Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ministère éducation nationale enseignement supérieur recherche

**Direction des personnels, de la modernisation et de l'administration**

**Service du pilotage des services académiques et de la modernisation**

**Sous-direction du pilotage de l'informatique**

**Bureau des études techniques et des plans d'informatisation**

DPMA A3/MB
n° 2006-0077
Affaire suivie par
Mahfoud Baradi
Téléphone
01 55 55 36 87
Fax
01 55 55 08 87
Mél.
Mahfoud.baradi
@education.gouv.fr

61-65 rue Dutot
75015 Paris 015 SP

Paris le 18 MAI 2006

Le ministre de l'éducation nationale, de l'enseignement supérieur et de la recherche

à

Mesdames et messieurs
les rectrices et recteurs d'académie

Mesdames et messieurs
les inspectrices et inspecteurs d'académie

**Objet :** Mise en œuvre de bornes WIFI ouvrant des accès aux ressources internes[1] du système d'information.

Mes services sont régulièrement interrogés sur les conditions de mise en œuvre du WIFI (Wireless Fidelity) sur les infrastructures académiques (services et établissements scolaires). Il est bien évident que ces dispositifs qui réduisent notamment les contraintes de câblage des bâtiments, doivent pouvoir se déployer dans les sites de l'éducation nationale au plus grand profit de l'efficacité de l'action administrative et éducative.

Cependant, au regard des risques inhérents à cette technologie, la mise en œuvre doit s'effectuer dans des conditions de sécurité adaptées à l'accès aux ressources internes du système d'information, ouvertes sur les réseaux RACINE et AGRIATES (cercles de confiance Intranet inter académique et Intranet académique).

Vous trouverez ci-dessous les principes de déploiement du WIFI dans ce contexte.

## 1 - Obligation de signalement de la mise en place d'une borne WIFI

Toute mise en place d'une borne WIFI susceptible d'ouvrir des accès aux ressources internes du système d'information académique **devra faire l'objet d'un signalement préalable à l'ingénieur de sécurité RACINE (ISR)** auquel il appartiendra, en liaison avec le responsable de la sécurité des systèmes d'information académique (RSSI), de vérifier ou de contrôler que la mise en service s'effectue dans les conditions de sécurité requises.

## 2 - le confinement des accès WIFI

Les bornes d'accès WIFI doivent impérativement être confinées sur une zone du réseau local qui sera isolée de toutes autres ressources sensibles par un dispositif de sécurité de type pare-feu ou équivalent. La gestion des règles de sécurité sur cet équipement devra être contrôlée par l'ingénieur de sécurité RACINE (ISR)[2].

---

[1] Ouvertes aux personnels de l'éducation nationale ou ayant droits dûment habilités

[2] En coordination avec le responsable de la sécurité des systèmes d'information académique (RSSI)

De façon générale, chaque borne devra être dédiée à des personnes ayant le même niveau d'habilitation.

**3 - Authentification des postes de travail et des utilisateurs**

Toute borne WIFI ouvrant des accès aux ressources internes du système d'information du service ou de l'établissement devra permettre une authentification du poste de travail (et, dans la mesure du possible, de l'utilisateur) ainsi qu'un chiffrement des échanges.

Pour ce faire, il sera privilégié les bornes intégrant les protocoles 802.11i / WPA 2 (ou versions plus évoluées) associés à une authentification de l'utilisateur de type EAP / RADIUS.

**4 - Fourniture éventuelle d'un service d'accès de type HotSpot**

Pour toute borne n'intégrant pas de dispositif d'authentification et de chiffrement, l'accès WIFI proposé s'apparente à un accès de type HotSpot (borne d'accès public WIFI).
Dans ce cas de figure, notamment si cet accès s'ouvre sur l'Internet, la personne juridiquement responsable (PJR) du service ou de l'établissement est soumise aux mêmes obligations que les fournisseurs d'accès Internet (FAI). Il convient donc de bien prendre en compte l'ensemble des éléments juridiques avant ouverture de ce type d'accès. Vous trouverez en annexe 1 une note de synthèse réalisée dans le cadre de l'assistance juridique[3] souscrite par mes services conformément aux orientations du schéma directeur de la sécurité (SDSSI)

Ces dispositifs sont généralement mis en place pour couvrir les besoins de personnes non reconnues par la gestion d'identité mise en œuvre au niveau de l'établissement ou du service. La sécurité de tels dispositifs pourra être avantageusement renforcée par l'attribution d'un compte d'accès limité et temporaire.

**5 - Les modalités d'accès aux ressources internes du système d'information**

- ✓ **L'accès aux ressources intranet ouvertes sur les réseaux RACINE (applications de gestion…)**

L'accès aux ressources sensibles devra se faire au travers d'une procédure permettant de reconnaître en toute confiance l'utilisateur final.

L'authentification forte, telle que la mise en œuvre dans le cadre de RACINE-API (accès poste isolé) au travers d'un support cryptographique de chiffrement et de signature électronique, offrira le niveau de sécurité le plus élevé.

**Cependant, il est de la responsabilité de l'ISR (ingénieur sécurité RACINE)[2] de proposer, à la personne juridiquement responsable (PJR) du site, la solution qu'il jugera adaptée aux besoins et au contexte. L'ISR accompagnera la mise en place de la solution en prenant le soin d'en vérifier l'efficacité au cas par cas.**

---

[3] Qui peut être (pour rappel) sollicitée à tout moment par le RSSI académique

✓ **L'accès aux ressources extranet (messagerie ...)**

L'accès aux ressources extranet est réalisé dans les mêmes conditions de sécurité que celles appliquées sur RACINE pour un usager provenant d'Internet. L'authentification de l'utilisateur, s'il y a lieu, est prise en charge directement au niveau de la ressource (application, équipement de concentration ...).

*
* *

Je vous saurais gré de bien vouloir porter ces consignes à la connaissance des responsables des services ou des établissements mis sous votre responsabilité.

Les pôles de compétences réseau (académie de Clermont-Ferrand) et sécurité des systèmes d'information (académie d'Aix-Marseille) pourront accompagner vos équipes pour la mise en œuvre.

Mes collaborateurs restent à votre disposition pour de plus amples informations.

Pour le ministre et par délégation :
le directeur des personnels, de la modernisation
et de l'administration

Dominique ANTOINE

**PJ :** Annexe 1- Recommandations juridiques relatives à l'implémentation de bornes Wi-Fi
Annexe 2 - Recommandations techniques de mise en œuvre du Wi-Fi (pôle de compétences réseaux de l'académie de Clermont-Ferrand)
Annexe 3 - Recommandations de sécurité en matière de déploiement des Wi-Fi (pôle national de compétences sécurité d'Aix-Marseille)

**CPI :** Pôle national de compétences réseau de Clermont-Ferrand
Pôle national de compétences sécurité des SI d'Aix-Marseille
SDTICE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

# Annexes Techniques WI-FI

**Annexe 1 - Recommandations juridiques relatives à l'implémentation de bornes Wi-Fi**

**Annexe 2 - Recommandations techniques de mise en œuvre du Wi-Fi (pôle de compétences réseaux de l'académie de Clermont-Ferrand)**

**Annexe 3 - Recommandations de sécurité en matière de déploiement des Wi-Fi (pôle national de compétences sécurité d'Aix-Marseille)**

ANNEXE 1 :

# MINISTERE DE L'EDUCATION NATIONALE

# ACCES WI-FI ET RESPONSABILITES

## RESPONSABILITES D'UN SERVICE OU D'UN ETABLISSEMENT DANS LE CADRE DE LA MISE EN PLACE D'UN RESEAU WI-FI

NOTE de synthèse

11 avril 2006

ALAIN BENSOUSSAN

## NOTE SYNTHETIQUE :

Deux axes de réflexion nécessitent d'être soulevés pour répondre aux problématiques de responsabilités en matière d'infrastructures Wi-Fi à savoir, d'une part, le contenu transitant sur le réseau en tant que sources de responsabilité et d'autre part, l'infrastructure réseau.

### 1 Le contenu transitant sur le réseau

Pour permettre d'appréhender les problématiques de responsabilité des personnes juridiquement responsables (PJR) qui installent un réseau Wi-Fi connecté à l'Internet au sein de leur service ou établissement, il est important de savoir pour quelle personne l'usage de ce réseau est autorisé.

En effet, le réseau peut est réservé soit à une catégorie identifiée de personnes (groupe fermé d'utilisateurs = réseau indépendant) soit au contraire ouvert à tous ce qui n'implique pas nécessairement le même niveau de responsabilité.

La responsabilité sera ainsi susceptible de varier entre notamment une responsabilité identique à celle d'un professionnel de l'Internet (application de la loi pour la confiance dans l'économie numérique) ou d'un opérateur télécommunications (application de la loi du 9 juillet 2004).

Quoi qu'il en soit, différents risques peuvent d'ores et déjà être identifiés à savoir :

- le secret des correspondances ;
- certaines infractions dont notamment une atteinte aux Systèmes de Traitement Automatisé de Données (STAD)

#### 1.1 Le secret des correspondances

Un réseau Wi-Fi permet à la fois la transmission de contenus destinés à de la correspondance privée ou publique. Or la correspondance est une composante de la personnalité et certains principes visent à garantir la liberté de communication dont notamment le secret des correspondances.

Depuis 1991 ((Loi du 10/07/1991) le principe du secret des correspondances englobe la correspondance émise par la voie électronique dès lors qu'elle est privée.

Or sur un réseau radioélectrique de type Wi-Fi, l'accès aux échanges est facilitée du fait même de la technologie utilisée (ondes radioélectriques) ce qui rend plus facile l'interception des informations par un tiers non identifié.

Il est donc nécessaire de sécuriser le réseau déployé sous peine éventuellement de voir la responsabilité du service ou de l'établissement engagée pour négligence.

Pour rappel, l'auteur de la violation est puni d'un an d'emprisonnement et de 45 000 € d'amende.

Il n'est pas exclu, à titre d'exemple, qu'une personne estimant que ses correspondances aient été détournées, utilisées, ne vienne pas rechercher la responsabilité de la PJR pour ne pas avoir mis en œuvre des procédés de sécurisation adéquat sur le réseau déployé.

### 1.2 Les infractions informatiques classiques

En raison de la technologie utilisée et **dans l'hypothèse d'une absence de sécurisation du réseau les risques d'infraction se trouvent accrus.**

Une personne malveillante pourrait ainsi s'introduire sur le poste de l'utilisateur et sur le Système d'Information du service ou de l'établissement pour modifier, détruire, voler des données.

Sans rentrer dans une liste exhaustive des risques liés au déploiement d'un réseau Wi-Fi non sécurisé et qui pourrait entraîner la responsabilité d'un service ou établissement notamment par négligence. Il est cité ci-après quelques infractions courantes avec les sanctions associées :

- Atteinte volontaire au fonctionnement d'un STAD (entrave, altération du fonctionnement, virus …) : 5 ans de prison et 75 000 € d'amende
- Atteinte volontaire aux données 5 ans de prison et 75 000 € d'amende

### 1.3 Les autres risques identifiés

Outre les atteintes à l'intégrité des données de type correspondance privée ou publique circulant sur le réseau, l'accès à l'Internet depuis le réseau Wi-Fi du service ou de l'établissement permet divers actes répréhensibles à l'intérieur de la structure qui pourrait engager la responsabilité de la PJR (ex : tenue de propos raciste, accès à des sites pornographique pour des mineurs, actes de terrorisme …).

Sans même évoquer d'actes répréhensibles, il n'est pas exclu qu'un utilisateur du réseau Wi-Fi puisse divulguer, et sans que ce dernier soit de mauvaise foi, des informations confidentielles ou non du Ministère.

A cet égard, le service ou l'établissement devra réfléchir à la mise en place de divers outils pour limiter sa responsabilité. **A cet effet, et pour minimiser sa responsabilité des conditions générales d'utilisation pourraient s'avérer utiles de même que la généralisation de login password pour tracer l'utilisation des services sur le réseau**.

S'agissant des parties concernées, outre l'installateur du réseau, du FAI et celle du service ou de l'établissement, il ne faut pas négliger la responsabilité éventuelle du ministère qui autorise la mise en place de ce type de réseau. Celle-ci pourrait être d'autant plus grande si ce dernier entendait relier l'ensemble des services et établissements via cette technologie.

## 2 L'Infrastructure réseau

Trois points peuvent être abordés en terme de responsabilité.

### 2.1 Les conditions d'établissement

A titre liminaire, la mise en place d'un réseau Wi-Fi au sein d'un établissement scolaire ne nécessite aucune déclaration auprès de l'ARCEP (autorité de régulation des postes et communications électroniques) puisque dans cette hypothèse le réseau est qualifié de réseau interne.

A l'inverse si l'objectif poursuivi est de relier plusieurs services ou établissements, le réseau est alors qualifié de réseau indépendant et nécessite une déclaration. Le défaut de déclaration est sanctionné par une amende de 75 000 € et un an d'emprisonnement.

### 2.2 Intégrité des personnes

Même s'il existe peu de risque à priori sur la santé publique, puisque les antennes Wi-Fi rayonnent avec une puissance maximale de 100 mW très inférieure par exemple aux antennes GSM, un principe d'attention a été retenu par l'AFSSE (agence française de sécurité sanitaire environnementale). Ce principe d'attention vise à prendre en compte les préoccupations des personnes en déclinant toute une série de mesures portant à l'attention de ces dernières certains éléments (notamment le niveau d'exposition aux ondes).

Par ailleurs, il est toujours à craindre que l'installation en elle même soit faite de façon artisanale et donc susceptible de créer un préjudice physique corporel (ex : chute d'antenne, installation électrique défectueuse).

La responsabilité pénale de l'établissement ou du service pourrait donc être recherchée.

### 2.3 Perturbations

Il existe des risques de « perturbations » avec d'autres installations du fait de l'installation d'un hot spot Wi-Fi.

Il pourrait donc dès lors être reproché au service ou à l'établissement scolaire d'avoir perturbé les équipements existants d'un autre opérateur. Un risque de désinstallation des équipements n'est pas exclu et nécessite de prévoir des engagements forts avec un installateur pour éviter toute action d'un autre opérateur pour des problèmes de compatibilité électromagnétique. En cas d'incompatibilité et nuisance, une éventuelle action de l'opérateur pour la réparation des dommages directs est possible.

Une réflexion générale pourrait donc être instruite pour savoir s'il n'est pas nécessaire de disposer d'une architecture technique cohérente au sein des services et établissements scolaires, de conditions d'utilisation applicables pour tous les établissements quels qu'ils soient.

* *

*

ministère éducation nationale enseignement supérieur recherche

Pôle National de Compétences Réseaux

# Annexe 2 :
# Recommandations techniques Wi-Fi au sein de l'Education Nationale

| | | |
|---|---|---|
| Rédacteur : | Gilles Chaideyrou<br>Jean-Philippe Feugnet | Date et signatures |
| Approuvé par : | DSR - Bureau DPMA/A3<br>Michel Affre<br>Mahfoud Baradi | Date et signature |

# Suivi des versions

| Version | Date | Rédacteur(s) | Nature de la modification | Lecteur(s) | Validation DSR |
|---|---|---|---|---|---|
| 1.0 | 10/04/2006 | J-Ph. Feugnet, Th. Chich | Première diffusion | M. Baradi, G. Chaideyrou, pôle d'Aix-Marseille, groupe RACINE. | |

# Table des matières

# Préambule

Malgré l'intérêt suscité par le WiFi à ses débuts, le manque de sécurité initial a constitué un frein à son développement dans le cadre d'usages professionnels. Avec les avancées réalisées dans les domaines du chiffrement et de l'authentification, il est maintenant possible d'intégrer des réseaux de type WIFI dans des structures professionnelles sans dégrader les modèles de sécurité. Ces progrès techniques, accompagnés par la mise à mal du "modèle économique" des réseaux WIFI, amènent à une rationalisation progressive de l'utilisation du WiFi.

Il est désormais possible d'ouvrir le réseau de l'éducation nationale au WiFi, sans diminuer son niveau de sécurité. Ce document propose une approche, s'appuyant uniquement sur les contraintes légales et de sécurité, pour définir les réseaux WiFi utilisables en fonction des ressources ou données accédées.

Au préalable, il convient de rappeler certains éléments importants au moment de décider de l'opportunité de construire un réseau WIFI :

- L'intérêt autour du WIFI s'est initialement nourrit des arguments de facilité de déploiement et d'économies financières liées à la suppression du cablage. On a pu imaginer une salle de classe sans fil, sans connectique, où l'élève équipé de son micro-ordinateur portable est directement relié au réseau dès son entrée dans la pièce, sans effort et sans contrainte. En réalité, la nécessité de disposer d'alimentations électriques pour tous les portables ou de dispositifs de charge (de moins en moins efficaces au fur et à mesure que les batteries s'altèrent) limite rapidement la portée de ses arguments. De même les mécanismes de sécurisation nécessaires au déploiement des réseaux WIFI induisent des coûts d'administration et de maintenance qu'il faut mettre en balance avec le coût d'un cablage.
- La nécessité légale pour les personnes juridiquement responsables des établissements de l'éducation nationale de limiter l'utilisation des réseaux aux seules personnes habilitées ainsi que d'assurer la confidentialité d'un certain nombre de traitements, sont des éléments importants. Leur prise en compte induit là aussi des coûts d'administration et de maintenance.
- La nature des communications devant transiter sur le réseau WIFI doit aussi être pris en considération. L'expérience montre que la disponibilité et la qualité d'un réseau Wifi est loin d'être comparable à celle d'un réseau filaire. Le WIFI ne devrait pas être utilisé pour constituer une liaison d'importance vitale ou pour véhiculer des informations pouvant être critiques pour le fonctionnement de la structure.
- Enfin, les interrogations concernant la santé et l'environnement, que nous ne sommes pas compétents pour juger, doivent nécessairement être incluses dans une reflexion globale sur l'opportunité d'installer ou non un réseau WIFI.

Une fois ces différents éléments soigneusement pesés, le document que nous proposons est destiné à faciliter la mise en oeuvre des technologies WiFi dans les deux domaines où son emploi est parfaitement justifié, dès lors qu'on en a accepté et compris les contraintes :

- le traitement de la mobilité,
- l'interconnexion de structures au moyen de liaisons wifi.

Sur un réseau maillé comme celui de l'éducation nationale, intégrer le WiFi ne peut pas se faire en ignorant les contraintes de sécurité. Ce document tente d'aider l'ISR et tout responsable confronté à la mise en oeuvre d'un réseau WiFi, à choisir le niveau de sécurité à mettre en oeuvre, donc le type de WiFi à utiliser. Pour cela ce document présente :

- les différents mécanismes de sécurisation des connexions WiFi,
- une nomenclature des types de réseau WiFi en fonctions des mécanismes de sécurisation utilisés,
- les recommandations d'utilisation en fonction des données potentiellement accessibles.

# 1 Les outils de sécurisation du WiFi

Deux mécanismes concourrent à la sécurisation des réseaux WiFi : le chiffrement des communications et l'authentification des machines ou des utilisateurs.

## 1.1 Chiffrement des communications

Le chiffrement des communications est utilisé pour assurer la confidentialité des données qui transitent entre les machines et le point d'accès. Ce n'est un secret pour personne, les communications WiFi sont beaucoup plus facilement écoutables que celles d'un réseau filaire. Si le chiffrement n'est pas utilisé, la sécurité des systèmes et l'intimité des individus se trouvent très fortemenent compromises.
En WIFI, les connexions peuvent être chiffrées ou non, en utilisant une clé secrète partagée ou distribuée. Plus l'algorithme utilisé est résistant à la cryptanalyse, plus la confidentialité des communications est assurée.

### 1.1.1 Clé secrète partagée :

La clé utilisée pour chiffrer les communications est connue de tous les utilisateurs du WiFi. Or, il est illusoire de vouloir préserver un secret partagé par plus de quelques personnes. Il suffit qu'une personne le divulgue, involontairement ou non, pour que la confidentialité des communications soit compromise, quel que soit l'algorithme de chiffrement utilisé, sans qu'il soit même possible de déterminer l'origine de la fuite. De plus tous les utilisateurs utilisant la même clè, il leur est possible de "s'espionner" les uns les autres. Le niveau de sécurité du chiffrement reposant sur une clé partagée est donc très faible.

### 1.1.2 Clé secrète distribuée :

La clé utilisée pour chiffrer les communications est obtenue automatiquement lors de la phase d'authentification. Pour cela il faut utiliser obligatoirement une méthode d'authentification qui génére des clés de chiffrement (c.f. section 1.2.2 page suivante). L'un des apports importants de cette technologie est d'éviter que les utilisateurs n'utilisent la même clé et puissent "s'espionner" les uns les autres.

### 1.1.3 Les algorithmes de chiffrement

Ils sont au nombre de trois : le WEP, le WPA (ou TKIP) et le WPA 2 (ou AES).

**Le WEP :** historiquement le premier, défini par la norme 802.11. Il est fondé sur des méthodes cryptographiques qui étaient déjà connues pour leurs faibles résistances cryptographiques au moment de sa commercialisation. Le seul avantage du WEP est le faible niveau de puissance de traitement nécessaire. Vu le nombre outils disponibles et leurs facilités d'utilisation, n'importe qui peut décrypter les communications chiffrées avec le WEP. Le WEP est aujourd'hui incapable de garantir le secret d'une communication.

**Le WPA (ou TKIP) :** a été créé suite aux multiples failles de WEP et en attente de l'arrivée du WPA 2. Il s'agit de recommandations de la "Wi-Fi Alliance" concernant la mise en oeuvre de quelques mécanismes de la norme 802.11i, en attendant sa version définitive. En simplifiant, on reprend le WEP pour des raisons de compatibilité avec le matériel existant, et l'on lui ajoute le TKIP qui gére les clés de chiffrement et les change tous les 10 Ko de données échangées. Toutes les clés utilisées sont dérivées d'une clé mère. Il existe des failles dont l'exploitation à ce jour est plus difficile que pour le WEP. Les chercheurs sont dans une phase d'optimisation des algos qui ont permis le décryptage. Le résultat des optimisations (c.f. le DES et le WEP) est souvent une diminution des captures et du temps de calcul nécessaires au décryptage. A terme, des clés ou algorythmes réputés sûrs par leur longueur ou complexité le sont moins ou plus du tout.

**Le WPA 2 (ou AES) :** définit par la norme 802.11i. L'algorithme de chiffrement AES est utilisé pour le chiffrement des données et l'échande des clés, en faisant fi de la compatibilité avec le matériel existant[1]. Le contrôle de sécurité de la couche 2 est assuré par CCMP (Counter-mode/CBC-MAC-Protocol) qui utilise lui aussi l'AES. C'est la solution à utiliser pour toute nouvelle installation.

Pour ménager la compatibilité avec les clients WiFi existants, il existe des points d'accès qui permettent d'utiliser simultanément les trois protocoles.

## 1.2 L'authentification

Pour des problèmes de responsabilité légale, il s'agit d'un critère d'importance au moins égale au chiffrement. En fonction des ressources accédées, l'authentification doit assurer que l'utilisateur est légitime et qu'il se connecte au bon réseau. Tant que l'utilisateur n'est pas authentifié, il n'a pas accès au réseau WiFi. Tout comme pour RACINE API, on peut considérer qu'authentifier le poste client revient à authentifier l'utilisateur.

Le protocole EAP a été retenu pour l'authentification du WiFi. Il met en oeuvre deux mécanismes : les méthodes d'authentifications EAP et les méthodes de transport de l'authentification EAP.

### 1.2.1 Les méthodes d'authentification EAP

Les méthodes d'authentification permettent l'authentification de l'utilisateur ou du poste. Elles peuvent se classer en trois catégories :

- basique : login/passwd (par exemple EAP/MD5),
- certificat : l'utilisateur ou le poste possède un certificat,
- certificat "incopiable" : l'utilisateur ou le poste possède un certificat dont la clé privée est stockée sur un support très difficilement copiable.

### 1.2.2 Les méthodes de transport de l'authentification EAP

La robustesse des différentes méthodes d'authentification EAP (c.f. section 1.2.1) n'est pas équivalente. Par exemple la méthode d'authentification basique est très sensible à l'écoute. Ce n'est pas le cas des méthodes basées sur des certificats. En effet ces dernières utilisent des technologies de chiffrement assymétrique, naturellement conçues pour permettre l'authentification sur les liaisons écoutables.

#### Authentification EAP transportée en clair

Initialement EAP est prévu pour une utilisation sur un réseau filaire, sans chiffrement des informations. Cette méthode de transport associée à une méthode EAP basique n'est pas une méthode d'authentification robuste sur un réseau WiFi.

#### Authentification EAP transportée dans un tunnel chiffré :

Afin d'assurer la confidentialité des échanges EAP sur le réseau WiFi, 3 solutions concurrentes sont possibles : EAP/TLS, PEAP ou TTLS. Elles ont en commun d'utiliser un tunnel TLS (successeur de SSL) pour transporter l'authentification EAP. Dans ce document, ces solutions sont donc rassemblées sous la dénomination *TLS. Ces méthodes d'authentifications qui génèrent des clés sont les seules qui permettent d'utiliser le chiffrement par clés secrètes distribuées (c.f. section 1.1.2 page précédente). L'établissement

[1] L'AES est un algorithme de chiffrement qui nécessite une grande puissance de traitement que ne peuvent pas fournir les matériels de première génération conçus uniquement pour le WEP.

des connexions TLS peut être l'occasion d'authentifier les différents intervenants de la connexion (le serveur d'authentification et la machine cliente). Cette vérification optionnelle permet de se protéger contre certaines modalités d'attaques *Man-in-the-Middle*.

**EAP/TLS :**
- décrit dans le RFC 2716
- un certificat par poste client et par serveur d'authentification avec ou sans vérification réciproque des certificats,
- une PKI devient rapidement indispensable pour gérer les certificats,
- ne transporte que des méthodes d'authentification EAP.

**PEAP :**
- proposé par Microsoft, Cisco, RSA,
- certificat uniquement pour le serveur d'authentification avec ou sans vérification du certificat par les postes clients,
- ne transporte que des méthodes d'authentification EAP.

**TTLS :**
- proposé par Funk Software,
- certificat uniquement pour le serveur d'authentification avec ou sans vérification du certificat par les postes clients,
- transporte les méthodes d'authentification EAP mais aussi n'importe qu'elle autre.

### 1.2.3 Quel niveau de confiance accorder à l'authentification ?

La confiance accordée à l'authentification dépend :

- de la méthode d'authentification EAP utilisée (c.f. 1.2.1 page précédente),
- de la méthode de transport utilisée (c.f. 1.2.2 page ci-contre).

Authentifier le serveur d'authentification est impératif si l'on souhaite :

- être sûr que les utilisateurs se connectent au bon serveur d'authentification,
- se protéger contre certaines modalités d'attaques *Man-in-the-Middle*.

Lorsque l'authentification du serveur d'authentification est activée, il faut absolument que le poste utilisateur vérifie le certificat du serveur ET refuse automatiquement la connexion en cas de doute. Il ne faut pas laisser ce choix à l'utilisateur, à l'inverse de ce que font les navigateurs Web avec les certificats des sites en https.

# 2 Types de réseaux WiFi suivant les associations chiffrement et authentification

Le tableau 1 dresse une nomenclature des combinaisons possibles entre chiffrements et authentifications. L'indice obtenu n'indique pas un niveau de sécurité ou de confiance. Il permet juste d'identifier un couple chiffrement/authentification pour réutilisation dans les tableaux 2 page 11 et 3 page 13.
Une nouvelle technologie dans un des deux domaines rajouterait un nouveau numéro.
La découverte d'une nouvelle faille de sécurité protolaire ne changerait pas les indices du tableau 1 mais pourrait entraîner une modification dans les tableaux 2 page 11 et 3 page 13.

Quelques remarques sur le tableau 1 :

- les méthodes ne garantissant pas la confidentialité des communications sont rassemblées dans la ligne "Aucun ou clés partagées ou WEP" : elles sont toutes regroupés sous le même identifiant dans la mesure où elles ont toutes pour caractéristique de ne pas offrir un niveau de confidentialité suffisant. Par exemple, les applications couramment installé dans les zones pédagogiques n'utilisent pas toutes, loin de là, des protocoles de chiffrement au niveau applicatif (https, par exemple). Des login/mot de passe ou des informations personnelles à caractère privé pourraient être encore plus facilement interceptés en WIFI qu'ils ne le sont en filaire ou sous Internet.
- les méthodes d'authentification à faible niveau de confiance sont rassemblées dans la colonne "Aucune ou EAP basique".
- transporter l'authentification basique en clair ou par TLS sans vérification des certificats ne protège pas d'une simple attaque de type Man-in-the-Middle qui permet de récupérer assez simplement et rapidement un grand nombre de couples login/mot de passe. On doit considérer ces méthodes d'authentification comme équivalentes et peu dignes de confiance.

Exemple de lecture du tableau 1 : une installation WiFi utilisant WPA 2 avec authentification par PEAP, un serveur d'authentification avec certificat vérifié par les postes clients et des certificats clients dont la clé privée associée est stockée sur un support cryptographique inviolable sera de type 12.

| Authentification des utilisateurs ou des postes / Chiffrement des communications | Aucune ou EAP basique | EAP-TLS | | | EAP-TLS avec authentification du serveur d'authentification par certificat vérifié | | |
|---|---|---|---|---|---|---|---|
| | | Type d'authentification utilisée | | | Type d'authentification utilisée | | |
| | | Basique | Certificat | Certificat, clé privée inexportable | Basique | Certificat | Certificat, clé privée inexportable |
| Aucun ou clés partagées ou WEP | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| WPA (TKIP) | 2 | 2 | 3 | 4 | 5 | 6 | 7 |
| WPA 2 (AES) | 2 | 2 | 8 | 9 | 10 | 11 | 12 |

TAB. 1 – Nomenclature des types de réseau WiFi

# 3 Les types de réseaux locaux ou zones d'un site RACINE

Les réseaux locaux présents sur un site RACINE sont organisés en différentes zones. Dans le tableau 2 page 11, la dénomination de ces zones reprend celle validée par la DSR et présentée dans le document "Cadre Organique des réseaux RACINE "[2]. Ces dénominations sont reprises ci-après.

**Zone Internet (I) :** La zone I (INTERNET) DOIT être l'unique point d'accès Internet pour le site concerné. A priori la zone I n'héberge aucune ressource.

**Zone Extranet (E) :** c'est la zone de transit de tout utilisateur ou de tout flux hors du périmètre RACINE (arrivant de l'Internet et désirant accéder à des services offerts par le centre de ressources) . Le contrôle des utilisateurs est géré sur cette zone. Elle ne permet l'accès qu'à des ressources d'un périmètre fonctionnel très encadré. Seuls les processus et les données de moindre sensibilité sont accessibles à partir de cette zone.
La zone E ne peut héberger que des ressources de faible sensibilité mises sous la responsabilité exclusive de la personne habilitée par le chef de centre informatique.
La politique de sécurité appliquée à la zone est vérifiée par l'ISR.
La traçabilité des accès aux ressources partagées de la zone est OBLIGATOIRE. Le dispositif DEVRAIT permettre d'identifier l'initiateur (personne ou poste) de la connexion. Les traces DOIVENT être conservées pour une durée de 12 mois.

**Zone de service établissements (A) :** c'est la zone de transit des utilisateurs de postes de travail dont l'usage est exclusivement réservé aux personnels de l'éducation nationale en établissement scolaire (ou ayants droits désignés par le chef d'établissement). Elle permet l'accès à toutes les ressources, quel que soit leur degré de sensibilité, mises à disposition de l'établissement scolaire.
La zone A n'est accessible directement de l'extérieur du centre de ressources qu'au travers d'un réseau RACINE (AGRIATES ou API).
Hormis les équipements de gestion de la sécurité, la zone A ne peut héberger que des ressources, de sensibilité limitée, mises sous la responsabilité exclusive de la personne habilitée par le chef de centre informatique.
La politique de sécurité appliquée à la zone est vérifiée par l'ISR.
La traçabilité des accès aux ressources de la zone est exigée. Le dispositif devrait permettre de mettre en évidence les adresses IP et Ethernet des équipements à l'initiative de la connexion. Les traces doivent être conservées pour une durée de 12 mois.
La zone A ne peut héberger que des ressources mises sous la responsabilité d'une personne désignée par le chef de centre.

**Zone collectivités (C) :** c'est la zone de transit des utilisateurs de postes de travail dont l'usage est exclusivement réservé aux personnels (ou ayants droits désignés par le représentant de la collectivité) de la collectivité agréée sur RACINE par convention signée au niveau académique. Elle permet l'accès à toutes les ressources quel que soit leur degré de sensibilité mises à disposition de la collectivité.
La zone C n'est accessible directement qu'au travers un réseau RACINE (ADRIA-TIC ou API).
La zone C ne peut héberger que des ressources de faible sensibilité mises sous la responsabilité exclusive de la personne habilitée par le chef de centre informatique.
La politique de sécurité appliquée à la zone est vérifiée par l'ISR.
La traçabilité des accès aux ressources de la zone est EXIGEE. Le dispositif DEVRAIT permettre de mettre en évidence les adresses IP et ETHERNET des équipements à l'initiative de la connexion. Les traces DOIVENT être conservées pour une durée de 12 mois.

[2] document disponible à http ://pole-reseaux.ac-clermont.fr/racine/doc/cadre-organique%20RACINE-V5%205.doc

**Zone de services de ressources à accès restreint (R) :** contient toutes les ressources sensibles du système d'information. Ces ressources sont à accès restreint avec des règles de sécurité fixées au cas par cas. La zone R est également la zone de transit des utilisateurs des services de l'académie avec application d'une politique locale de confinement (VLAN).
La zone R est accessible directement au travers d'un réseau RACINE-1 ou RACINE-API.
L'accès à la zone R à partir des zones A,C ou E n'est possible qu'au travers d'un relais applicatif réglementé.
La zone R ne peut héberger que des ressources mises sous la responsabilité de la personne habilitée par le chef de centre informatique en coordination avec l'ISR.
La traçabilité des accès aux ressources de la zone est EXIGEE. Le dispositif DEVRAIT permettre de mettre en évidence les adresses IP et ETHERNET des équipements à l'initiative de la connexion. Les traces DOIVENT être conservées pour une durée de 12 mois.

**Zone Z :** d'autres zones, appelées génériquement zones Z, hébergent des ressources ou services qui ne sont pas obligatoirement mis sous la responsabilité exclusive du centre informatique. Le niveau de sécurité à installer dépend des services proposés et des autres zones éventuellement accessibles. A définir au moins avec la PJR et l'ISR.

**Zone Z, Hot-spot Internet :** il s'agit de proposer un accès à Internet pour des utilisateurs ne relevant pas de la PJR.

**Zone Z, réseau enseignement :** ce réseau accueille toutes les stations et éventuellement les serveurs destinés à l'enseignement.

**Zone Z, réseau sans ressources :** réseau mis en oeuvre pour des besoins souvent très spécifiques ou ponctuels (démonstrations, expositions, conférences, ...) et sans ressources vitales accessibles.

# 4 Intégration du WiFi dans un réseau

## 4.1 Les cas d'utilisations

Quel que soit le besoin de mobilité, l'utilisation du WiFi peut être ramenée à trois grands cas d'utilisation :

**Extension d'un réseau local :** les utilisateurs de WiFi accèdent aux ressources d'un réseau local comme s'ils étaient connectés en filaire à ce réseau.

**Accès à des services :** les utilisateurs du WiFi accèdent à un ou plusieurs services identifiés (Hot Spot, ...). Dans ce cas, un certain nombre de dispositifs vise à limiter les possibilités d'utilisation du réseau permettant par là-même d'allèger les exigences de sécurité sur le réseau WIFI. Typiquement, le réseau est alors limité à l'utilisation de certains protocoles avec adossement de transport.

**Interconnexion de bâtiments :** le WiFi est utilisé pour raccorder des réseaux situés dans des bâtiments distants.

## 4.2 Où situer les points d'accès sur le réseau local ?

Deux solutions se présentent. Le point d'accès WIFI est raccordé directement au réseau local ou à une DMZ.

**Le point d'accès WiFi est raccordé directement au réseau local :**
- transparent pour tous les utilisateurs et tous les protocoles,
- s'il faut n points d'accès pour couvrir l'étendue d'une structure, il faut multiplier n par le nombre de zones RACINE (c.f. section 3 page 7) utilisant le WiFi,
- pas d'application d'une politique de sécurité possible en dehors de on/off sur les points d'accès.

**Le point d'accès WiFi est raccordé à une DMZ :**
- dans le cadre d'une extension d'un réseau local il peut être difficile du trouver le compromis entre l'application d'une politique de sécurité et transparence pour les utilisateurs,
- dans le cadre d'une extension d'un réseau local, cela pourra nécessiter la mise en oeuvre d'outils (serveurs WINS, DNS, ...) pour en permettre le fonctionnement des applications utilisant la diffusion pour fonctionner,
- un point d'accès peut donner accès à plusieurs zones RACINE (c.f. section 3 page 7), sous réserve d'utilisation des VLAN et de multiples SSID,
- possibilité d'établir une politique de sécurité fine.

En raison de l'impossibilité d'appliquer une politique de sécurité et de la multiplication potentielle des points d'accès, le raccordement direct dans un réseau local est à éviter. De plus, l'usage de type "Accès à des services" implique tout naturellement que le point d'accès soit dans une DMZ.

## 4.3 Quel type de WiFi pour quel réseau local ou quel service ?

Qu'il s'agisse d'étendre un réseau local ou d'ouvrir des services spécifiques, le niveau de sécurité des communications WiFi, donc le type de réseau WiFi (c.f. section 2 page 5) à utiliser, dépend des ressources accédées ou accessibles.

Le présent chapitre traite de l'adéquation entre les types de réseau WiFi définis dans le tableau 1 page 5 et les réseaux de l'éducation nationale dans le cadre de l'extension de réseau ou de l'ouverture des services via le WiFi. Les différentes solutions possibles sont synthétisées dans le tableau 2 page ci-contre.

L'utilisation du WiFi pour interconnecter des bâtiments est traité au chapitre 4.4.

## Lecture du tableau 2 page suivante

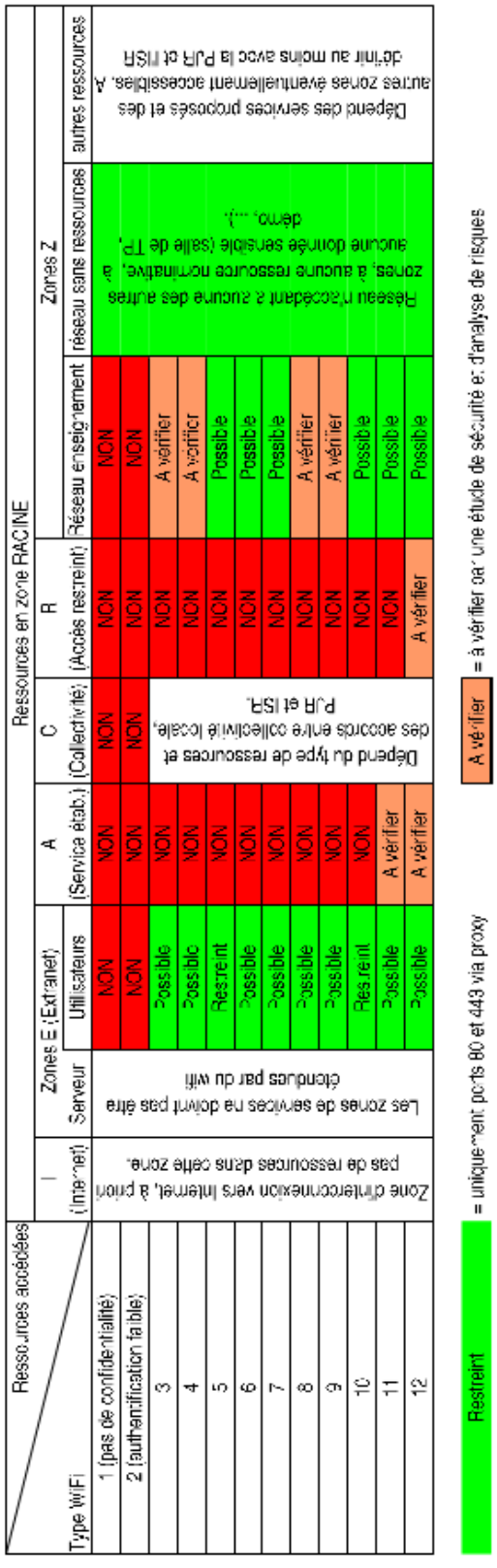
Le tableau 2 page ci-contre présente les types de réseaux WiFi devant être utilisés pour accèder aux zones précédemment définies, sans présumer de l'endroit où est raccordé le point d'accès WiFi.
Les cases rouges ("*NON*") signalent une inadéquation entre le niveau de sécurité obtenu et la zone RACINE.
Une case verte ("*Possible*") indique une adéquation à priori sans problème.
Une case verte ("*Restreint*") indique une adéquation à priori sans problème si l'utilisateur peut utiliser uniquement les protocoles 80 et 443 via un proxy.
Une case orange ("*A vérifier* ") indique qu'une étude est à mener pour s'assurer que le niveau de sécurité est conforme à la zone RACINE et aux usages prévus[3].
Dans le cas des cases vertes ("*Possible*" et "*Restreint*") et oranges ("*A vérifier* ") l'ISR pourra utiliser le "Guide méthodologique pour la réalisation d'une étude wifi" produit par le pôle de sécurité d'Aix-Marseille pour affiner son choix.

Si le point d'accès WiFi est situé dans une DMZ, le facteur déterminant le type de WiFi à utiliser est la zone de ressources la plus contraignante à laquelle les utilisateurs auront accès. Si le point d'accès est directement intégré dans une zone, le type de réseau WiFi à utilisé sera un de ceux autorisés pour la zone concernée.
Ces deux méthodes de lecture sont cohérentes grace aux politiques de sécurité qui régissent les connexions inter-zones (c.f. cadre organique RACINE). D'après la lecture du tableau 2 page suivante un point d'accès situé en zone Z peut être de type 12, type aussi utilisable pour une zone A. Pour autant, cela ne permet pas aux utilisateurs du WiFi de la zone Z d'accéder aux ressources d'une zone A car cela est interdit par la politique de sécurité.

Les points suivants sont à préciser :

- Les réseaux de types 5 et 10 utilisent une authentification par login/mot de passe sujette à diffusion, involontaire ou non. On connait la difficulté de maintenir un bon niveau de sécurité avec une telle solution. C'est pour cela que les accès doivent être restreints via un proxy, uniquement sur les ports 80 et 443.
- Pour le réseau collectivité, le niveau de sécurité serait à définir entre la collectivité, la PJR et l'ISR. Les réseaux marqués en rouge ne seraient acceptables que si la collectivité dégage la PJR et l'ISR de toute responsabilité,
- Pour un accès à un Hot-Spot Internet, l'établissement devra remplir les engagements légaux des fournisseurs d'accès à Internet,
- Lorsque le certificat du serveur est vérifié par les postes clients c'est que à minima ce certificat est géré par une PKI. Dans le cas d'un environnement PKI maîtrisé par l'éducation nationale, on peut se poser la question du surcoût d'activer la vérification du certificat client, certainement faible dans bien des cas.

[3] Par exemple un réseau WiFi de type 12 est possible pour la zone R mais autorise-t-on pour autant le WiFi sur les postes informatiques qui gérent les examens ?




TAB. 2 – Le WiFi pour étendre un réseau ou proposer des services.

## 4.4 Quel type de WiFi pour l'interconnexion de bâtiments ?

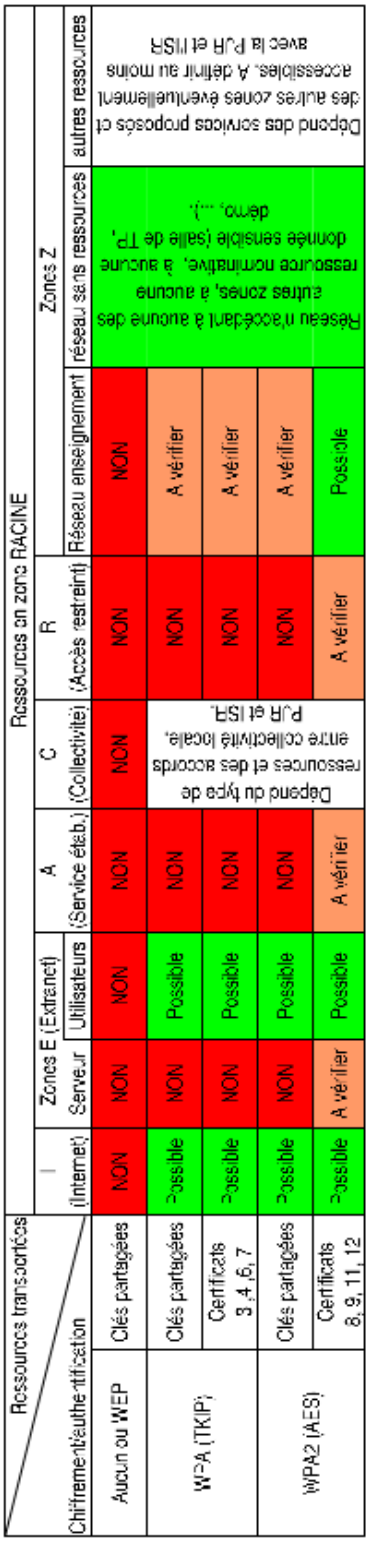
L'utilisation du WiFi en mode "pont" permet d'interconnecter les réseaux informatiques de bâtiments distincts. Comme différents réseaux d'une même structure peuvent être présents dans les différents bâtiments, une telle interconnexion peut transporter simultanément plusieures zones RACINE (c.f. section 2 page 5). Dans ce cas, le niveau de sécurité à mettre en place sur le lien d'interconnexion sera celui de la zone la plus exigeante.
Une case verte ("*Possible*") indique une adéquation à priori sans problème.
Une case orange ("*A vérifier* ") indique qu'une étude est à mener pour s'assurer que le niveau de sécurité est conforme à la zone RACINE et aux usages prévus.
Dans le cas des cases vertes ("*Possible*" ) et oranges ("*A vérifier* ") l'ISR pourra utiliser le "Guide méthodologique pour la réalisation d'une étude wifi" produit par le pôle de sécurité d'Aix-Marseille pour affiner son choix.
Les numéros présents dans les cases "*certificats*" font références à la nomenclature du tableau 1 page 5.

L'interconnexion de bâtiment utilise un mode de fonctionnement particulier du WiFi, nommé "pont". Dans le cadre d'un "pont", le point d'accès échange avec un autre point d'accès. Ces points d'accès ne sont pas accédés directement par les utilisateurs et leurs paramètres de configuration sont inconnus des utilisateurs. Seuls les administrateurs du réseau ont besoin de les connaître. A nos yeux et dans la mesure où ceux-ci sont de confiance et d'un nombre restreint, c'est le seul cas où les clés partagées nous semblent acceptables pour assurer le chiffrement. Dans certain cas, il nous paraît raisonnable de penser que la possession de la clé partagée suffit comme mécanisme d'authentification des points d'accès.
Cependant il faut avoir conscience que le changement des clés par une personne mal intentionnée est difficilement détectable et lui permet par la suite de déchiffrer les communications. Dans le cas d'utilisation de clés partagées par les points d'accès en mode pont, il faut donc que l'accès physique à ces points d'accès soit particulièrement bien contrôlé afin d'empêcher une telle opération.

Le tableau 3 page ci-contre indique le type de réseau WiFi à mettre en oeuvre en fonction des zones RACINE transportées par l'interconnexion.

### Commentaires sur le tableau 3 page suivante

- Les réseaux utilisant le WEP comme chiffrement sont interdits car la confidentialité de la communication n'est pas assurée.
- L'authentification concerne les points d'accès, et non plus les utilisateurs ou postes, avec une approche similaire à l'authentification des équipements de chiffrement des réseaux RACINES.




TAB. 3 – Le WiFi pour interconnecter des bâtiments.

# 5 Recommandations finales

Toute nouvelle installation doit utiliser du matériel conforme à la norme 802.11i et permettant la mise en oeuvre de tous les mécanismes de sécurité définis par la norme802.11i.

Les mécanismes de sécurité à mettre en oeuvre seront ceux obtenus après lecture du tableau 2 page 11 ou du tableau 3 page 13.

Cette recommandation peut paraître excessive. Elle ne l'est pas. Le matériel compatible 802.11i s'est généralisé donc son coût a fortement diminué.
Dans un réseau WiFi ce n'est plus le matériel WiFi qui coûte le plus cher. C'est toute l'architecture à mettre en oeuvre pour gérer la sécurité.
Lors d'une première installation, acheter du matériel comptatible 802.11i permet de faire évoluer le niveau de sécurité du réseau WiFi en mettant en oeuvre les mécanismes de sécurité au fur et à mesure que les besoins d'authentification et de confidentialité évolueront, ce qui ne manquera pas de se produire.

Il reste le cas des réseaux WiFi existants. Il faudra vérifier à l'aide de ce document et du "Guide méthodologique pour la réalisation d'une étude wifi" produit par le pôle de sécurité d'Aix-Marseille, leur adéquation avec les zones RACINE utilisant ces réseaux. Les réseaux WiFi non conformes aux recommandations seront à faire évoluer le plus rapidement possible afin de maintenir le niveau de sécurité global du réseau de l'éducation nationale.

ministère éducation nationale enseignement supérieur recherche

ACADEMIE D'AIX-MARSEILLE

**Pôle national de compétences de la sécurité des systèmes d'information d'Aix-Marseille**

# Annexe 3:
# Recommandations de sécurité pour le déploiement des réseaux Wi-Fi au sein de l'Education Nationale

| | |
|---|---|
| Rédacteur : Jean-Louis Brunel | Date et signatures |
| Approuvé par : DSR - Bureau DPMA/A3<br>Michel Affre<br>Mahfoud Baradi | Date et signature |

## Suivi des versions

| Version | Date | Rédacteur(s) | Nature des modifications | Pages modifiées | Validation |
|---|---|---|---|---|---|
| Document de travail | 23/03/2006 | Jean-Louis Brunel | Création | Toutes | |
| V0.9 | 29/03/2006 | Jean-Louis Brunel | Remarques J.P. Feugnet. | Page 4,5 | |
| V1.0 | 12/04/2006 | Jean-Louis Brunel | Intégration remarques DPMA-A3. Mise en forme. | Toutes | |
| V1.1 | 14/04/2006 | Jean-Louis Brunel | Explicitation des sigles EBIOS et DCSSI | Page 4,6 | |

# SOMMAIRE



# 1 Introduction

L'objet cette recommandation est de préciser le cadre de mise en œuvre et une démarche pour le déploiement des réseaux wifi à l'éducation nationale. Notre institution est aujourd'hui confrontée à des demandes de déploiement de réseaux sans fils. Les raisons en sont multiples et notamment légitimées par la gestion de la mobilité, les facilités de déploiement offertes par le wifi ainsi que par la possibilité de s'affranchir de contraintes difficilement surmontables avec les réseaux filaires.

Toutefois, il n'est pas possible de déployer un réseau wifi de façon identique à un réseau Ethernet classique. La nature même du média le rend particulièrement vulnérable à différents types d'attaques. L'impossibilité de maîtriser totalement la propagation du signal ou d'empêcher le brouillage de celui-ci, les failles dans les protocoles cryptographiques associés à la protection du wifi rendent obligatoire une étude de risque préalablement à tout déploiement. La potentialité des menaces et les vulnérabilités intrinsèques liées au wifi fait que le niveau de risque est nettement plus important qu'avec les réseaux traditionnels. La mise en œuvre d'un réseau wifi doit ainsi faire l'objet d'une étude et éventuellement de dispositifs de sécurité spécifiques.

S'il n'est pas possible d'envisager l'exhaustivité des cas de figure, les risques peuvent être appréciés au travers des usages et des informations véhiculées par le réseau. La plupart d'entre eux peuvent être ramenés à une des typologies connues analysées par le pôle de compétences de Clermont. La démarche d'analyse de risques proposée par le pôle d'Aix-Marseille doit fournir les éléments de choix pour un déploiement maîtrisé en terme de risques.

Les risques génériques auxquels sont confrontés les réseaux wifi ont fait l'objet d'une étude de la DCSSI dont les recommandations peuvent être étendues à notre institution. Dans tous les cas, il convient de garantir à un niveau suffisant :

- *la disponibilité et la qualité de service face aux agressions en saturation ;*
- *le caractère intègre des contenus face aux actes de malveillance ;*
- *la confidentialité des échanges face à des interceptions passives ;*
- *la qualité des preuves techniques d'accès aux services et des actions notamment pour assurer (..) l'engagement de responsabilité.*

# 2 Déploiement du réseau Wifi

L'étude préalable à la mise en œuvre du réseau Wifi, telle qu'elle est présentée en introduction, doit préciser les objectifs fonctionnels poursuivis. Elle doit, en particulier, préciser le type d'utilisation qui sera fait de ce réseau (extension de réseau existant, interconnexion entre deux réseaux, accès de type hot spot) ainsi que le cercle de confiance, selon la classification Racine, dans lequel il sera mis en œuvre. Cette description

fonctionnelle doit être accompagnée d'une description des usages ainsi que des données qui seront véhiculées sur le réseau.

La nature des données et des fonctions utilisées sur le réseau wifi ainsi que le cercle de confiance définissent un niveau de sensibilité du réseau. En fonction de celui-ci, le tableau de synthèse proposé par le pôle de Clermont sera utilisé pour déterminer si l'usage du wifi est envisageable, la nécessité éventuelle d'une analyse de risque plus approfondie, et le cas échéant les protocoles cryptographiques et d'authentification à utiliser.

Si une analyse de risque est nécessaire, une approche simple et pragmatique dérivée de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) sera utilisée. Le pôle de compétences d'Aix-Marseille est à la disposition des académies pour les aider à la réalisation de telles études.

Le dossier produit à l'issue de l'étude (étude préalable seule ou étude préalable suivi d'une analyse de risque approfondie) a valeur de recommandation. Il appartient à la personne juridiquement responsable de l'entité de valider le dossier et de décider sur la base de celui-ci le niveau de risque accepté. Si le niveau de risque accepté remet en cause le niveau de sécurité requis pour les réseaux RACINE, le dossier doit être communiqué à la DSR par l'ISR.

# 3 Protections physiques

Dans le cadre de l'étude d'implantation d'un réseau wifi, la sécurité physique est à traiter en premier lieu. L'étude doit déterminer en particulier :

- les risques environnementaux et les protections destinées à y faire face (onduleurs pour se prémunir contre la foudre par exemple) ;
- l'accessibilité au site et aux équipements wifi ainsi que les mesures de contrôles ou limitations d'accès physiques à mettre en œuvre ;
- la couverture du réseau et les mesures envisagés pour surveiller physiquement le site, le cas échéant.

# 4 Protections logiques

Les algorithmes de chiffrement, les méthodes d'authentification et les modes de transport associés ainsi que leurs conditions d'utilisation sont précisés dans le document de Clermont. Ils déterminent des niveaux ou profils de protection chiffrement/authentification. L'étude doit permettre de choisir parmi l'un de ces profils de protection.

# 5 Synthèse de la démarche à mettre en œuvre

La synthèse récapitule les recommandations pour la mise en œuvre des réseaux wifi au sein de notre institution : il s'appuie sur celle proposée par la DCSSI (Direction centrale de la sécurité des systèmes d'information).

**Recommandation générale**

Rappel : les recommandations s'appliquent aux réseaux à mettre en œuvre et aux réseaux existants.

- Étude préalable au déploiement :
  - description de la zone et du type de réseau ;
  - description des données et fonctions utilisées sur le réseau ;
- Choix des objectifs de sécurité en termes de :
  - Disponibilité
  - Intégrité des contenus et fonctions
  - Confidentialité des échanges
  - Qualité des preuves techniques d'accès aux services et des actions.
- Analyse approfondie des risques.

**Recommandation concernant la protection physique**

- étude préalable de l'environnement du site (risques naturels)
- étude physique du site ;
- vérification de la zone de couverture.

**Recommandation concernant la protection logique et organisationnelle**

- choix du profil de protection chiffrement/authentification en fonction des recommandations de Clermont;
- configuration des points d'accès ;
- mise en œuvre d'un pare-feu.
- justification des choix.

**Documents applicables**

[réf.1] Note sur l'usage du wifi au sein de l'Education Nationale – DPMA-A3
[réf.2] Étude d'intégration du WIFI dans les réseaux de l'Éducation Nationale. Pôle de compétences réseau Clermont-Ferrand
[réf.3] Recommandation sur la démarche à mettre en œuvre pour le déploiement des réseaux Wifi au sein de l'Education Nationale. Pôle de compétences sur la sécurité des systèmes d'informations. Aix-Marseille
[réf.4] Guide méthodologique pour la réalisation d'une étude wifi. A venir.