensible Authentication Protocol - IETF RFC 3748) pour fournir une authentification mutuelle et centralisée. Initialement développé pour les réseaux locaux filaires, il a ensuite été utilisé par la norme IEEE 802.11i pour le contrôle d'accès aux réseaux locaux sans fil et la distribution des clés cryptographiques.

Le standard 802.1X permet de contrôler l'accès au réseau au niveau de la couche 2 – couche liaison – du modèle OSI tout en s'appuyant sur des protocoles d'authentification de couche supérieure pour fournir les moyens de bloquer l'accès aux ressources du réseau local jusqu'à ce que l'utilisateur ou l'équipement soit correctement identifié et authentifié par un point d'accès.

### 5.3.2 Authentification 802.1X

L'architecture d'authentification IEEE 802.1X est constituée de trois entités :

- Le client 802.1X (« supplicant ») : c'est le système à authentifier : par exemple une station voulant joindre le réseau Wi-Fi.
- Le contrôleur (« authenticator ») : c'est l'entité qui contrôle l'accès au réseau, par exemple le point d'accès d'un réseau sans fil.
- Le serveur d'authentification (« authentication server ») : c'est l'entité qui vérifie les accréditations présentées par le demandeur et qui prend la décision d'autorisation.

Le protocole EAP est destiné à encapsuler des protocoles d'authentification et les informations de contrôle relatives, il est basé sur un nombre limité de messages (Request, Response, Success, Failure). C'est un cadre de travail pour le transport de méthodes d'authentification variées telles qu'EAP-TTLS PEAP, EAP-TLS. Pour que les messages EAP puissent être transportés sur un réseau local, 802.1x définit EAPOL (EAP over LAN) pour encapsuler les paquets EAP.

C'est le protocole utilisé dans les réseaux sans fils entre le client et le contrôleur qui ne fait que transmettre les messages au serveur d'authentification. Les communications entre le contrôleur et le serveur d'authentification utilisent des protocoles de plus haut niveau qui ne sont pas imposés par la norme tel que RADIUS ou Diameter (IETF RFC 3588).

### 5.3.3 Contrôle d'accès basé sur le port (port-based authentication)

Pour gérer les autorisations d'accès au réseau, 802.1X scinde le port du point d'accès en deux ports logiques : le port contrôlé et le port non contrôlé.

Le port non contrôlé ne gère que les trames EAPOL (EAP encapsulation over LANs) spécifiques à 802.1X, (ce sont les messages d'authentification entre le « supplicant » et le serveur d'authentification).

Le port contrôlé est le seul port qui peut permettre les communications avec le réseau, il peut prendre deux états :

- non-authentifié : l'accès au réseau est refusé.
- authentifié : l'accès au réseau est permis

*Dans le cadre du déploiement de réseaux sans fil basés sur la norme 802.11i dans un EPLE, le serveur d'authentification pourrait être par exemple le module freeRadius du serveur EOLE AMON.*

**CE QU'IL FAUT RETENIR**

- **Tant qu'il n'est pas authentifié, le client ne peut pas avoir accès au réseau.**
- **Seuls les échanges liés au processus d'authentification sont relayés vers le serveur d'authentification par le port non contrôlé du point d'accès. Une fois identifié et authentifié par le serveur d'authentification, le port contrôlé du point d'accès laisse passer le trafic lié au client.**

## 5.4 Radius

RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification et de journalisation (Authentication Authorization Accounting AAA). Il est défini par les RFC 2865 (RADIUS authentication) et RFC 2866 (RADIUS accounting) de juin 2000. Par extension, on appelle serveur Radius, un serveur d'authentification qui implémente le protocole Radius (Remote Authentication Dial In User Service). FreeRadius est une implantation de radius très utilisée publiée sous licence GPLv2.

### 5.4.1 Radius et 802.1X-EAP

La RFC 3580 décrit les spécifications d'usage de 802.1X avec Radius. Les serveurs radius sont utilisés comme serveur d'authentification dans le protocole 802.1X. Les clients radius (NAS) représentent les contrôleurs (authenticator) dans le protocole 802.1X, ce sont les commutateurs ou les points d'accès sans fil. Ils interrogent serveur radius pour savoir si une entité (le client ou supplicant dans 802.1X) est autorisée à accéder à une ressource (un réseau, un vlan). Le serveur Radius est capable d'envoyer au contrôleur le numéro du VLAN qui doit être affecté au port sur lequel est connecté le poste de travail. Il n'y a jamais de communication directe entre le poste de travail (le client ou supplicant dans 802.1X) et le serveur. Ce sont les contrôleurs 802.1X qui relaient les messages d'authentification. Radius supporte un grand nombre de méthodes d'authentification EAP et plus particulièrement les méthodes basées sur TLS décrites dans la suite du document. Il peut interroger divers types de bases d'authentification externes telles qu'une base de domaine Windows, une base LDAP une base MySQL, etc.

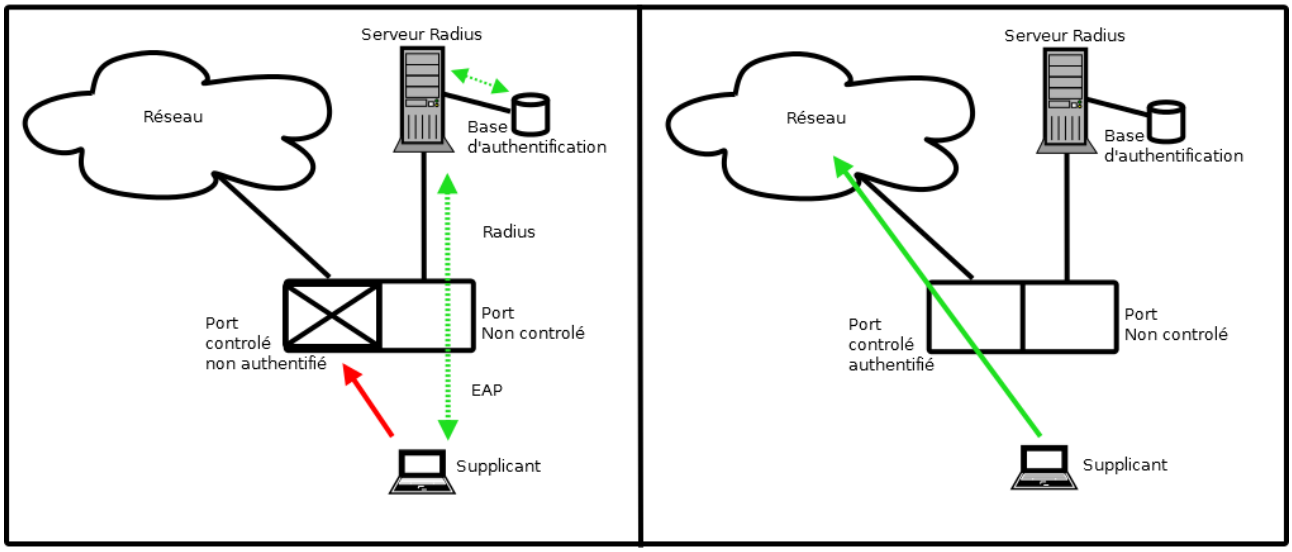



Figure 1 : Authentification 802.1X avec Radius

### 5.4.2 Délégation d'authentification

Une autre fonctionnalité intéressante des serveurs RADIUS réside dans le fait qu'ils peuvent être utilisés pour rediriger les requêtes d'authentification vers un autre serveur RADIUS. Le terme realm (royaume) est utilisé pour désigner la notion de domaine de noms de domaines. Cette fonctionnalité permet à des utilisateurs en déplacement de s'authentifier en interrogeant leur serveur de rattachement. La figure 2 décrit le cas d'un utilisateur académique s'authentifiant sur une base de données centrale depuis un établissement.

Le serveur de l'établissement est paramétré pour rediriger les requêtes dont l'identifiant est de la forme user@ac-academie vers le serveur radius.ac-academie.fr.

Le serveur radius.ac-academie.fr doit également être configuré pour accepter les requêtes d'authentification du serveur de l'établissement. Pour que ce type d'authentification soit robuste, il est impératif de protéger la communication entre les deux serveurs par un mécanisme cryptographique efficace (un tunnel IPsec par exemple).

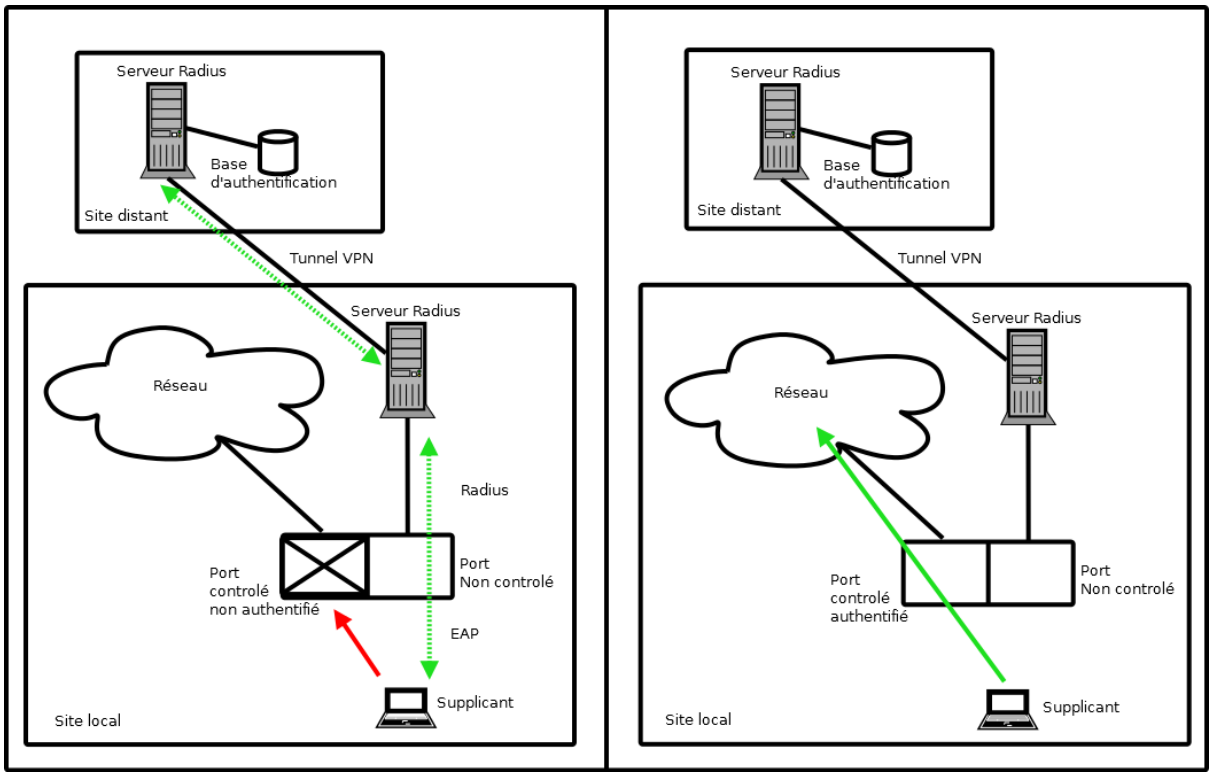



Figure 2 : Délégation d'authentification

## 5.5 Vue d'ensemble de la sécurité 802.11i

Les grandes catégories de menaces visant les réseaux sans fil, sont les mêmes que pour les réseaux filaires. La différence fondamentale dans le degré de protection à mettre en place est qu'un attaquant n'a pas besoin d'avoir un accès physique aux bâtiments ou de compromettre une machine pour accéder au réseau local. Il a simplement besoin d'être dans la zone de couverture du réseau sans fil pour pouvoir intercepter ou injecter des communications. En outre la portée du réseau peut être considérablement étendue par l'utilisation d'antennes directionnelles très performantes. La sécurité d'un réseau Wi-Fi dépend pour partie des mécanismes d'authentification utilisés afin d'identifier les utilisateurs du réseau de manière univoque et sûre et des mécanismes cryptographiques mis en œuvre afin de protéger les communications sans-fil. Les mécanismes de sécurité inclus dans les premières versions de la norme 802.11 se sont rapidement avérés insuffisants. L'amendement 802.11i apporte une réponse à cette problématique en fournissant une protection au niveau de la couche liaison du modèle OSI (niveau 2)entre un point d'accès et une station (mode infrastructure) ou entre deux stations (mode ad-hoc).

Ses objectifs sont :

- d'assurer le contrôle d'accès au réseau par le support d'un service d'authentification de l'entité homologue. (confirmer que l'entité est autorisée à accéder au réseau après avoir vérifié son identité)
- d'assurer l'authentification de l'origine de données (confirmer la source des trames de données)
- de protéger la confidentialité et l'intégrité des trames de données.

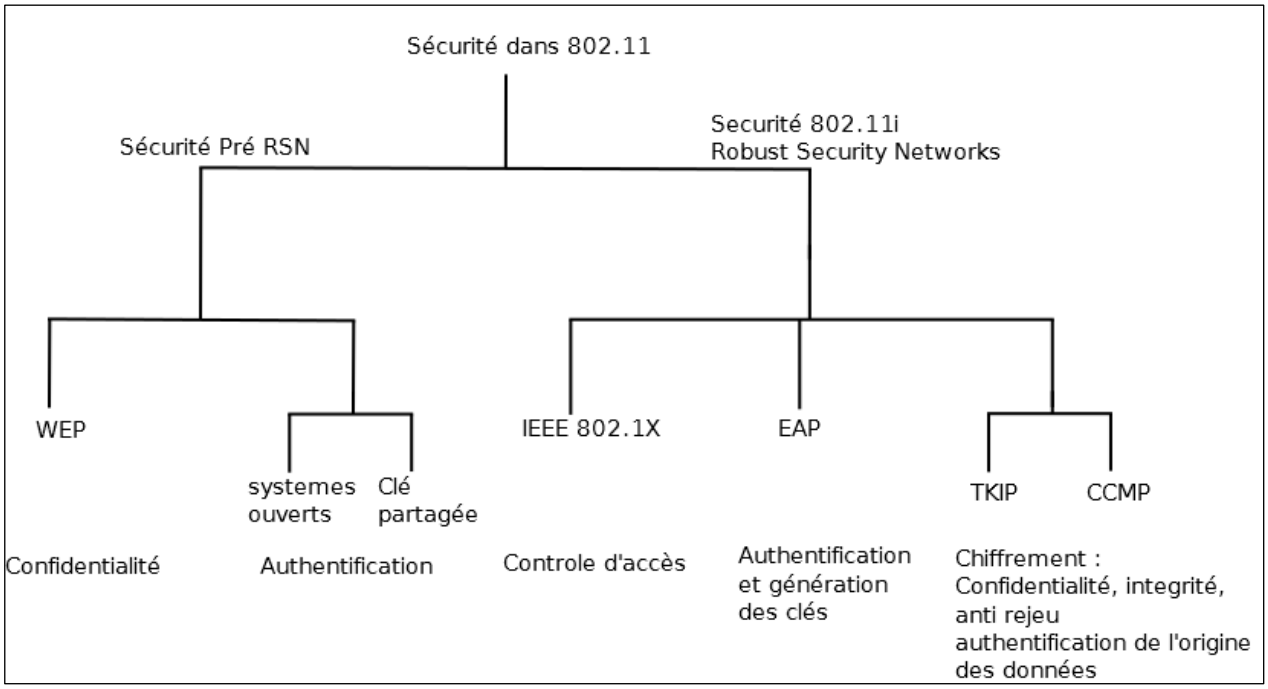



Figure 3 : Sécurité 802.11

802.11i propose deux modes d'authentification et introduit un véritable concept de session, à l'issue de la phase d'authentification, chaque client se retrouve avec une clé de session propre qui servira à opérer le chiffrement. Elle adresse également les problèmes de rejeu et d'injection de trafic, et s'appuie sur des algorithmes de chiffrement reconnus et efficaces pour assurer la confidentialité et l'intégrité des données. L'architecture sécurisée introduite par 802.11i est baptisée RSN (Robust Security Network). Elle utilise le protocole IEEE 802.1X pour les contrôles d'accès, s'appuie sur EAP pour l'authentification, la rotation et la distribution des clés cryptographiques, et supporte l'utilisation des mécanismes d'intégrité et de chiffrement TKIP et CCMP. Les fonctions de sécurité initiales de la norme 802.11, bien qu'inefficaces, sont conservées et rebaptisées sécurité pré-RSN.

**Ce que 802.11i ne traite pas :**

- Un RSN assure la sécurité au niveau 2 du modèle OSI, la couche liaison. Il fournit une protection pour le trafic entre une station sans fil et le point d'accès associé, ou entre deux stations sans fil. Il ne fournit pas de sécurité de bout en bout au niveau applicatif, par exemple entre la station et un serveur de messagerie, parce que la communication entre ces entités nécessite plusieurs liens. Pour assurer la sécurité de bout en bout, il faut mettre en œuvre d'autres mécanismes de sécurité, tels que TLS ou IPsec. En outre, les fonctionnalités de sécurité des RSN ne s'appliquent qu'à la partie sans fil du réseau local, pas aux communications sur les réseaux câblés.
- La disponibilité -capacité à accéder aux services- du réseau n'est pas non plus protégée.

- Un RSN ne fournit pas de protection contre les attaques en saturation -le fait d'envoyer une grande quantité de messages pour saturer le service et le rendre inutilisable - ou contre le brouillage des ondes physiques. Un attaquant peut également profiter du fait que les trames de gestion ne sont pas protégées pour dé-authentifier ou dissocier les clients du réseau.

### 5.5.1 RSN-RSNa

Un RSN est défini comme un réseau sans fil ne permettant que des associations RSNA. Une RSNA (Robust Security Network Association) est une relation de sécurité établie par un échange appelée 4-Way Handshake qui valide que les deux parties de l'association possèdent une clé maître appelée PMK, synchronise l'installation de clés temporaires, confirme la sélection des suites de chiffrement pour finalement autoriser l'accès au réseau par le port contrôlé 802.1X du point d'accès. Le trafic n'est permis qu'après le succès de l'authentification 802.1X et l'installation réussie des clés cryptographiques.

Le fonctionnement d'un RSNa comporte quatre phases :

- la mise en accord sur la politique de sécurité
- l'authentification
- la dérivation et la distribution des clés cryptographiques
- le chiffrement et l'intégrité des trames de données

Bien que ce document se focalise sur les réseaux de type infrastructure, ces concepts restent valables dans un contexte de réseaux ad-hoc où les entités jouent à la fois les rôles du point d'accès et de la station.

### 5.5.2 Mise en accord sur la politique de sécurité

La phase de mise en accord sur la politique de sécurité est décrite par la Figure 4.

Les politiques de sécurité supportées par le point d'accès sont diffusées dans les trames Beacon et Probe Response elles-mêmes répondant à un message Probe Request du client. L'établissement d'un RSNa commence par une authentification ouverte standard (toujours positive) comme celle utilisée dans les réseaux ouverts. La réponse du client aux politiques de sécurité supportées est incluse dans le message Association Request validé par le message Association Response du point d'accès. Elle permet de déterminer :

- les méthodes d'authentification supportées (802.1X, clé pré-partagée (PSK))
- le protocole de sécurité (CCMP ou TKIP) pour le chiffrement du trafic unicast
- le protocole de sécurité pour le chiffrement du trafic en diffusion (multicast)
- le support de la pré-authentification permettant aux utilisateurs de se pré-authentifier avant de basculer sur un nouveau point d'accès.

### 5.5.3 Protocoles de chiffrement

L'amendement de la norme IEEE 802.11i définit les deux protocoles suivants de confidentialité des données pour assurer la confidentialité et l'intégrité :

- TKIP (RC4 + Mickael)
- CCMP (AES)

#### 5.5.3.1 TKIP

TKIP a été pensé en tant qu'évolution du WEP et introduit par WPA dans la norme IEEE 802.11I. Il continue de s'appuyer sur l'algorithme de chiffrement à flot RC4. La méthode d'initialisation de RC4 étant entièrement revue, une réponse sérieuse aux problèmes de sécurité rencontrés avec WEP est apportée. Cependant, si l'évolution par rapport à WEP a été bénéfique, l'algorithme de chiffrement à flot RC4 est désormais considéré comme peu sûr du point de vue cryptographique.

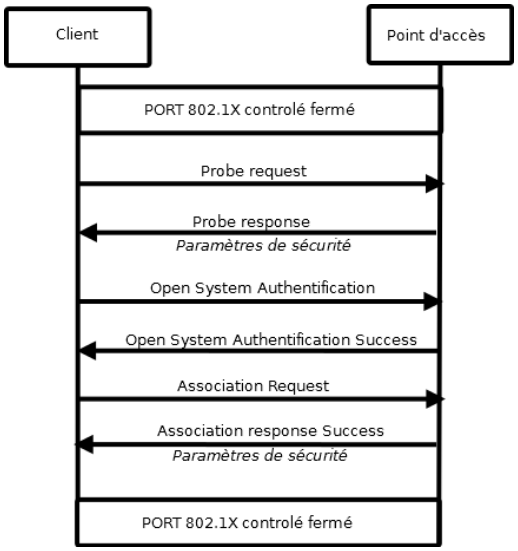



Figure 4 : RSNa Phase 1 mise en accord sur la politique de sécurité

Fin 2008, Martin Beck et Erik Tews ont publié une attaque sur TKIP permettant dans certaines conditions de déchiffrer des trames arbitraires émise par un point d'accès à destination d'une station et d'injecter du trafic arbitraire à destination de la station considérée. Cette attaque et les recommandations pour s'en protéger sont mentionnées dans les bulletins d'actualité CERTA-2008- ACT-045 2 et CERTA-2008-ACT-047 3 du CERT-FR4.

TKIP est considéré comme obsolète dans la révision de 2012 de la norme 802.11 (IEEE 802.11-2012 page 94). L'amendement 802.11n n'est pas compatible avec TKIP (les connexions utilisant TKIP ou WEP y sont considérées comme des connexions 802.11g avec un débit théorique ne pouvant dépasser 54Mbit/s).

#### 5.5.3.2 CCMP AES

Depuis plusieurs années, l'algorithme de chiffrement et de contrôle d'intégrité AES CCMP (utilisé par WPA2 basé sur l'algorithme de chiffrement par bloc AES) également introduit dans la norme 802.11I est supporté par la quasi-totalité des matériels Wi-Fi. Il est considéré comme robuste et aucune attaque cryptographique réaliste d'AES-CCMP n'est connue à ce jour. Il s'agit donc de l'algorithme à privilégier afin de protéger la confidentialité et l'intégrité des communications Wi-Fi.

Toutes les cartes Wi-Fi certifiées 802.11n supportent obligatoirement CCMP. Tous les équipements certifiés WPA2 par la Wi-Fi alliance supportent le chiffrement CCMP-AES ainsi que tous les équipements ayant obtenus le label Wi-Fi CERTIFIED après le mois de mars 2006.

**CE QU'IL FAUT RETENIR**

- **Tout nouveau déploiement de réseau sans fil sécurisé DEVRAIT utiliser le chiffrement CCMP AES ou de niveau de sécurité supérieur.**

## 5.6 Gestion des clés

La sécurité offerte par le chiffrement des transmissions repose essentiellement sur des clés secrètes. Plus ces clés seront utilisées, plus un attaquant aura des données chiffrées à analyser, et plus il aura de chances de réussir des attaques. C'est pourquoi il est souvent souhaitable de limiter la validité des clés employées. La norme 802.11i prévoit un mécanisme de renouvellement des clés cryptographiques effectivement utilisées.

Les fonctions de chiffrement, d'intégrité et d'authentification reposent sur plusieurs clés cryptographiques différentes qui ont une durée de vie limité. Après une authentification réussie, des clés temporaires (de sessions) sont créées par un mécanisme de "poignées de main" le 4 way hanshake et régulièrement mises à jour jusqu'à la fermeture du contexte. Deux familles de clés sont définies par la norme pour protéger les trafics de diffusion et le trafic unicast.

### 5.6.1 Clés de groupe (Group Key Hierarchy)

Les clés de groupe (GTK) sont destinées à protéger le trafic de diffusion (multicast / broadcast) du réseau. Elles sont générées régulièrement par le point d'accès à partir d'une clé maitre (GMK) et sont distribuées de manière sécurisée aux clients.

### 5.6.2 Clés unicast (Pairwise Key Hierarchy)

La « Pairwise Key Hierarchy », définit les clés conçues pour la protection du trafic unicast entre le client et le point d'accès. Ces clés différentes mais interdépendantes sont dérivées à partir d'une clé maitre, la PMK (Pairwise Master Key) obtenue pendant la phase d'authentification selon le processus décrit par la Figure 5.

La PMK en elle-même n'est jamais utilisée pour le chiffrement ou le contrôle d'intégrité. Elle n'est utilisée que pour la génération de clés de chiffrement temporaires suivantes :

- La KCK destinée à authentifier les échanges pendant la dérivation des clés, (preuve la connaissance de la PMK par une vérification d'intégrité durant le 4-Way handshake)
- La KEK destinée à assurer la confidentialité des échanges pendant la dérivation des clés (chiffrement la GTK)
- La TEK destinée à assurer la confidentialité et l'intégrité des communications en chiffrant les messages échanges pendant la durée de la session.

Ces clés temporaires sont dérivées à partir de la PMK, et de paramètres qu'un attaquant peut capturer en écoutant le réseau pendant le 4-Way handshake. La PMK est donc la pierre angulaire de la sécurité de la solution. La dérivation de la PMK dépend de la méthode d'authentification choisie :

- dans le mode EAP (WPA entreprise) elle est générée par la méthode d'authentification EAP sélectionnée
- dans le mode clé partagée (WPA personnel) elle dérivée de la clé partagée (la PSK) par l'algorithme public PBKDF2

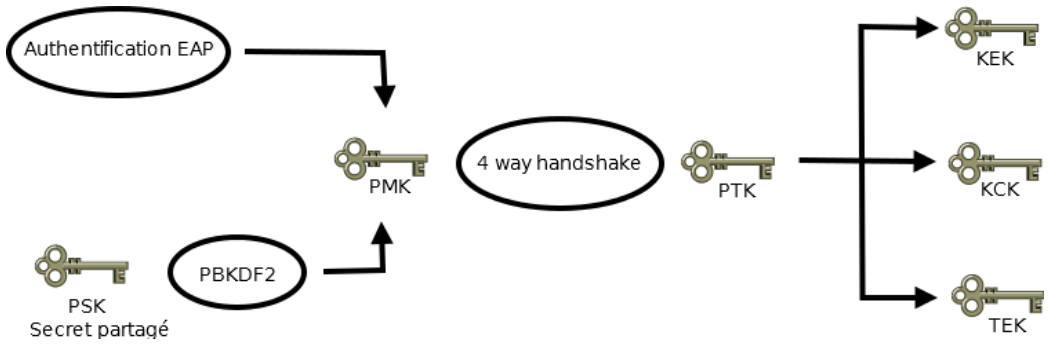



Figure 5 : Dérivation des clés cryptographiques

PBKDF2 est une fonction standard (RFC2898), conçue pour être lente qui sert à dériver une clé de longueur arbitraire à partir d'un mot de passe. Elle met en œuvre un nombre conséquent (plus de 8000 dans WPA/WPA2-PSK) d'itérations de la fonction de hash HMAC-SHA1 pour atteindre un temps de calcul conséquent. Lors d'un accès légitime, la lenteur n'est pas prohibitive car la dérivation n'est faite qu'une seule fois.

Par contre lors d'une attaque, il faut exécuter la fonction pour chaque nouveau mot de passe à tester. Ces itérations sont très importantes car elles permettent d'accroitre considérablement le temps nécessaire à un attaquant pour réussir une attaque en force brute. Dans le cadre de l'amendement 802.11i, PBKDF2 utilise le SSID du réseau comme une graine d'aléa, ou salt anglais, afin bloquer les attaques par dictionnaires pré calculés, couramment appelés "Rainbow Tables".

Ceci implique qu'un éventuel dictionnaire pré calculé WPA/WPA2-PSK ne pourra être utilisé que pour les SSID qui auront été utilisés pour sa création. Cette raison justifie la préconisation d'opter pour un SSID personnalisé, éventuellement unique, quand on configure son accès.

### 5.6.3 4-way Handshake

Le 4-Way Handshake décrit par la Figure 6 est un échange de quatre messages EAPOL transitant en clair entre le client et le point d'accès qui permet de :

- confirmer la connaissance mutuelle de la PMK, et ainsi assurer une certaine forme d'authentification.
- dériver et installer de nouvelles clés temporelles sur la station et le point d'accès et de fournir l'assurance de l'utilisation de nouvelles clés de chiffrement et d'intégrité.

La PTK contenant les clés de chiffrement temporaires KCK KEK et TEK est générée à partir de la PMK, des adresses MAC des points d'accès et du client et de deux nombres aléatoires Anonce et Snonce générés respectivement par le point d'accès et le client.

1. la réception du premier message contenant Anonce le client ayant généré SNonce est en mesure de dériver la PTK, il construit alors le deuxième message en y intégrant un code d'intégrité (MIC Message Integrity Code) calculé avec à la clé KCK qu'il vient de générer.
2. À la réception du deuxième message contenant SNonce, le point d'accès est en mesure de dériver la PTK à son tour, grâce à la KCK il vérifie alors le code d'intégrité du message 2, s'il est valide alors il a l'assurance que le client connait la PMK et qu'il a dérivé les clés temporelles. Il construit le 3eme message en y intégrant un code d'intégrité (MIC) calculé avec à la clé KCK
3. À la réception du troisième message le client vérifie le code d'intégrité pour valider le fait que le point d'accès connait la PMK et qu'il a dérivé les clés temporelles.

4. Le quatrième message indique que le client a correctement installé les clés temporelles et qu'il est prêt à commencer le chiffrement des données. Après sa réception le point d'accès installe les clés temporelles et les deux entités sont en mesure de chiffrer leurs communications.

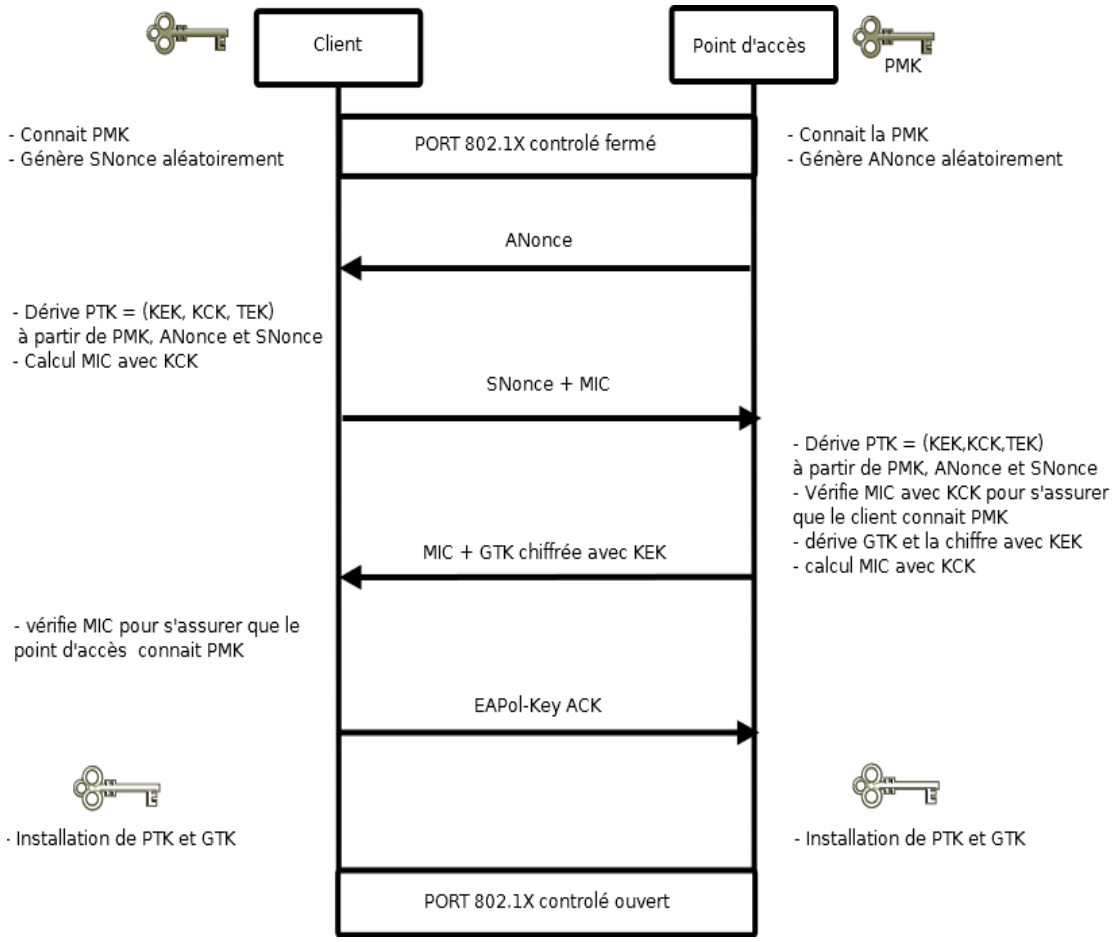



Figure 6 : 4 way handshake

Si le 4-Way Handshake est un succès alors le port IEEE 802.1X contrôlé passe à l'état autorisé et la station peut alors communiquer avec le réseau de manière sécurisée en utilisant le protocole de chiffrement déterminé.

### 5.6.4 Authentification et distribution de la clé maitre (PMK)

Les deux modes d'authentification (PSK et 802.1X) supportés n'offrent pas les mêmes garanties de sécurité.

#### *5.6.4.1 Authentification PSK*

Dans le mode PSK, c'est la clé partagée qui joue le rôle de la PMK décrite plus haut et qui assure une authentification implicite. Tous les équipements du réseau sans fil (points d'accès, stations) partagent donc la même PMK. Or c'est la connaissance de cette PMK par une station qui permet son authentification par le point d'accès. Cela signifie que plutôt qu'authentifier le client, un point d'accès vérifie qu'il est membre d'un groupe autorisé, le groupe qui partage la clé. **Le mode PSK n'offre donc pas d'authentification des clients dans le sens commun du terme**. Néanmoins le client authentifie le point d'accès fournissant l'assurance que l'on se connecte au bon réseau.

La clé partagée est également utilisée avec le SSID du réseau pour générer les clés cryptographiques (uniques pour chaque client sans fil) qui serviront au chiffrement et le contrôle d'intégrité Wi-Fi. Les protocoles de dérivation des clés étant publics, et les paramètres aléatoires transmis en clair toute personne ayant connaissance du mot de passe peut déterminer toutes les clés de chiffrement utilisées. **Le mode PSK n'offre donc pas un bon niveau de confidentialité**.

**Vulnérabilités :**

- Il est illusoire de vouloir préserver un secret partagé par plusieurs personnes. Il suffit qu'une personne le divulgue, volontairement ou non, pour que l'authentification et la confidentialité des communications soit compromise, quel que soit l'algorithme de chiffrement utilisé.
- Si un mot de passe faible est utilisé, une phrase courte par exemple, une attaque par dictionnaire hors ligne peut facilement deviner le PSK et compromettre tout le réseau.

**Précautions :**

- Choisir un SSID personnalisé et unique sans relation avec une activité sensible
- Choisir un mot de passe robuste et le changer régulièrement

**CE QU'IL FAUT RETENIR**

- **Le mode d'authentification par clé partagée WPA-PSK convient particulièrement pour sécuriser un point d'accès Wi-Fi unique avec un petit nombre d'utilisateurs, sans contrainte de confidentialité des flux entre terminaux du réseau Wi-Fi.**
- **Par contre, le niveau de sécurité devient faible pour un usage professionnel nécessitant un grand nombre de points d'accès ou pour un grand nombre d'utilisateurs.**

#### *5.6.4.2 Authentification 802.1X-EAP*

Le mode d'authentification 802.1X EAP décrit par la **Erreur ! Source du renvoi introuvable.**, utilise le tandard 802.1X pour réaliser une authentification mutuelle entre la station et le point d'accès, ainsi que la génération et le transfert de la clé PMK. Chaque fois qu'un utilisateur ou qu'un équipement est authentifié une nouvelle clé est générée pour être utilisée pendant la durée de la session de l'utilisateur.

Ce mode demande donc à ce que l'on installe un serveur d'authentification et fourni un cadre qui permet l'utilisation de plusieurs méthodes d'authentification.

Dans 802.11i les trois entités définies par l'architecture d'authentification IEEE 802.1X sont :

- la station voulant joindre le réseau sans fil (supplicant)
- le point d'accès au réseau sans fil (authenticator)
- Le serveur d'authentification (authentication server)

Le protocole EAPOL est utilisé pour transporter les messages d'authentification EAP entre la station et le point d'accès utilisent alors que le protocole RADIUS est le plus utilisé pour transférer les messages entre le point d'accès et le serveur d'authentification.

Le port 802.1X contrôlé est bloqué pendant tout le processus interdisant ainsi à la station d'accéder au réseau, seuls les échanges EAPOL liés au processus d'authentification sont relayés vers le serveur d'authentification par le port non contrôlé du point d'accès. Même lorsque l'authentification a réussi le port contrôlé demeure fermé jusqu'à l'installation des clés de chiffrement temporelles générées par le 4-way handshake.

Lorsque l'authentification réussie, la station et le point d'accès sont en possession de la clé maître (PMK) utilisée pour établir les clés temporelles et pierre angulaire de la sécurité. L'amendement 802.11i ne spécifie pas comment cette clé doit être générée, c'est le rôle de la méthode EAP. Il ne spécifie pas non plus comment elle doit être délivrée à la station, c'est toujours le rôle de la méthode EAP, ni au point d'accès car la liaison avec le serveur d'authentification est filaire.

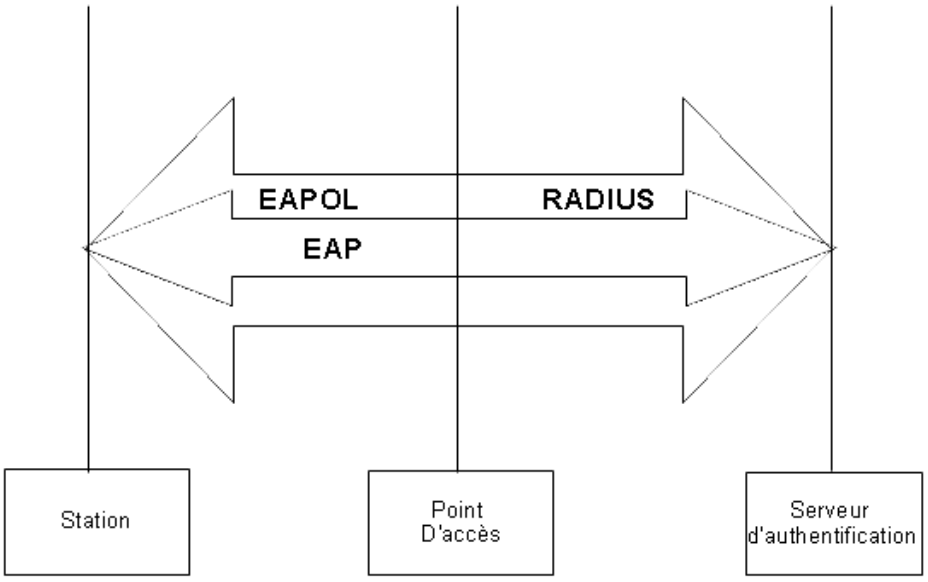



Figure 7 : Encapsulation EAP

### *Dialogue entre le point d'accès et le serveur d'authentification*

La connexion entre le serveur d'authentification et le point d'accès n'entre pas dans le périmètre de la norme 802.11i et est supposée sécurisée. Cette connexion servant notamment à la transmission des clés de chiffrement, il est crucial qu'elle soit protégée de bout en bout en intégrité et en confidentialité et qu'une authentification mutuelle robuste soit utilisée. Il en va de du serveur d'authentification lui-même dont la compromission engendrerait l'effondrement total de la sécurité du réseau sans fil.

### *Choix de la méthode d'authentification EAP*

La norme 802.11i fonctionne au niveau des couches 1 et 2 du modèle OSI, elle ne spécifie donc pas les protocoles d'authentification des couches supérieures utilisés en conjonction de 802.1X

Ces protocoles sont utilisés pour fournir d'une part, un échange d'authentification mutuelle entre le client et le serveur d'authentification et d'autre part pour générer les clés de session utilisées par le client et le point d'accès sur la liaison sans fil. Ce sont donc des éléments cruciaux en termes de sécurité.

C'est sur la méthode d'authentification choisie que repose la génération de la clé PMK pierre angulaire de la sécurité ainsi que son transport sécurisé jusqu'au point d'accès. Le choix de cette méthode est donc un élément fondamental dans le déploiement d'un réseau en mode "entreprise".

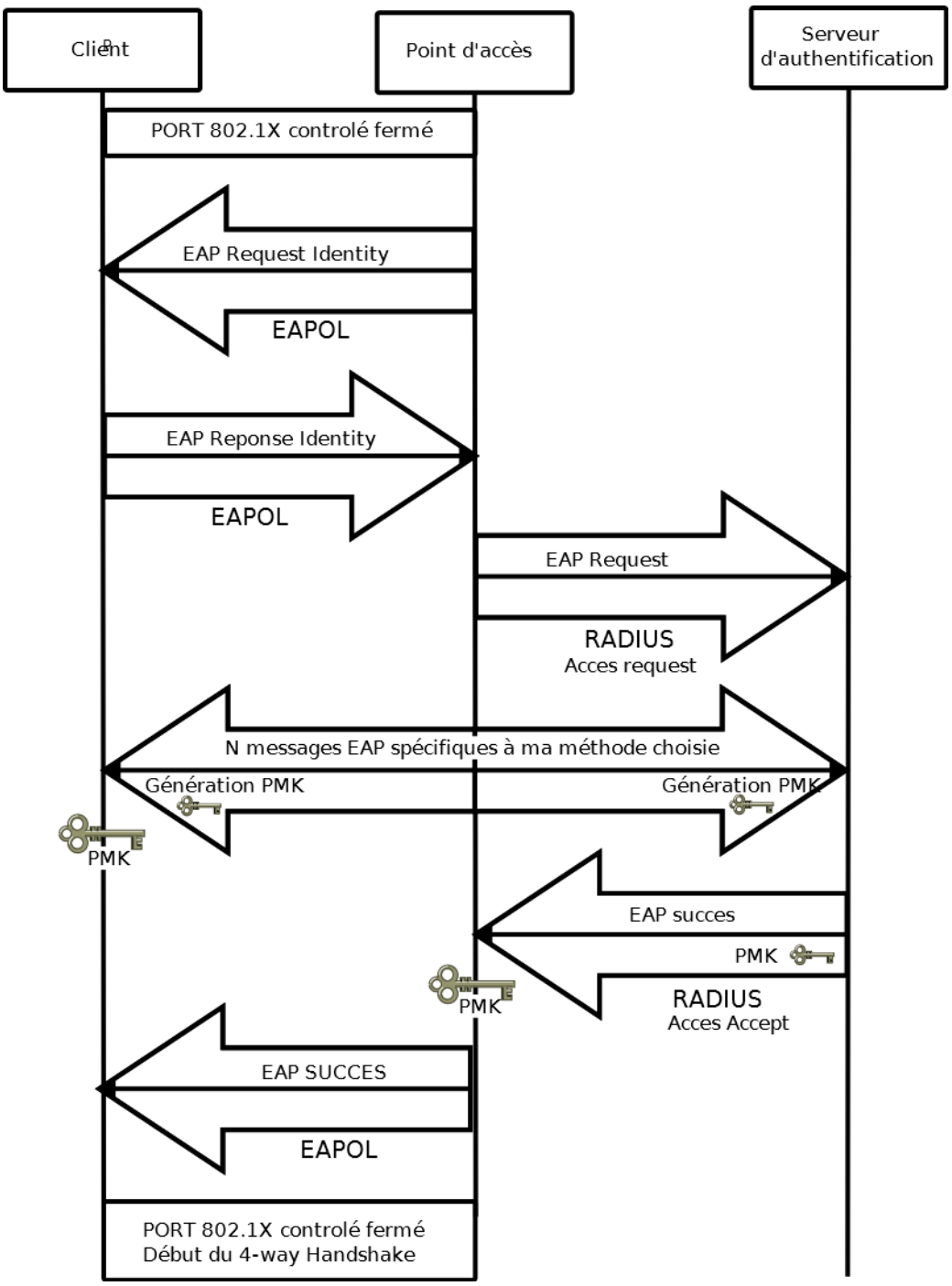



Figure 8 : Authentification 802.1X

Afin d'assurer la confidentialité des échanges EAP plusieurs solutions utilisent le protocole TLS pour établir un tunnel.

Les principaux protocoles utilisables sont EAP-TLS, EAP-TTLS et PEAP :

- EAP/TLS
- EAP/TTLS
- PEAP

**Vulnérabilités :**

- Compliqué à mettre en œuvre, nécessite une structure informatique avec une pki au moins pour les certificats serveurs,
- Faille dans la méthode eap (leap...),
- Attaques possibles de type homme du milieu (« man in the midle » ou « MITM », en anglais), interceptant les flux via un point d'accès pirate (« rogue access point » ou « rogue ap », en anglais).

Précautions :

- Configuration fine des stations avec une vérification obligatoire des certificats de l'AS par le client,
- Pas d'acceptation par l'utilisateur de certificats refusés par le système,
- Bon choix des méthodes EAP,
- Sécurisation du backend d'authentification (Radius vers annuaire).

# 6 Appréciation des risques et niveaux de sécurité

## 6.1 Introduction

L'objet de cette section est de fournir des éléments d'appréciation des risques dans le cadre du déploiement de réseau Wi-Fi au sein des établissements publics locaux d'enseignements (EPLE) et des écoles.

Elle s'adresse en priorité aux DSI, RSSI et DAN de l'éducation nationale.

Bien qu'il ne soit pas possible de lister de façon exhaustive les cas d'utilisation du Wi-Fi, les risques peuvent être appréciés au travers des usages envisagés et des types d'informations véhiculées sur les différents segments du réseau. Cette section fournit des éléments méthodologiques et des critères de choix pour accompagner :

- un déploiement maîtrisé en termes de risques au niveau de l'EPLE ou de l'école, ainsi que pour les systèmes d'information académiques ou ministériels auxquels ils sont connectés ;
- l'exercice d'un contrôle par le chef d'établissement ou le directeur d'école du déploiement et de l'utilisation du réseau.

Il s'agit de donner aux chefs d'établissement et aux directeurs les éléments d'appréciation et des conseils pour qu'ils puissent assurer leurs responsabilités pédagogique, administrative et juridique lors du dialogue avec les acteurs du projet. Ils pourront ainsi dialoguer, en connaissance de cause, de la conception de l'infrastructure Wi-Fi jusqu'à sa réalisation et à la mise en œuvre des dispositifs visant à limiter fortement les risques juridiques et ceux pesant sur leur système d'information et sur les usagers de l'établissement ou de l'école.

## 6.2 Contextes d'utilisation du Wi-Fi en établissement et école

Préalablement à tout déploiement Wi-Fi, il est primordial de se demander, ce que l'on attend de cette infrastructure. L'expression des besoins auxquels répond sa mise en place doit être effectuée localement avec toutes les parties prenantes.

La définition des usages doit être clairement établie et c'est grâce à leur spécification que l'on pourra définir l'architecture appropriée, faire le choix des équipements, et mettre en place les mesures de sécurité adéquates.

Nous nous contenterons de rappeler ici les grandes questions qu'il importe de se poser avant toute implantation du Wi-Fi :

- À quels services souhaite-t-on accéder ?
- Quels sont les utilisateurs concernés ?
- Avec quels équipements ?
- Dans quels lieux ?

Pour plus de détails sur cette phase de définition des besoins, le lecteur se reportera au fascicule « Usages et cadre juridique » du présent référentiel.

## 6.3 Appréciation des risques

### 6.3.1 Les risques métiers

Les principaux risques métiers (ou événements redoutés dans la terminologie EBIOS) sont les suivants :

| Risques Métiers | Niveau organisation | Conséquences - Impacts | Gravité |
|---|---|---|---|
| ER0- Divulgation d'informations « sensibles » autres que données à caractère personnel | National<br>Académique<br>EPLE/école | • contentieux avec parents d'élèves, personnel ou usagers. | Limitée |
| ER1- Divulgation de données à caractère personnel | National<br>Académique<br>EPLE/école | • sanctions CNIL pour non-respect des obligations imposées par la loi informatique et liberté ;<br>• contentieux avec parents d'élèves, personnel ou usagers. | Limitée |
| ER2- Usage illicite du réseau de l'EPLE ou de l'école | National<br>Académique<br>EPLE/école | • préjudice causé à des tiers ;<br>• responsabilité du chef d'établissement ou du directeur d'école engagée. | Limitée |
| ER3- Exposition des élèves mineurs à des contenus inappropriés | EPLE/école | • préjudice causé aux élèves ;<br>• contentieux avec parents d'élèves ;<br>• responsabilité du chef d'établissement ou du directeur d'école engagée. | Important |

| Risques Métiers | Niveau organisation | Conséquences - Impacts | Gravité |
|---|---|---|---|
| ER4- Impossibilité d'établir les événements survenus sur le réseau | National<br>Académique<br>EPLE/école | • impossibilité de répondre à une requête judiciaire ou une enquête administrative ;<br>• responsabilité du chef d'établissement ou du directeur d'école engagée. | Limitée |
| ER5- Dysfonctionnement ou impossibilité d'assurer la conduite des enseignements | EPLE/école | • annulation ou report d'un cours | Négligeable à limité |
| ER6- Difficulté ou impossibilité de réaliser un acte administratif ou de gestion | EPLE/école | • Les impacts peuvent être très divers et doivent faire l'objet d'une analyse en fonction de chaque contexte. | Négligeable à limité. Analyse complémentaire requise selon le contexte. |

### 6.3.2 Objectifs de sécurité

Par défaut, le choix de traitement des risques et le suivant :

- acceptation pour les risques négligeables ;
- réduction pour les risques jugés importants.

| Risques métiers | Gravité | Choix de traitement | | | |
|---|---|---|---|---|---|
| | | Acceptation | Évitement | Réduction | Transfert |
| ER0- Divulgation d'informations « sensibles » autres que données à caractère personnel | Limitée | | | X | |
| ER1- Divulgation de données à caractère personnel | Limitée | | X | (X) | |
| ER2- Usage illicite du réseau de l'EPLE ou de l'école | Limitée | | (X) | X | |
| ER3- Exposition des élèves mineurs à des contenus inappropriés | Important | | | X | |
| ER4- Impossibilité d'établir les événements survenus sur le réseau | Limitée | X | | (X) | |
| ER5- Dysfonctionnement ou impossibilité d'assurer la conduite des enseignements | Négligeable à limité | X | | (X) | |
| ER6- Difficulté ou impossibilité de réaliser un acte administratif ou de gestion | Négligeable à limité | X | | (X) | |

Légende et définitions :

- X choix de traitement principal ;
- (X) choix de traitement secondaire.

**Acceptation** : traitement consistant à assumer les conséquences sans prendre de mesure de sécurité supplémentaire.
**Évitement** : traitement consistant à éviter la situation à risque (abandon ou changement de contexte).
**Réduction** : prise de mesures diminuant l'impact et/ou la probabilité de l'événement redouté.
**Transfert** : traitement consistant à partager tout ou partie des pertes occasionnées par un sinistre, voire à en faire assumer la responsabilité par un tiers.

## 6.4 Recommandations

Les recommandations de la présente note s'appuient sur celles que L'ANSSI publie dans son document [Réf. 1]. Elles préconisent en particulier :

- de ne pas utiliser le Wi-Fi pour faire transiter des informations sensibles à caractère confidentiel ou sinon d'utiliser des moyens de chiffrement supplémentaire (IPSEC, TLS par exemple);
- dans tous les cas de définir une politique de sécurité pour la mise en œuvre d'un réseau Wi-Fi. Cette politique doit être ajustée le plus précisément possible, à l'issue d'une analyse de risques, afin de bien identifier les objectifs de sécurité à satisfaire et de lister les mesures de sécurité qui en découlent. Qu'elles soient techniques et/ou organisationnelles, elles ne doivent pas imposer des contraintes irréalistes pour les utilisateurs qui motiveraient ces derniers à les contourner. Dans tous les cas, la mise en place du Wi-Fi pouvant être une vulnérabilité majeure au niveau du système d'information de l'organisme, cette politique doit être validée au plus haut niveau de l'organisme par une autorité en mesure d'assumer les risques résiduels ;
- d'appliquer 23 recommandations afin de conserver la maîtrise et le bon usage des réseaux Wi-Fi. Lorsque les points d'accès, les terminaux et plus généralement les systèmes d'information utilisés le permettent, ces recommandations doivent être imposées techniquement. Cela concerne notamment les aspects d'authentification, de protection cryptographique et de mise à jour des terminaux.

En fonction du contexte et des enjeux qui sont fonction du risque et de leur potentialité, ces 23 recommandations ne sont pas toutes applicables ou justifiées. Le tableau ci-après justifie l'application de ces recommandations en fonction des risques et du type d'utilisation.

Dans le tableau ci-dessous les recommandations sont explicitées en fonction des différents contextes recensés précédemment et des risques.

Note : dans ce tableau, « (CTX) » signifie que l'application de la recommandation est fonction du contexte.

| Recommandations ANSSI | | Applicable | Risques | Observations |
|---|---|---|---|---|
| R1 | N'activer l'interface Wi-Fi que lorsqu'elle celle-ci doit être utilisée. | OUI | ER2 | Définir les plages horaires de connexion possibles. |
| R2 | Afin de garder le contrôle sur la connectivité du terminal, désactiver systématiquement l'association automatique aux points d'accès Wi-Fi configurés dans le terminal. | NON<br>(CTX) | | Non recommandé dans le cadre pédagogique |
| R3 | Maintenir le système d'exploitation et les pilotes Wi-Fi du terminal en permanence à jour des correctifs de sécurité. | OUI | ER0, ER1, ER4, ER5, ER6 | Organiser la mise à jour des terminaux dépendant de l'organisation. |
| R4 | Éviter tant que possible de se connecter à des réseaux sans fil inconnus ou qui ne sont pas de confiance. | OUI | ER0, ER1, ER3 | Des dispositifs sont à implanter sur les terminaux pour bloquer ces possibilités. Il ne doit pas être possible sur un terminal mis à disposition de l'élève de se connecter à un réseau Wi-Fi hors de contrôle.<br>Cette remarque s'applique également au personnel de l'éducation. |
| R5 | Bloquer, par configuration du pare-feu local, les connexions entrantes via l'interface Wi-Fi. | OUI | ER0, ER1 | Des dispositifs de pare feu local sont à implanter dans les terminaux. |

| Recommandations ANSSI | | Applicable | Risques | Observations |
|---|---|---|---|---|
| R6 | Respecter la politique de sécurité de l'entité, en particulier s'agissant des moyens cryptographiques d'authentification ainsi que de protection en confidentialité et en intégrité qui doivent être mis en œuvre. | OUI | ER0, ER1, ER3 | Mettre en place des chartes. |
| R7. | Ne pas brancher de bornes Wi-Fi personnelles sur le réseau de l'entité | OUI | ER0-ER6 | Mettre en place des chartes.<br><br>Pas d'obligation générale pour le responsable de contrôle des Wi-Fi sauvages |
| R8 | En situation de mobilité, lors de toute connexion à des points d'accès Wi-Fi qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport), préalablement à tout échange de données, utiliser systématiquement des moyens de sécurité complémentaires (VPN IPsec par exemple). | NON | | Recommandations à rappeler dans le cadre d'utilisation de personne nomade |
| R9. | Plus largement, lorsque des données sensibles doivent être véhiculées via un réseau Wi-Fi, l'utilisation d'un protocole de sécurité spécifique, tel que TLS ou IPsec, doit être mis en œuvre | OUI | ER0, ER1 | L'ANSSI a publié des recommandations de sécurité relatives à IPSec 2 qu'il convient de suivre pour une mise en œuvre sécurisée de ce protocole.<br><br>Voir également les recommandations du pôle réseaux |

| Recommandations ANSSI | | Applicable | Risques | Observations |
|---|---|---|---|---|
| R10 | Configurer le point d'accès pour utiliser un chiffrement robuste. le mode WPA2 avec l'algorithme de chiffrement AES-CCMP est fortement recommandé. Pour les points d'accès personnels, utiliser le mode d'authentification WPA-PSK (WPA-Personnel) avec un mot de passe **long** (une vingtaine de caractères par exemple) et complexe, d'autant plus que ce dernier est enregistré et n'a pas besoin d'être mémorisé par l'utilisateur. | OUI | ER0, ER1, ER2 | L'utilisation d'un mot de passe faible peut réduire à néant la sécurité du réseau Wi-Fi. La notion de complexité d'un mot de passe est abordée dans les recommandations de sécurité relatives aux mots de passe de l'ANSSI. |
| R11 | Lorsque l'accès au réseau Wi-Fi n'est protégé que par un mot de passe (WPA-PSK), il est primordial de changer régulièrement ce dernier mais également de contrôler sa diffusion. En particulier, il convient de :<br>• ne pas communiquer le mot de passe à des tiers non autorisés (prestataires de services par exemple);<br>• ne pas écrire le mot de passe sur un support qui pourrait être vu par un tiers non autorisé;<br>• changer le mot de passe régulièrement et lorsqu'il a été compromis. | OUI<br>(CTX) | ER0, ER1, ER2 | Envisager un SSID avec un mot de passe différent et changé régulièrement pour les prestataires. |

| Recommandations ANSSI | | Applicable | Risques | Observations |
|---|---|---|---|---|
| R12. | Pour les réseaux Wi-Fi en environnement professionnel, mettre en œuvre WPA2 avec une infrastructure d'authentification centralisée en s'appuyant sur WPA-Entreprise (standard 802.1X et protocole EAP), ainsi que des méthodes d'authentification robustes | OUI<br><br>(CTX) | ER0, ER1, ER2 | Note : Un abonné à un réseau Wi-Fi protégé par WPA-PSK peut très simplement intercepter les données échangées par un autre abonné de ce même réseau. L'utilisation de WPA-PSK ne permet donc pas de garantir la confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi.<br><br>En environnement professionnel, EAP reste alors à privilégier. Différentes méthodes d'authentification basées sur le protocole EAP peuvent être utilisées, mais certaines sont à éviter car elles peuvent présenter des vulnérabilités.<br><br>Parmi les méthodes d'authentification EAP les plus robustes associées au label, WPA-Entreprise, EAP-TLS est à privilégier. Elle exige toutefois une Infrastructure de Gestion de Clés (IGC), avec clé privée et certificat à déployer auprès de chaque utilisateur.<br><br>Lorsqu'EAP est utilisé, il convient par ailleurs que les clients vérifient l'authenticité du serveur d'authentification. |
| R13. | Configurer le Private VLAN invité en mode Isolated lorsque que le point d'accès Wi-Fi prend en charge cette fonctionnalité | OUI<br><br>(CTX) | ER0, ER1, ER2 | Note : La fonction de Private VLAN contribue à la protection en confidentialité des flux entre terminaux connectés à un même réseau Wi-Fi. |

| Recommandations ANSSI | | Applicable | Risques | Observations |
|---|---|---|---|---|
| R14 | Ne pas conserver un nom de réseau (SSID) générique et proposé par défaut. Le SSID retenu ne doit pas être trop explicite par rapport à une activité professionnelle ou une information personnelle. | OUI | ER2 | désactiver la diffusion du nom SSID car conserver un SSID par défaut peut fortement réduire la sécurité d'un réseau Wi-Fi en mode WPA-PSK. |
| R15 | Désactiver systématiquement la fonction WPS (Wi-Fi Protected Setup) des points d'accès. | OUI<br><br>(CTX) | ER2 | Note : WPS simplifie l'authentification d'un terminal sur un réseau WPA2 (par code PIN par exemple) mais réintroduit une vulnérabilité importante qui en réduit fortement l'intérêt du point de vue de la sécurité |

| Recommandations ANSSI | | Applicable | Risques | Observations |
|---|---|---|---|---|
| R16 | Sécuriser l'administration du point d'accès Wi-Fi, en :<br>a. utilisant des protocoles d'administration sécurisés (HTTPS par exemple);<br>b. connectant l'interface d'administration à un réseau filaire d'administration sécurisé, a minima en y empêchant l'accès aux utilisateurs Wi-Fi;<br>utilisant des mots de passe d'administration robustes | OUI | ER2 | |
| R17 | Configurer le point d'accès pour que les évènements de sécurité puissent être supervisés.<br>En environnement professionnel, il est préférable de rediriger l'ensemble des évènements générés par les points d'accès vers une infrastructure centrale de supervision | OUI | ER2 | |
| R18 | Maintenir le microgiciel des points d'accès à jour. | OUI | ER0-ER2, ER4 | Organiser le suivi des mises à jour. |
| R19 | Ne jamais sous-estimer la zone de couverture d'un réseau Wi-Fi. Ne jamais penser être à l'abri de tout risque du fait de l'isolement géographique du point d'accès Wi-Fi. | OUI | ER0-ER2 | |

| Recommandations ANSSI | | Applicable | Risques | Observations |
|---|---|---|---|---|
| R20 | En environnement professionnel, isoler le réseau Wi-Fi du réseau filaire et mettre en place des équipements de filtrage réseau permettant l'application de règles strictes et en adéquation avec les objectifs de sécurité de l'organisme. Comme pour le point d'accès, l'équipement de filtrage doit être paramétré pour que puissent être supervisés les évènements de sécurité. | OUI | ER0-ER6 | Cela ne signifie pas qu'ils soient nécessairement étanches, non communicants et dotés d'accès indépendants à internet.<br><br>Le niveau d'isolation souhaité s'obtient alors en interposant des équipements de sécurité entre les équipements Wi-Fi et le réseau filaire de l'EPLE ou de l'école. |
| R21 | Si un réseau Wi-Fi "visiteurs" doit être mis en place, il est recommandé de déployer une infrastructure dédiée à cet usage, isolée des autres et ne donnant accès à aucune ressource du réseau interne. Ce réseau doit par ailleurs avoir sa propre politique de sécurité beaucoup plus restrictive. | PARTIELLEMENT | ER2 | Les visiteurs d'un EPLE ou d'une école, qu'ils fassent partie de la communauté éducative, de la collectivité territoriale ou des prestataires, peuvent avoir besoin de certaines ressources du réseau interne, notamment des ressources d'impression.<br>Dans le cas ou cet accès leur est accordé on veillera à le restreindre aux seuls équipements concernés. |
| **En environnement Active Directory** | | | | |
| R22**:** Mettre en œuvre les GPO nécessaires à l'application de stratégies de sécurité verrouillant les configurations Wi-Fi des postes clients Windows, de manière à appliquer techniquement différentes recommandations indiquées dans ce document | | OUI<br><br>(CTX) | | |

| Recommandations ANSSI | Applicable | Risques | Observations |
|---|---|---|---|
| R23 Afin de ne pas les communiquer aux utilisateurs, déployer sur les postes Windows les informations de connexion au Wi-Fi par GPO (nom de réseau, clé d'accès, certificats éventuels si la méthode EAP le nécessite, etc.). | OUI<br><br>(CTX) | | |

## 6.5 Architecture de sécurité dans les réseaux

### 6.5.1 Segmentation et confinement

Le nombre d'utilisateurs amenés à utiliser le réseau Wi-Fi depuis des postes nomades (ordinateurs portables, tablettes, smartphones), dans le cadre de la pédagogie dans les établissements scolaires et les écoles est en constante augmentation. Cette tendance pose des problèmes de sécurité de l'information. Le réseau Wi-Fi étant destiné à faire circuler les mêmes informations sensibles que les réseaux filaires, il est indispensable de s'assurer qu'il ne constitue pas un maillon faible de l'infrastructure systèmes et réseaux.

Pour limiter au mieux les impacts aux niveaux de nos systèmes d'information il est nécessaire de mettre en place des processus organisationnels et techniques permettant d'une part d'informer les utilisateurs et d'autre part de fournir une infrastructure fiable et performante.

Nous allons voir dans cette section les différentes possibilités, en termes d'architecture réseau, pour sécuriser au mieux les accès aux services numériques à travers le réseau sans fil.

Les services accédés peuvent se regrouper en trois grandes familles, selon leur localisation :

- services en ligne sur Internet
- services sur le réseau local de l'EPLE ou de l'école
- services numériques sur le réseau Racine

Dans tous les cas de figure les architectures proposées ne visent pas à restreindre l'utilisation pédagogique mais plutôt à faciliter les usages, tout en définissant des contrôles d'accès entre les segments de réseaux et en diminuant le nombre de services et/ou de machines visibles sur le réseau local.

La segmentation des réseaux en académie est formalisée par les recommandations « Pascal » qui ne sont pas forcément retraduites dans les établissements scolaires (EPLE) et les écoles. En tout état de cause, en EPLE, aucun point d'accès Wi-Fi ne doit être installé sur le réseau RACINE-AGRIATES.

Pour autant la sécurité d'une infrastructure sans fil repose avant tout sur une architecture segmentée aux niveaux 2 et 3 permettant l'introduction d'une politique de filtrage pertinente avec d'un côté, un segment dit « Wi-Fi » et de l'autre côté des segments abritant le réseau filaire de l'établissement ou de l'école.

La segmentation de l'architecture est nécessaire pour se prémunir contre les attaques réseau ou la propagation des virus et des vers.

La politique de filtrage sur le segment « Wi-Fi » doit être particulièrement restrictive.

**CE QU'IL FAUT RETENIR**

- **En EPLE, aucun point d'accès Wi-Fi ne doit être installé sur le réseau RACINE-AGRIATES.**

### 6.5.2 Avantages et inconvénients d'une solution basée sur un portail captif

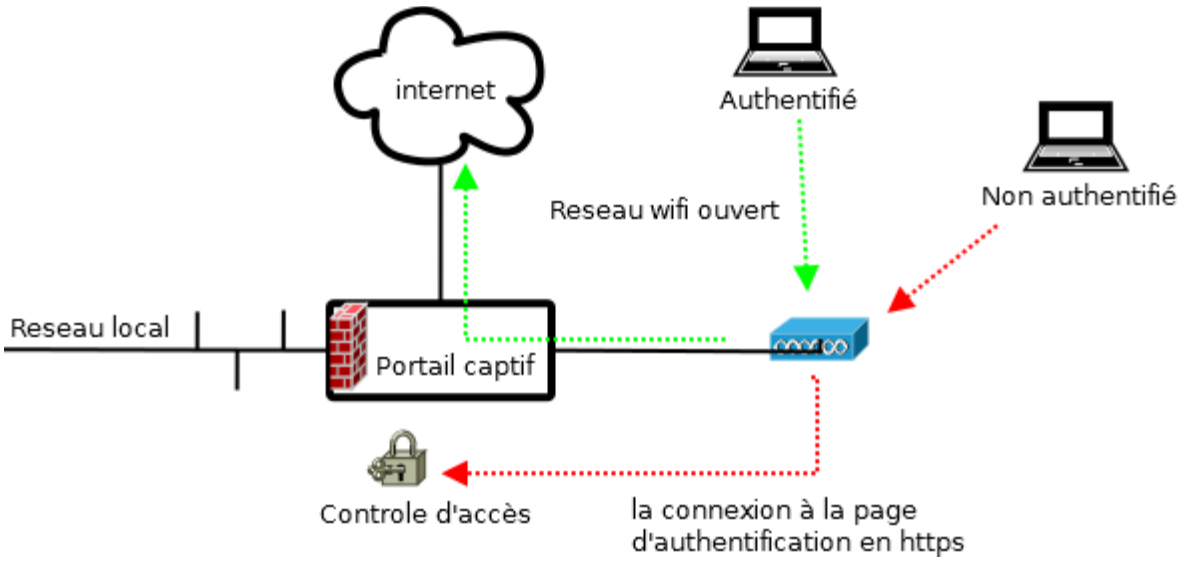
Pour contrôler l'accès des utilisateurs associés à un réseau Wi-Fi semi-ouvert, une solution est de le coupler à une passerelle d'authentification (portail captif) entre le réseau sans fil et le réseau externe.

Utilisés à l'origine par les opérateurs souhaitant déployer des réseaux d'accès publics à Internet par Wi-Fi, les systèmes basés sur un portail captif proposent une authentification à une application Web d'enregistrement, la mise en place autorisations pour l'accès au réseau et le suivi des clients enregistrés.

Les avantages prêtés à une telle architecture sont sa simplicité de gestion pour l'administrateur et d'utilisation pour l'utilisateur qui n'a besoin que d'un navigateur pour se connecter. Cependant l'absence de chiffrement du trafic fait que cette architecture manque de fiabilité et que les menaces pesant sur les utilisateurs conduisent à une limitation des usages autorisés.

**Principe :**

Le réseau wifi est ouvert et isolé. Il permet l'association aux points d'accès sans authentification ni chiffrement de n'importe quel équipement.




Phase 1 : Un dispositif en coupure filtre tous les flux pour interdire tout trafic sortant et redirige le trafic http sur une application web d'authentification.

Phase 2 : Une fois que son identité est vérifiée, le client est enregistré et l'accès à certains services est autorisé (typiquement http, https, smtps, pops imaps).

**Avantages**

Le principal avantage d'un portail captif est sa facilité d'utilisation.

Il permet de gérer les visiteurs sans avoir à les inscrire dans l'annuaire de l'établissement.

**Inconvénients**

Les portails captifs posent généralement des problèmes de sécurité à plusieurs niveaux :

- Du fait de l'absence de 802.1X, le contenu des requêtes d'authentification n'est pas sécurisé. Le risque d'espionnage du flux d'authentification est assez important. Depuis n'importe quelle borne sans fil ou prise réseau, une personne malveillante peut capter la majorité de ces flux réseaux. La compromission de la machine supportant le portail exposerait les données d'authentification des utilisateurs.
- Le lien radio n'étant pas protégé, le trafic des utilisateurs peut être espionné par tous ceux qui sont dans la zone de couverture du point d'accès (voire plus).
- Outre l'interception des données (éventuellement sensibles), des attaques de type « MITM » sont possibles, permettant le vol de session, voire celui des identifiants confidentiels des usagers.

Précautions

La liste de précautions suivante est donnée à titre indicatif et ne permet pas de pallier les faiblesses originelles des réseaux semi-ouverts :

- Les utilisateurs devraient être clairement informés du caractère non sécurisé du réseau dès la page de connexion.
- Il devrait leur être recommandé de recourir de préférence à des protocoles de messagerie sécurisés (pops, imaps, smtps).
- Le nombre de ports de sortie devrait être réduit au strict nécessaire (notamment dns, icmp, http, https, smtps, imaps, pops) et aux protocoles standard chiffrant les données (ssl, ipsec, tls).
- Les certificats utilisés par l'application d'enregistrement devraient être reconnus dans les navigateurs.

# 7 Glossaire des termes

| Acronyme | Définition |
|---|---|
| AFSSET | Agence Française de Sécurité Sanitaire de l'Environnement et du Travail |
| ANSES | Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail |
| ANSSI | Agence Nationale de la Sécurité des Systèmes d'Information |
| AP | Access Point (Point d'accès) |
| ARCEP | Autorité de Régulation des Communications Electroniques et de la Poste |
| ATSS | personnel Administratifs, Techniques, Sociaux et de Santé |
| BYOD | Bring your Own Device |
| EAP | Extensible Authentication Protocol |
| LDAP | Lightweight Directory Access Protocol |
| PIRE | Puissance isotrope rayonnée équivalente |
| TLS | Transport Layer Security |