# RECOMMANDATIONS DE DÉPLOIEMENT DU PROTOCOLE 802.1X POUR LE CONTRÔLE D'ACCÈS À DES RÉSEAUX LOCAUX

## GUIDE ANSSI

ANSSI-PA-043
07/08/2018

**PUBLIC VISÉ :**

Développeur **Administrateur** **RSSI** **DSI** Utilisateur

# Informations

## Attention

Ce document rédigé par l'ANSSI présente les « **Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux** ». Il est téléchargeable sur le site `www.ssi.gouv.fr`.



Ces recommandations n'ont pas de caractère normatif, elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

## Évolutions du document :

| VERSION | DATE | NATURE DES MODIFICATIONS |
|---|---|---|
| 1.0 | 07/08/2018 | Version initiale |

# Table des matières

# 1
# Introduction

Dès lors qu'il héberge des données sensibles telles que des secrets industriels, des numéros de cartes de crédit ou même des données personnelles, un système d'information devient une cible de choix pour un attaquant. Les menaces les plus courantes d'une analyse de risque prennent en compte le piégeage d'un équipement interne par une source externe, cependant la connexion d'équipements externes au système d'information local est souvent négligée pour les raisons suivantes :

- les utilisateurs sont considérés comme de confiance ;
- des mesures techniques ou opérationnelles empêchent un visiteur de connecter son équipement à un réseau interne.

Ces hypothèses sont souvent mises en avant mais l'architecture physique d'un système d'information évolue dans le temps, notamment au gré des différents déménagements. Une prise réseau précédemment affectée à un bureau peut se retrouver dans une zone publique et exposer le système d'information de l'entité à un visiteur. Un utilisateur légitime peut également connecter pour diverses raisons un équipement personnel ou un équipement réseau au système d'information interne ou fournir un secret d'authentification tel qu'un mot de passe d'accès à un réseau Wi-Fi à une personne extérieure, exposant également le système d'information à différentes menaces préalablement éludées.

Afin de traiter ces différents problèmes, il est possible d'appliquer le principe de défense en profondeur et d'ériger des barrières supplémentaires sur le réseau du système d'information. Leurs rôles seront principalement de limiter les connexions d'équipements au strict nécessaire et de superviser les évènements intervenant sur le réseau afin de détecter des comportements suspects. Ces deux fonctions répondent à des objectifs de sécurité préventifs et réactifs afin d'augmenter le niveau de sécurité du système d'information.

Ce document détaille le fonctionnement d'un tel réseau local, appelé *réseau à accès contrôlé*, qu'il soit filaire ou sans fil et présente les recommandations de mise en œuvre d'une telle technologie, reposant sur le protocole 802.1X [1]. Le chapitre 2 décrit l'architecture et les composants principaux d'un tel réseau. Le chapitre 3 présente les fonctions de sécurité apportées par cette solution et les bonnes pratiques à appliquer afin d'augmenter le niveau de sécurité du réseau considéré.

## 1.1 Dénominations

Les termes présentés dans cette section, en rapport avec les réseaux à accès contrôlés, sont utilisés tout au long du document.

- **Réseau 802.1X** : réseau à accès contrôlé.

- **AAA** : *Authentication, Authorization, Accounting* (Authentification, Autorisation et Traçabilité).
- **Serveur AAA** : serveur offrant les services d'authentification, d'autorisation et de traçabilité des évènements. Nous utiliserons le terme *serveur* pour désigner le serveur AAA dans ce document.
- **Client** : élément de confiance d'un *réseau 802.1X* servant de point d'accès au réseau (commutateur, point d'accès Wi-Fi…). Cet élément est appelé *authenticator* dans la norme 802.1X [1].
- **Supplicant** [1] : logiciel sur l'équipement d'extrémité cherchant à se connecter à un réseau à accès contrôlé, afin de fournir une connectivité Ethernet à l'équipement d'extrémité.
- **EAP** : *Extended Authentication Protocol*, protocole réseau permettant d'abstraire le mécanisme d'authentification spécifique utilisable.
- **EAPoL** : *Extended Authentication Protocol over LAN*, protocole d'encapsulation de trames `EAP` sur des réseaux locaux. C'est un protocole qui repose sur Ethernet et qui dispose de son propre *Ethertype* [2] `0x888E`.
- **Réseau à accès contrôlé** : réseau dont l'accès doit être protégé par des mécanismes AAA.
- **Réseau de confiance** : réseau *maîtrisé* dans lequel le *serveur* et les *clients* communiquent.

1. Ce terme anglais ne dispose d'aucune traduction française standard, il est utilisé tel quel dans le document.
2. L'Ethertype est un numéro positionné dans l'en-tête d'une trame Ethernet qui identifie le protocole réseau encapsulé.

# 2
# Architecture d'un réseau local à accès contrôlé

## Objectif

Détailler le fonctionnement général d'un réseau 802.1X, des différents équipement qui le composent et des protocoles sous-jacents sur lesquels il repose.

Nous traitons dans ce document des cas de déploiement suivants :

- contrôle des connexions filaires à un réseau local ;
- contrôle des connexions sans fil et distribution des clés cryptographiques nécessaires à leur sécurisation.

Un réseau local à accès contrôlé requiert l'utilisation d'une infrastructure 802.1X, définie dans le document [1]. De façon synthétique, une telle infrastructure est construite autour de plusieurs *clients* (*e.g.* des commutateurs, des points d'accès sans fil) qui offrent des ports de connexion à des *supplicants*. L'état de ces ports est contrôlé par un *serveur* au moyen d'un protocole présenté section 2.1.1. Le *serveur* communique avec les *clients* au travers d'un *réseau de confiance* et il autorise ou refuse l'ouverture d'un port à un *supplicant* après authentification de ce dernier.

Le *serveur* dispose aussi d'un service de journalisation qui enregistre les évènements liés aux accès réseaux (tentatives de connexion, déconnexions…). Il fournit également les clés cryptographiques nécessaires à la sécurisation des échanges sans fil entre *supplicants* et bornes d'accès. La figure 2.1 schématise l'ensemble des éléments que l'on retrouve dans une infrastructure 802.1X.

Dans sa dernière évolution, ce standard définit un moyen de sécuriser la connexion filaire entre le *supplicant* et le *client* par des moyens cryptographiques, au même titre qu'une connexion sans fil. Cette fonctionnalité, appelée `MACsec`, n'est pas abordée dans ce document car elle est peu implémentée dans les *supplicants* et dans les *clients* actuels. Des détails sur cette technologie peuvent être consultés dans le document [5].

## 2.1 Composants d'un réseau 802.1X

### 2.1.1 Serveur

Le *serveur* est le composant central d'un *réseau à accès contrôlé*. Il centralise les fonctions d'authentification et d'autorisation des *supplicants* et la fonction de journalisation des évènements remontés

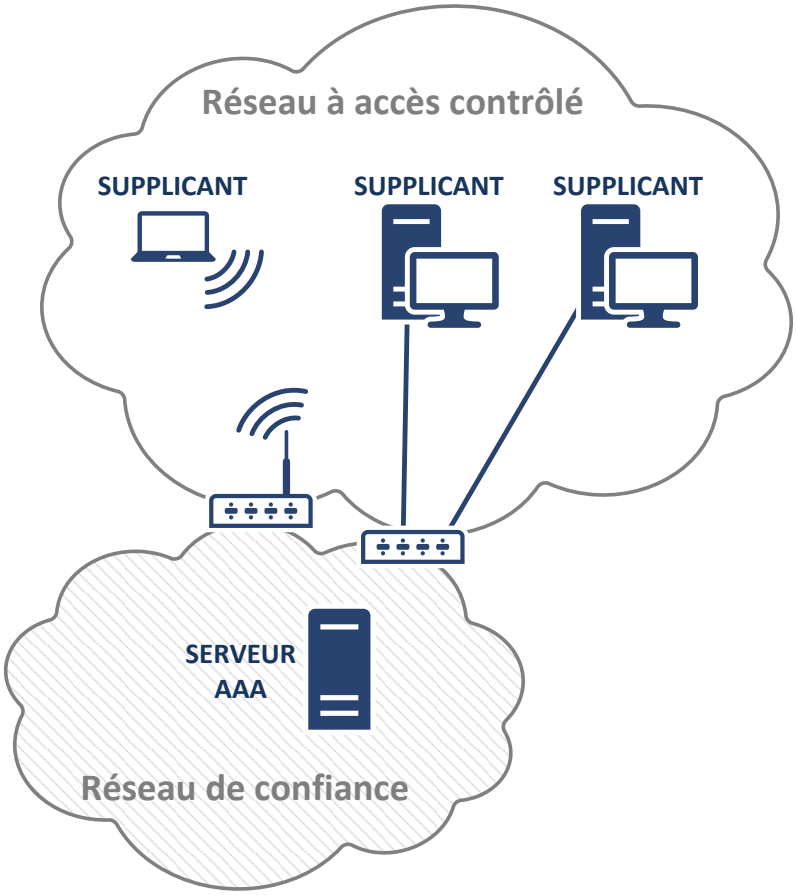


FIGURE 2.1 – Composants principaux d'un réseau à accès contrôlé

par les *clients*. Situé dans le *réseau de confiance*, il décide si la connexion d'un *supplicant* au *réseau à accès contrôlé* est autorisée ou refusée. Par défaut, si aucune réponse n'est fournie par le *serveur*, le port reste dans l'état fermé et le *supplicant* n'a pas accès au réseau. Il est donc indispensable qu'un *serveur* soit joignable à tout moment pour assurer la disponibilité du réseau.

La norme [1] ne spécifie pas le protocole à utiliser pour les échanges entre les clients et le *serveur*, tant que celui-ci permet de contrôler l'état des ports des clients. Elle cite cependant en exemple les protocoles RADIUS [31] et Diameter [25]. De plus, le document [22] spécifie le comportement d'un serveur RADIUS dans le cadre d'un *réseau 802.1X*. Ces deux protocoles sont ainsi devenus les standards utilisés dans les *réseaux 802.1X*.

Le protocole Diameter est le successeur du protocole RADIUS. Il est le standard d'authentification des équipements sur des réseaux de téléphonie mobile 3G et 4G. Cependant il est rarement implémenté dans les *clients* utilisés dans les systèmes d'information traditionnels [20, 21, 27].

R1

### Choix d'un protocole AAA dans un réseau à accès contrôlé

De part l'absence de support du protocole Diameter dans les *clients* les plus courants des systèmes d'information, l'utilisation du protocole RADIUS est recommandée dès

lors qu'un *réseau à accès contrôlé* doit être mis en place sur un système d'information.

### 2.1.2 Réseau de confiance et clients

Le *réseau de confiance* est le réseau utilisé par les équipements d'une infrastructure 802.1X pour les communications nécessaires à son fonctionnement. Il transporte les informations d'authentification et d'autorisation des équipements finaux et les différentes données de journalisation remontées par les *clients* au *serveur*. Ce réseau de confiance est considéré comme *sûr*, sans hypothèse sur les protocoles qu'il transporte. Le trafic réseau généré par ces échanges est négligeable.

Les informations d'authentification et d'autorisation échangées entre les *clients* et le *serveur* sont détaillées dans la RFC2865 [31] et les informations de journalisation dans la RFC2866 [30].

Les *clients* d'un *réseau 802.1X* sont des équipements tels que des commutateurs (*switchs*) ou des points d'accès Wi-Fi qui fournissent une connectivité au *réseau à accès contrôlé* à l'aide de *ports de connexion*. Il sont connectés au réseau de confiance, pour contacter le *serveur*. Les *ports de connexion* peuvent se trouver dans deux états :

- dans l'état *autorisé*, un port accepte tout trafic en provenance et à destination du *supplicant* connecté, notamment le trafic IP ;
- dans l'état *non autorisé*, seul le trafic `EAPoL` est autorisé entre le *client* et le *supplicant*.

Par défaut, ils sont dans l'état non autorisé et leur changement d'état est commandé par le *serveur* après authentification et autorisation d'un *supplicant*. Durant cette phase d'authentification, détaillée au §2.1.4, les *clients* réalisent une rupture protocolaire entre le *supplicant* et le *serveur*. En effet, la communication avec les *supplicants* s'effectue au moyen du protocole `EAPoL` alors qu'elle s'effectue à l'aide du protocole du *réseau de confiance* entre les *clients* et le *serveur* (RADIUS sur IP dans la plupart des cas). La connectivité Ethernet des *supplicants* est donc inexistante avant leur autorisation d'accès au *réseau à accès contrôlé*. Ce fonctionnement est rappelé figure 2.2.

### 2.1.3 Réseau à accès contrôlé

Le *réseau à accès contrôlé* est le réseau dont les accès doivent être maîtrisés. Il est connecté aux différents *clients* et aux *supplicants*. Le terme *réseau à accès contrôlé* désigne par extension l'ensemble des réseaux utilisateurs (physiques ou virtuels) dont l'accès doit être contrôlé centralement.

### 2.1.4 Supplicants

Les *supplicants* cherchent à se connecter au *réseau à accès contrôlé* au travers des ports de connexion offerts par les *clients*. L'accès à ce réseau est autorisé ou refusé après une phase d'authentification et d'autorisation dans laquelle les trois équipements (*supplicant*, *clients* et *serveur*) interagissent. Une fois leur accès au réseau autorisé, les *supplicants* sont connectés au *réseau à accès contrôlé*.

## 2.2 Synoptique de connexion

La connexion à un *réseau à accès contrôlé* s'effectue en quatre étapes.

**Initialisation :** le *client* détecte la tentative de connexion du *supplicant* à un port dont l'accès est contrôlé, il active le port en mode *non autorisé*.

**Identification :**

- le *client* transmet au *supplicant* une demande d'identification (trame `EAP-Request/Identity`) ;
- le *supplicant* retourne au *client* son identité (trame `EAP-Response/Identity`) ;
- le *client* transmet l'identité du *supplicant* au *serveur* (paquet `Access-Request`).

**Négociation `EAP` :**

- le *serveur* envoie au *client* un paquet contenant la méthode d'authentification demandée au *supplicant* (paquet `Access-Challenge`) ;
- le *client* transmet la demande du *serveur* au *supplicant* au travers d'une trame `EAP-Request` ;
- si le *supplicant* accepte cette méthode, il procède à l'étape d'authentification au moyen de celle-ci, sinon il renvoie au *client* les méthodes qu'il supporte et l'étape de négociation recommence.

**Authentification :**

- le *serveur* et le *supplicant* échangent des messages `EAP-Request` et `EAP-Response` par l'intermédiaire du *client* suivant la méthode d'authentification choisie,
- le *serveur* fournit une réponse `Access-Accept` ou `Access-Reject` suivant le résultat de l'authentification et de l'autorisation du *supplicant* :
  - si la réponse est `Access-Accept`, le *client* bascule le port de connexion dans l'état *autorisé*, le *supplicant* dispose ainsi d'une connectivité Ethernet au réseau à accès contrôlé,
  - si la réponse est `Access-Reject`, le port reste dans l'état *non autorisé* et le *supplicant* ne dispose d'aucun accès réseau hormis au travers du protocole `EAP`.

À la fin de la connexion (déconnexion logicielle entrainant un message EAP dédié ou changement de statut du lien physique), le *client* modifie l'état du port à *non autorisé*. La figure 2.2 récapitule les échanges intervenant lors d'une connexion d'un *supplicant* à un *réseau à accès contrôlé*.

## 2.3 Protocoles d'authentification

Dans une infrastructure 802.1X, l'authentification des *supplicants* repose sur le protocole `EAP`, défini dans le document [6]. Ce protocole d'authentification extensible définit plusieurs méthodes d'authentification possédant différents niveaux de sécurité. Les méthodes d'authentification les plus fréquemment utilisées sont détaillées dans cette section.

### 2.3.1 EAP-MD5

Authentification du *supplicant* reposant sur un protocole par défi-réponse et sur la fonction de hachage `MD5` [6]. Cette méthode offre un faible niveau de sécurité, car vulnérable à des attaques par dictionnaires et de l'homme du milieu. De plus, elle ne permet pas d'authentifier le serveur et ne peut pas être utilisée dans des réseaux sans fil de part l'absence de négociation des clés cryptographiques durant l'authentification.

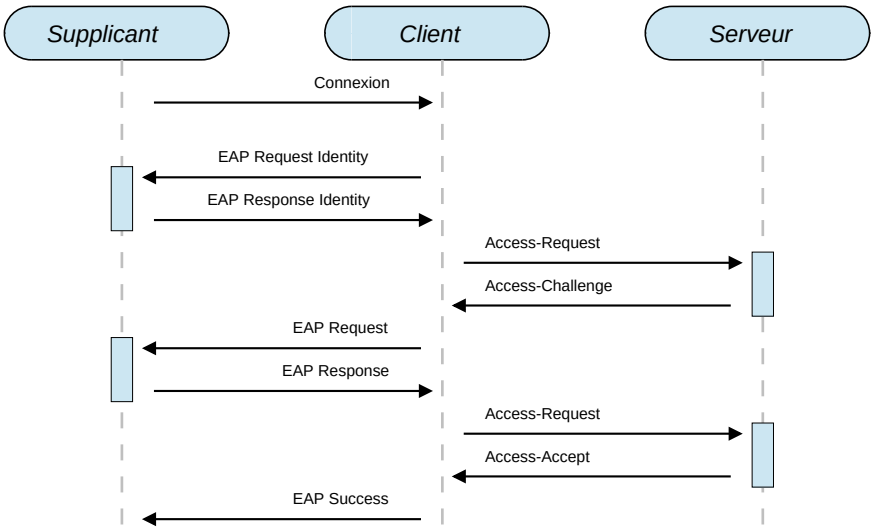


FIGURE 2.2 – Logigramme de connexion à un *réseau 802.1X*

### 2.3.2 EAP-MSCHAPv2

Authentification mutuelle des correspondants qui repose sur un mot de passe et des défis cryptographiques. Cette méthode offre un niveau de sécurité faible, elle est vulnérable à des attaques par dictionnaires et sa résistance est équivalente à celle d'une clé DES [32].

### 2.3.3 EAP-TLS

EAP-TLS est un protocole d'authentification mutuelle du *supplicant* et du *serveur* par certificats. Cette authentification est réalisée à l'aide d'un *handshake TLS* [16] dont la mise en œuvre sur EAP est définie dans le document [33]. Cette méthode nécessite que le *serveur* et chaque *supplicant* possèdent un certificat. Elle impose donc l'utilisation d'une infrastructure de gestion de clés dans le système d'information.

Ce protocole d'authentification est considéré comme sûr. Il expose cependant l'identité du *supplicant* durant la connexion, au travers du *Common Name* du certificat ou du champ `Identity` de la réponse EAP. Suivant le scénario de déploiement envisagé, cette information peut être considérée comme sensible. Le mode *privacy*, défini au paragraphe 2.1.4 de la [33], traite ce problème en modifiant le séquencement des opérations dans le *handshake TLS*. L'implémentation de cette fonctionnalité est cependant optionnelle et elle reste peu implémentée dans les serveurs et les *supplicants* existants.

### 2.3.4 EAP-PEAP

Ce protocole d'authentification est souvent dénommé `PEAP` dans la littérature. Initialement créé et défini par Microsoft, ses spécifications sont disponibles en accès libre sur le site de l'éditeur [3]. Le protocole `PEAP` propose plusieurs versions et évolution. À la date de publication de ce document, la dernière version applicable de ce protocole est disponible dans le document [4].

3. Voir `https://msdn.microsoft.com/en-us/openspecifications/`.

Le protocole PEAP fonctionne en deux phases. Durant la première phase, le *serveur* s'authentifie auprès du *supplicant* au moyen d'un certificat pour créer un tunnel TLS entre les deux parties. Il procède ensuite à l'authentification du *supplicant* dans le tunnel TLS au moyen d'une méthode EAP appelée *méthode interne* [4]. Les échanges réalisés par cette méthode interne sont protégés par le tunnel TLS établi.

Cette construction permet l'utilisation de protocoles reposant sur les mots de passe pour l'authentification des *supplicants*. La méthode d'authentification interne la plus couramment utilisée est la méthode EAP-MSCHAPv2 et dans ce cas, le protocole est appelé PEAP-MSCHAPv2. PEAP peut également utiliser d'autres méthodes internes comme EAP-TLS pour authentifier les *supplicants*.

Le protocole PEAP requiert uniquement un certificat *serveur*, l'utilisation de certificats *clients* est optionnelle et dépend de la *méthode interne* choisie. La mise en œuvre de ce protocole permet d'atteindre un niveau de sécurité correct, sous réserve d'appliquer les recommandations détaillées dans le chapitre 3 de ce document.

### 2.3.5 EAP-TTLSv0

Le protocole EAP-TTLSv0, aussi appelé EAP-TTLS, est un protocole d'authentification en deux phases, dont le fonctionnement est similaire au protocole PEAP. Ces protocoles restent cependant différents et incompatibles. Durant la première phase, le *supplicant* authentifie le *serveur* au moyen d'un certificat afin de créer un tunnel TLS entre les deux parties. L'authentification du *supplicant* s'effectue durant la seconde phase, à l'intérieur du tunnel TLS précédemment créé et à l'aide d'une méthode d'authentification interne (*inner method*). Cette méthode peut être une méthode EAP (EAP-MD5 par exemple) ou non EAP comme MSCHAPv2. Dans la majorité des déploiements, les méthodes internes utilisées sont PAP, EAP-MD5, EAP-MSCHAPv2 ou MSCHAPv2.

Le protocole EAP-TTLSv0 est défini dans le document [26] [5] et il présente plusieurs avantages :

- l'identité du *supplicant* est masquée durant la phase d'authentification ;
- plusieurs méthodes internes peuvent être utilisées, sachant qu'elles sont souvent déjà mises en place dans un système d'information ;
- il requiert uniquement un certificat serveur, l'utilisation de certificats *clients* n'est pas obligatoire.

L'utilisation de ce protocole permet d'atteindre un niveau de sécurité correct sous certaines conditions de déploiement, détaillées dans le chapitre 3.

4. Traduction de la dénomination *inner method* utilisée dans la norme.
5. Le protocole EAP-TTLSv1, défini dans un draft IETF, n'est pas un standard et il est rarement implémenté.

# 3
# Recommandations de déploiement

### Objectif

Configurer de façon sécurisée les différents éléments d'un réseau 802.1X et comprendre les limites de sécurité d'un tel déploiement.

## 3.1 Authentification, autorisation et protocoles

### 3.1.1 Authentification et autorisation

Lorsqu'un *supplicant* tente de se connecter à un *réseau 802.1X*, il fournit une identité. Il est donc possible d'autoriser sa connexion en fonction uniquement de l'identité qu'il déclare, cependant un tel fonctionnement abaisse le niveau de sécurité du réseau à celui d'un réseau ouvert. L'authentification est donc un pré-requis nécessaire à l'autorisation de connexion de *supplicants* à un réseau 802.1X.

**R2**

#### Authentification des supplicants

Il est fortement recommandé d'authentifier les *supplicants* qui tentent d'accéder à un *réseau 802.1X*.

Le *supplicant* traverse des étapes d'authentification et d'autorisation au moment de sa connexion. Ces deux fonctions de sécurité sont complémentaires et non redondantes : en effet, un utilisateur peut être *authentifié* par un certificat et une clé privée associée ou par un nom d'utilisateur et un mot de passe, sans qu'il soit pour autant autorisé à accéder au réseau. L'authentification est donc un des critères nécessaire à l'autorisation, mais il n'est pas suffisant.

**R3**

#### Autorisation des supplicants

Il est fortement conseillé d'autoriser la connexion de *supplicants* au moyen d'une liste exhaustive d'identités autorisées à se connecter et de s'assurer de la cohérence de l'identité utilisée entre les phases d'identification et d'authentification.

L'objectif de la recommandation R3 est double. En premier lieu, elle permet de s'assurer que l'identité utilisée durant la phase d'autorisation est valide et en second lieu, qu'elle correspond à celle utilisée durant la phase d'authentification. À titre d'exemple, la politique d'accès *tout supplicant authentifié est autorisé* n'est pas recommandée car elle ne vérifie pas la validité de l'identité du *supplicant* lors de la phase d'autorisation.

Les données d'authentification sont des données secrètes. Il est donc nécessaire de les protéger en confidentialité et en intégrité pour éviter leur fuite et leur utilisation sur des équipements tiers.

R4

### Secrets d'authentification

Il est recommandé de mettre en œuvre des mesures permettant d'assurer la confidentialité et l'intégrité des éléments secrets présents dans le *serveur*, les *clients* et les *supplicants*.

Les mesures qui permettent de respecter la recommandation R4 varient suivant les types d'éléments secrets (mot de passe, clé privée…) et les équipements qui les manipulent. La sécurité des mots de passe dans les *clients* dépend des méthodes de stockage et de sauvegarde implémentées (présence ou non dans le fichier de sauvegarde, inscription en clair dans un fichier ou dans l'interface de configuration…), mais aussi des accès physiques aux équipements. Un attaquant disposant d'un accès physique à un *client* pourra déployer diverses méthodes pour extraire le secret de l'équipement.

La protection des secrets d'authentification des *supplicants* dépend de leur nature. En effet, la confidentialité d'un mot de passe ne peut pas être contrôlée par des moyens techniques. La protection d'une clé privée peut cependant s'effectuer de différentes façons (clé privée non exportable dans un magasin de certificats, *token* cryptographique, droits d'accès…).

Les éléments secrets du *serveur* sont sa clé privée d'authentification et les mots de passe utilisés par les *clients*. Leur protection nécessite une gestion rigoureuse des droits d'accès et, dans le cas de la clé privée, l'utilisation éventuelle d'un module de sécurité externe [6].

## 3.1.2 Protocoles d'authentification

Lorsqu'un *supplicant* s'authentifie sur un *réseau 802.1X*, il est important de s'assurer que toute information sensible ou secrète échangée durant l'authentification (mot de passe, clé de session…) ne puisse pas être récupérée par un attaquant, au moyen d'une écoute passive ou d'une attaque active (attaque de l'homme du milieu par exemple).

R5

### Utilisation de protocoles d'authentification sécurisés

Il est fortement recommandé d'utiliser des protocoles d'authentification possédant les propriété suivantes :

- utilisation d'une couche cryptographique standard ;
- authentification mutuelle entre le *supplicant* et le *serveur* ;
- masquage de l'identité du supplicant durant la phase d'authentification, si le contexte le justifie.

Les méthodes d'authentification `EAP-TLS`, `EAP-TTLS` et `EAP-PEAP` dans ses dernières versions peuvent respecter la recommandation R5. En revanche, les méthodes d'authentification non encapsulées telles que `EAP-MSCHAPv2` et `EAP-MD5` ne respectent pas cette recommandation.

6. *Hardware Security Module*.

De plus, lorsqu'une méthode d'authentification (telle que MSCHAPv2) est utilisable au travers d'un protocole non encapsulé (*e.g.* EAP-MSCHAPv2) et d'un protocole encapsulé (*e.g.* EAP-TTLS-MSCHAPv2), un attaquant se faisant passer pour un point d'accès (filaire ou sans fil) peut transmettre les trames non protégées récupérées du *supplicant* dans le tunnel qu'il a monté avec le *serveur*. Il obtient ainsi l'accès au réseau et potentiellement des informations sur les éléments secrets du client. Cette attaque est applicable au protocole EAP-TTLS (voir section 14.1.11 du document [26]) et au protocole PEAP sous certaines conditions.

R6

### Suppression du support des méthodes non encapsulées

L'authentification de *supplicants* à l'aide de méthodes non encapsulées n'est pas recommandée. La configuration du *serveur* doit explicitement interdire l'utilisation de ces méthodes non encapsulées pour ne pas dégrader la sécurité du système mis en place.

## 3.1.3 Réseau sans fil

Lorsque l'accès à réseau sans fil est contrôlé par le protocole 802.1X, le point d'accès Wi-Fi instancie, à chaque connexion d'un *supplicant*, un *port de connexion* virtuel dont l'état est contrôlé par le *serveur*. Le fonctionnement de tels réseaux sans fil est détaillé dans le document [14] et dans la norme [3]. Cette dernière précise d'ailleurs que le protocole d'authentification utilisé doit authentifier mutuellement le *serveur* et le *supplicant*.

Ces réseaux sans fil sont appelés réseaux WPA2-Enterprise (parfois nommés WPA2-EAP)[7]. Contrairement aux réseaux sans fil personnels (aussi appelés réseaux WPA2), il n'est pas nécessaire de renseigner une clé de protection des échanges entre un équipement et la borne d'accès. Cette clé est négociée entre le *supplicant* et le *serveur* durant la phase d'authentification puis transmise à la borne par ce dernier dans le message Access-Accept. Chaque *supplicant* connecté dispose de sa propre clé de protection des données, renouvelée au moins à chaque connexion et indépendante des clés utilisées par les autres *supplicants*.

R7

### Mise en place d'un réseau sans fil 802.1X

Lorsqu'un réseau sans fil doit être mis en place, il est recommandé de déployer un réseau WPA2-Enterprise. Ce choix permet de contrôler l'authentification de chaque *supplicant* de façon indépendante et de bénéficier de protections cryptographiques robustes.

Les clés cryptographiques utilisées pour chiffrer et authentifier le trafic sans fil sont issues de données négociées entre le *serveur* et le *client* durant les premières étapes de l'authentification. Ces données sont négociées à l'aide de TLS pour les protocoles d'authentification EAP-TLS, EAP-TTLS et PEAP.

7. Seul le protocole WPA2 est mentionné ici. Le protocole WPA étant obsolète, il ne doit plus être utilisé.

R8

### Négociation des clés cryptographiques à l'aide de TLS

Il est recommandé d'utiliser une version de TLS récente et une suite cryptographique robuste dont le protocole d'échange de clé assure la propriété de confidentialité persistante [a].

L'application de la recommandation R8 assure que la compromission de la clé privée du *serveur* ou d'un *supplicant* ne remet pas en cause la confidentialité des connexions précédentes. Les recommandations de l'ANSSI sur les suites TLS à utiliser sont disponibles dans le document [16].

Les protocoles `EAP-TTLS` et `PEAP` sont des protocoles à authentification disymétriques, dans le sens où le mécanisme d'authentification du *serveur* diffère de celui du *client* dans la plupart des cas.

R9

### Liaison entre l'authentification externe et l'authentification interne

Dès lors qu'un protocole d'authentification asymétrique est mis en place, il est préférable :

- d'utiliser un protocole qui génère les clés cryptographiques à partir d'éléments négociés pendant les deux authentifications ;
- d'utiliser une méthode interne qui génère des éléments partagés.

Les clés cryptographiques générées par le protocole `EAP-TTLS` sont uniquement issues de l'authentification TLS du *serveur*. Les données échangées durant l'authentification interne ne sont pas prises en compte. Ce fonctionnement n'est pas optimal, car il permet à un attaquant d'effectuer une attaque de l'homme du milieu, en montant le tunnel TLS avec le *serveur* et en relayant les échanges liés à la méthode interne au *supplicant*. Il peut ainsi observer les échanges liés à l'authentification et obtenir des informations sur les authentifiants utilisés par le *supplicant* [19]. Des extensions existent pour pallier cette faiblesse, cependant celles-ci sont publiées dans des documents non standards, aujourd'hui expirés et elles restent rarement implémentées. L'utilisation du protocole `EAP-TTLS` doit donc obligatoirement s'accompagner de l'application de la recommandation R6.

Le protocole `PEAP` ne présente pas la même faiblesse. Les clés cryptographiques sont générées à partir de données issues de l'authentification TLS du *serveur* et des éléments négociés durant l'authentification interne. De plus, `EAP-MSCHAPv2` négocie des secrets partagés durant l'authentification. Le protocole `PEAP/EAP-MSCHAPv2` respecte donc la recommandation R9. Les faiblesses cryptographiques du protocole `EAP-MSCHAPv2`, détaillées dans le document [32], imposent cependant l'application de la recommandation R6 pour éviter toute dégradation du niveau de sécurité.

## 3.2 Réseau de confiance

La norme 802.1X fait état d'un *réseau de confiance* qui relie les *clients* et le *serveur*. Ce réseau véhicule plusieurs informations :

- les messages d'authentification et d'autorisation échangés entre les *supplicants* et le *serveur* ;
- la clé maîtresse de protection utilisée entre un *supplicant* et une borne d'accès sans fil ;
- les informations de journalisation échangées entre les *clients* et le serveur.

a. La confidentialité persistante est souvent désignée par l'acronyme PFS (*Perfect Forward Secrecy*).

### 3.2.1 Sécurité du serveur

Le *serveur* est l'élément critique d'un réseau 802.1X. Comme indiqué section 2.1.1, il contrôle l'ouverture de tous les ports de connexion offerts par les *clients*. Il est donc essentiel de limiter sa surface d'attaque afin de garantir son intégrité et sa disponibilité.

Les architectures virtualisées sont fortement présentes dans les systèmes d'information actuels. Malgré les nombreux avantages mis en avant par cette technologie, elle fait reposer le cloisonnement des applications sur des mécanismes logiques. Les scénarios d'attaque d'un service virtualisé sont donc plus nombreux que s'il est physiquement cloisonné (droits des administrateurs de l'hyperviseur, failles de l'hyperviseur, mémoire partagée entre services…). En conséquence, et conformément au guide [17] publié par l'ANSSI, la virtualisation du service RADIUS ne peut être réalisée que sur un hyperviseur hébergeant des services d'une même zone de confiance, ayant entre autres :

- les mêmes besoins de sécurité (confidentialité, intégrité, disponibilité) ;
- le même niveau d'exposition, c'est-à-dire accessible depuis des zones et par des personnes d'un niveau de confiance homogène.

**R10**

#### Protection du serveur

Il est recommandé d'implémenter le rôle de *serveur* sur une machine physique dédiée ou sur un socle virtualisé hébergeant des services soumis à un niveau d'exposition et à des besoins de sécurité identiques.

**R11**

#### Durcissement du système

La configuration du système sur lequel est installé le service RADIUS doit être durcie

La recommandation R11 s'inscrit dans un principe de défense en profondeur afin de retarder une compromission du *serveur* et de limiter une élévation de privilèges menant à un accès privilégié au système d'information. Le lecteur est invité à se référer au guide [8] publié par l'ANSSI pour durcir la configuration d'un système reposant sur GNU/Linux.

#### Attention

L'application des recommandations R10 et R11 est primordiale. L'utilisation de protocoles d'authentification par mots de passe nécessite que le serveur accède aux mots de passe des utilisateurs (ou à leur empreinte) pour vérifier la réponse au challenge envoyé. Dans le cadre d'un réseau Wi-Fi, un attaquant situé à proximité de la borne d'accès peut alors interagir avec le *serveur*. La compromission de ce dernier peut donc amener à une fuite immédiate des identifiants de connexion de l'ensemble des utilisateurs.

**R12**

#### Redondance des serveurs

Il est recommandé de disposer au minimum de deux *serveurs* dans le réseau de confiance pour répondre à un besoin nécessaire de disponibilité du service.

L'application de la recommandation R12 est facilitée par la possibilité d'enregistrer deux *serveurs* distincts dans la configuration de la grande majorité des équipements *clients* (commutateurs, points d'accès sans fil…). La mise en place de mécanismes de redondance plus évolués n'est dans ce cas pas nécessaire.

Selon les scénarios de déploiement, les *serveurs* peuvent être liés à différents services indispensables à leur fonctionnement (bases de données, annuaires…). Il convient dans ce cas de s'assurer que tous les éléments nécessaires au fonctionnement du service sont redondés.

### 3.2.2 Cloisonnement des flux

Les flux circulant dans le *réseau de confiance* sont uniquement des flux de service échangés entre les *clients* et le *serveur*. Aucun autre flux n'est légitime sur ce réseau, en particulier les flux des utilisateurs. Il convient donc de s'assurer que les flux utilisateurs du système d'information ne circulent pas dans le *réseau de confiance*. Il est également essentiel de s'assurer que les réseaux d'administration du système d'information ne peuvent pas être atteints trivialement en cas de compromission du *réseau de confiance* ou du *serveur*.

**R13**

#### Cloisonnement des flux de fonctionnement

Il est fortement recommandé de cloisonner le *réseau de confiance* dans un réseau dédié, distinct des réseaux des utilisateurs et d'administration.

L'application de cette recommandation peut s'effectuer de différentes manières (câblage distinct, utilisation de VLAN…). Dans tous les cas, seuls les *clients* doivent pouvoir se connecter directement au service RADIUS présent sur le *serveur*. Les flux d'administration, de journalisation et de sauvegarde du *serveur* ne sont pas traités dans ce document, mais le lecteur peut se référer aux documents [13] et [17] pour approfondir le sujet.

Afin de réduire la surface d'attaque du *réseau de confiance*, il est important de mettre des barrières de sécurité pour en limiter la probabilité de piégeage. Les *clients* sont situés à la frontière de ce réseau, leur configuration doit donc être durcie, comme indiqué dans le document [10] publié par l'ANSSI.

### 3.2.3 Intégrité et confidentialité des messages

Dans le *réseau de confiance*, les données d'authentification sont échangées au travers d'attributs `EAP` dans des paquets RADIUS. Selon la RFC [7], tout message RADIUS contenant au moins un attribut `EAP` doit présenter un motif d'intégrité valide dans le champ *Message-Authenticator*. Il en est de même pour chaque message de journalisation échangé entre les *clients* et le *serveur* [30] (champ *Authenticator*).

Cependant, les fonctions cryptographiques utilisées pour calculer ces motifs d'intégrité reposent sur un secret partagé entre *clients* et *serveur* et sur la primitive cryptographique `MD5`, peu sûre et non conforme aux recommandations de l'ANSSI [18].

R14

## Gestion des secrets partagés

Afin d'assurer *a minima* l'intégrité des messages échangés entre le *serveur* et les *clients*, il est fortement recommandé :

- d'utiliser un secret partagé distinct par *client* ;
- de générer des secrets aléatoires d'au moins 22 caractères ASCII imprimables (majuscules, minuscules, chiffres) [a] ;
- de superviser l'utilisation de ces secrets partagés, pour détecter toute utilisation anormale (authentification erronée d'un *client*, modification des fichiers de configuration…) ;
- de renouveler ces secrets sur une base régulière, afin de réduire la possibilité d'un attaquant à forger des trames intègres à destination du *serveur* en cas de découverte de l'un des secrets.

### Information

La mise en place d'un système de supervision est importante. Elle permet de détecter les comportements anormaux et de limiter le renouvellement régulier des secrets partagés si aucun comportement anormal n'est détecté.
Cette supervision peut être réalisée de différentes manières : détection de modification de la base des mots de passe, détection des erreurs de connexion en provenance des *clients*, détection de connexions provenant d'adresses IP inconnues…

### Attention

Lorsque la supervision détecte une utilisation anormale, le renouvellement des secrets partagés doit être effectué.

Dans le cas d'un réseau sans fil, la clé maîtresse de protection des échanges entre le *supplicant* et le *client* est envoyée par le *serveur* au *client* dans un attribut `EAP` après authentification et autorisation du *supplicant*. Son intégrité est portée par le secret partagé entre le *serveur* et le *client*, comme indiqué précédemment. Sa confidentialité n'est cependant pas assurée dans le réseau de confiance. Un attaquant en écoute sur le réseau peut donc intercepter cette clé maîtresse et en dériver toutes les clés nécessaires pour déchiffrer le trafic d'un *supplicant*.

R15

## Protection physique du réseau de confiance

Il est recommandé de protéger les équipements et les câbles du réseau de confiance contre les intrusions.

Certains *clients* disposent d'un *supplicant* qui permet de les authentifier avant d'accéder au réseau. Il devient donc possible d'authentifier les clients avant de leur permettre d'accéder au *réseau de confiance*.

*a*. L'ensemble des majuscules, minuscules et chiffres représente un espace de 62 caractères. Le choix de 22 caractères aléatoires permet d'obtenir une entropie de 128 bits.

R15 +

### Authentification des clients

Dans un souci de défense en profondeur, il est recommandé d'authentifier les *clients* auprès du *serveur* pour qu'ils accèdent au *réseau de confiance*.

Les échanges qui interviennent sur le réseau de confiance ne sont pas protégés en confidentialité et leur intégrité est portée par une fonction cryptographique faible. L'utilisation d'un protocole de communication sécurisé sur ce réseau permettrait de limiter l'exposition des éléments qu'il transporte. Plusieurs solutions ont été proposées, mais aucune d'elle ne s'est imposée comme standard implémenté par tous les fournisseurs de *clients* et de *serveurs* :

- le protocole RadSec, défini dans la RFC expérimentale [34] permet de protéger les échanges RADIUS à l'aide du protocole TLS ;
- les paquets RADIUS utilisent le protocole UDP, ils peuvent être protégés à l'aide du protocole DTLS [29] ;
- la RFC 3579 [7] recommande d'implémenter le protocole IPsec pour protéger les échanges RADIUS/EAP.

R15 ++

### Protection des échanges sur le réseau de confiance

Il est recommandé d'utiliser un protocole de communication sécurisé entre les *clients* et le *serveur* pour assurer la confidentialité, l'intégrité et le non-rejeu des informations échangées sur le *réseau de confiance*.

Selon les mécanismes proposés par les équipementiers et les fournisseurs de solutions de contrôle d'accès réseau, le lecteur est invité à consulter les guides [16] ou [15] publiés par l'ANSSI. Ces documents fourniront des recommandations de mise en œuvre sécurisée des protocoles standards TLS et IPsec.

### Information

Dans certains cas, les flux RADIUS empruntent des réseaux non maîtrisés. Ce cas peut se produire lorsque les *serveurs* sont hébergés dans un site central et les *clients* dans sites satellites, reliés entre eux via Internet ou des réseaux loués. La protection des flux est alors nécessaire et doit être réalisée de façon identique à celle décrite dans le guide [17] publié par l'ANSSI.

## 3.2.4 Journalisation

La gestion des journaux d'évènements associés aux équipements du réseau de confiance est une fonction de sécurité essentielle. En fonctionnement nominal, une telle architecture ne génère pas de messages d'erreur, aussi la surveillance des journaux permet de détecter des comportements suspects, d'anticiper et de réagir à des compromissions.

R16

### Journalisation des évènements

Il est fortement recommandé de :

- mettre en œuvre une fonction de journalisation des évènements générés par une infrastructure 802.1X ;

- superviser les évènements générés pour anticiper et répondre aux menaces.

Le lecteur est invité à se référer au document [13] qui traite de la mise en place d'une architecture de journalisation dans un système d'information.

## 3.3 Affectation dynamique de VLAN

La technologie de réseaux locaux virtuels ou VLAN est définie dans le standard IEEE 802.1Q [2]. Initialement créée pour limiter le trafic de broadcast au sein d'un réseau local, elle permet de créer différents réseaux locaux sur des mêmes liens physiques. Chaque VLAN est identifié par un numéro unique au niveau de la trame Ethernet et les ports des commutateurs sont associés à un ou plusieurs VLAN. Un équipement connecté à un port peut ainsi communiquer uniquement avec les équipements connectés au(x) même(s) VLAN. La connexion à un équipement situé dans un autre VLAN nécessite alors du routage.

Cette technologie concourt donc à augmenter le niveau de sécurité d'une infrastructure réseau car elle permet de séparer (virtuellement) dès le niveau 2 de la couche OSI les équipements qui ne doivent pas communiquer entre eux. Il faut néanmoins garder à l'esprit que sa seule utilisation ne permet pas de garantir une sécurité optimale du réseau, en particulier contre des écoutes de trafic ou des attaques actives. De plus, le cloisonnement par VLAN n'apporte pas le même niveau de sécurité qu'un cloisonnement physique ou par des moyens cryptographiques.

La norme 802.1X permet au *serveur* de configurer le VLAN du port de connexion d'un *supplicant* en fonction de données fournies durant l'authentification. Parmi tous les critères utilisables, on peut citer l'identifiant utilisé par l'utilisateur pendant l'authentification, l'adresse IP du commutateur ou de la borne d'accès à l'origine de la demande, le numéro de port de connexion ou le nom du réseau sans fil. De cette manière, le *supplicant* se retrouve automatiquement connecté dans un VLAN spécifique, déclaré dans le *serveur*. Il est ainsi possible de créer une infrastructure modulaire où les VLAN de connexion des *supplicants* sont gérés de façon centralisée et affectés dynamiquement.

Bien que séduisante, cette solution présente quelques problèmes de sécurité. Le numéro de VLAN à utiliser est envoyé par le *serveur* au *client* via le réseau de confiance, dans un champ non protégé du paquet RADIUS. Un attaquant disposant d'un accès au *serveur* ou au *réseau de confiance* pourra alors modifier ce champ et le VLAN d'affectation de chaque *supplicant*.

De plus, l'utilisation de cette fonctionnalité rend dynamique la configuration des *clients*, pouvant entrainer à terme des dysfonctionnements. L'affectation statique de VLAN et l'authentification des *supplicants* reste la méthode la plus efficace pour assurer la sécurité du réseau.

**R17**

### Affectation statique de VLAN

L'affectation statique de VLAN doit être employée en priorité.

R17 -

### Affectation dynamique de VLAN utilisateurs

Dès lors que l'affectation statique de VLAN n'est pas possible et que les *clients* permettent de filtrer localement les VLAN attribués, il est recommandé de préférer l'affectation dynamique de VLAN utilisateurs à une absence de VLAN.
Les VLAN d'administration ne doivent jamais être affectés dynamiquement.

### Attention

La fonction de filtrage par les *clients* des VLAN attribués est primordiale. En cas de compromission du *serveur* ou du *réseau de confiance*, elle permet de limiter localement les VLAN affectables à une liste blanche de VLAN utilisateurs.

Le lecteur est invité à se référer aux guides [10] et [17] pour obtenir de plus amples informations sur la bonne mise en œuvre des VLAN dans un système d'information.

## 3.4 Limites du 802.1X

La mise en place d'un *réseau 802.1X* apporte plusieurs fonctions de sécurité, dont une traçabilité précise des accès réseau effectués. Les messages de journalisation permettent par exemple d'identifier précisément les modifications de branchements d'équipements et les violations de politiques de sécurité. Cependant elle ne permet pas de protéger le système d'information contre toutes les menaces envisageables.

### 3.4.1 Branchement de concentrateurs

En premier lieu, il est possible de connecter un concentrateur réseau entre le port contrôlé et le *supplicant* pour connecter des équipements supplémentaires. L'ouverture du port est assurée par le *supplicant*, permettant ainsi aux équipements connectés au concentrateur d'accéder au réseau. Pour pallier ce problème , il est nécessaire d'intervenir dès le niveau 2 de la couche OSI et de limiter le nombre d'adresses MAC pouvant communiquer sur un port.

R18

### Lutte contre les branchements de commutateurs

Il est recommandé de configurer les équipements réseaux pour qu'ils autorisent les connexions en provenance et à destination d'une seule adresse MAC par port.

L'application de la recommandation R18 permet de s'assurer qu'un seul équipement connecté à un commutateur pourra communiquer au travers du réseau. Si l'adresse MAC du *supplicant* est l'adresse autorisée sur le port du *client*, le *supplicant* est alors le seul à disposer d'une connectivité au réseau à accès contrôlé.

### 3.4.2 Utilisation d'un matériel spécifique

Il est également possible d'utiliser un équipement spécifique à faible coût pour contourner les mécanismes de sécurité apportés par le protocole 802.1X sur un réseau filaire. De façon schématique,

cet équipement est installé entre le port de connexion du *client* et le *supplicant* et il redirige le trafic EAPoL vers le poste légitime et le reste du trafic vers le poste illégitime pour lui fournir un accès au réseau. Ce type d'équipement a fait l'objet de nombreuses publications [23, 28].

### Attention

En l'absence de prise en charge du protocole MACsec, aucune contre-mesure simple ne permet de lutter efficacement contre un tel scénario d'attaque.

Pour mener à bien cette attaque, il est nécessaire que le *supplicant* s'authentifie. Cela implique donc soit un utilisateur malveillant, soit un piégeage du lien entre le *supplicant* et le port du *client*, soit une authentification automatique du *supplicant*.

Dans les deux premiers cas, l'objectif recherché consiste à fournir une connectivité réseau à un équipement tiers, non maîtrisé par les équipes en charge du système d'information. Cet équipement pourrait être utilisé pour explorer le réseau, à l'aide d'outils non présents sur le poste légitime ou pour exfiltrer des données. Dans ce cas, le cloisonnement du réseau et le contrôle d'accès aux services proposés sont des fonctions de sécurité essentielles, destinés à réduire les actions du poste illégitime.

R19

### Cloisonnement et supervision des réseaux utilisateurs

Il est conseillé de cloisonner et de superviser les services offerts aux utilisateurs et d'authentifier les accès à ces services.

L'application de la recommandation R19 n'empêchera cependant pas un poste illégitime d'émettre des trames sur le réseau, puisqu'il dispose d'une connectivité au travers du matériel spécifique. Cependant, elle restreint l'accès aux services aux seuls postes et utilisateurs légitimes en érigeant des barrières supplémentaires.

Plusieurs solutions permettent d'instancier la recommandation R19. Parmi elles, l'authentification des utilisateurs sur chaque service est une bonne pratique à mettre en œuvre dès qu'elle est disponible. Plusieurs protocoles d'authentification peuvent être envisagés : TLS [16], Kerberos… Il est également possible de déployer des tunnels IPsec [15] entre chaque *supplicant* et une passerelle afin de filtrer les flux illégitimes.

Dans le cas où le *supplicant* s'authentifie automatiquement sur le réseau, sans intervention de l'utilisateur, la problématique diffère. Ce mode de fonctionnement peut être recherché pour assurer par exemple l'administration et la mise à jour à distance des équipements quand aucun utilisateur n'est connecté. Dans ce cas, il peut être judicieux de séparer les services offerts après authentification automatique du poste de travail de ceux offerts après authentification de l'utilisateur. Un attaquant obtiendra alors un accès aux services de mise à jour, mais pas aux applications métier. Ce comportement peut être obtenu grâce à l'affectation automatique de VLAN détaillée §3.3 ou par les mesures techniques permettant de répondre à la recommandation R19.

R20

### Restreindre les services accessibles en authentification automatique

Il est recommandé de limiter au strict nécessaire les services offerts sur un *réseau à accès contrôlé* où les équipements se connectent de façon automatique.

L'application de la recommandation R20 permet notamment de limiter les vulnérabilités liées aux réseaux de téléphonie sur IP (ToIP [8]). En effet, ces équipements s'authentifient automatiquement au réseau pour assurer une continuité de service. Si le réseau de ToIP est mutualisé avec le réseau bureautique d'une entité, tout attaquant pourra trivialement accéder aux services offerts, même en l'absence d'utilisateurs. Dans ce cas, la limitation des services offerts passe par une séparation stricte du réseau de ToIP et du réseau bureautique.

La technologie `MACsec` [5] permet également de lutter contre le branchement de matériel spécifique sur un port à accès contrôlé. Elle assure une protection en confidentité et en intégrité des échanges entre le *supplicant* et le *client*. Le port physique du *client* est donc ouvert, mais le trafic réseau est géré par un port virtuel n'acceptant que les trames chiffrées et authentifiées. Cette technologie est cependant rarement implémentée dans les *clients* et dans les *supplicants* actuels.

## 3.4.3 Limite intrinsèque

Les recommandations présentées dans cette section permettent de lutter efficacement contre le branchements de d'équipements illégitimes, cependant elles montrent leurs limites dès lors que le *supplicant* peut être transformé en routeur (niveau 3 du modèle OSI).

R21

### Maîtrise des équipements

Il est indispensable de maîtriser la configuration des équipements qui se connectent légitimement à un *réseau 802.1X* pour assurer la sécurité du réseau et limiter les possibilités de connexion d'équipements non autorisés.

La maîtrise des configurations requiert une gestion des droits associés aux utilisateurs et une supervision des configurations des différents équipements. Le lecteur est invité à se référer aux documents [8, 9, 11, 12, 17] publiés par l'ANSSI pour obtenir des détails supplémentaires.

8. *Telephony over IP*.

# 4
# Supplicants

Nous présentons ici les *supplicants* intégrés dans les systèmes d'exploitation les plus couramment utilisés et les protocoles d'authentification recommandés qu'ils supportent. Les *supplicants* fournis par les constructeurs de cartes réseau ne sont pas présentés.

## 4.1 Microsoft Windows 7

Le système d'exploitation Windows 7 supporte les connexions à des réseaux 802.1X, qu'ils soient filaires ou sans fil. Le *supplicant* intégré implémente les protocoles d'authentification `EAP-TLS` et `PEAP`. Lorsque le protocole `PEAP` est utilisé, les méthodes d'authentification internes configurables sont `EAP-TLS` ou `EAP-MSCHAPv2`.

La gestion de l'authentification 802.1X est déléguée à deux services différents, suivant le type de connexion utilisé. Sur des réseaux filaires, celle-ci est réalisée par le service *Configuration automatique de réseau câblé*, non démarré par défaut. Sur des réseaux sans fil, cette tâche est dévolue au *Service de configuration automatique WLAN*, démarré automatiquement lorsqu'un ordinateur dispose d'une carte réseau sans fil.

## 4.2 Microsoft Windows 8 et supérieurs

En plus des protocoles supportés par Windows 7 (voir §4.1), Windows 8 et les versions plus récentes supportent le protocole d'authentification `EAP-TTLS` couplé avec plusieurs méthodes d'authentification internes dont `MSCHAPv2`, `EAP-TLS` et `EAP-MSCHAPv2`.

Suivant le type de réseau, le service en charge de l'authentification est soit *Configuration automatique de réseau câblé* soit *Service de configuration automatique WLAN*.

## 4.3 Apple iOS 8 et supérieurs

Les équipements fonctionnant sous iOS 8 et supérieurs peuvent être connectés à des réseaux sans fil à accès contrôlés (voir §3.1.3). Le *supplicant* implanté dans ce système d'exploitation supporte les protocoles d'authentification `EAP-TLS`, `PEAP-MSCHAPv2` et `EAP-TTLS-MSCHAPv2`.

La configuration du protocole `EAP-TLS` requiert la présence préalable d'un certificat de connexion dans le magasin de certificats du système d'exploitation. La configuration du protocole `EAP-TTLS-MSCHAPv2` s'effectue lors de la connexion à un réseau sans fil utilisant ce protocole.

## 4.4 Apple Mac OS X 10.10 et supérieurs

Les postes de travail disposant du système d'exploitation Mac OS X en version 10.10 ou supérieure disposent également d'un *supplicant* qui gère le contrôle d'accès à des *réseaux 802.1X*. Ce *supplicant* supporte les protocoles d'authentification les plus courants, dont `EAP-TLS`, `PEAP-MSCHAPv2` et `EAP-TTLS-MSCHAPv2`. Il se configure directement dans les préférences réseau.

## 4.5 Linux et dérivés

Les postes de travail tournant sous le système d'exploitation Linux peuvent également se connecter à des *réseaux 802.1X*. Le *supplicant* le plus répandu est `wpa_supplicant`, il permet de gérer les connexions à des réseaux filaires et sans fil. Il supporte la plupart des protocoles d'authentification existants, dont les protocoles `EAP-TLS`, `EAP-TTLS-MSCHAPv2` et `PEAP-MSCHAPv2`.

Les environnements de bureau les plus populaires disposent d'outils permettant de configurer graphiquement l'accès à des *réseaux 802.1X*. Ces outils sont en réalité des interfaces graphiques de l'utilitaire `wpa_supplicant`.

Le système d'exploitation Android utilise également l'utilitaire `wpa_supplicant` pour la connexion à des réseaux à accès contrôlé.

# 5
# Cas d'usage

## Objectif

Étudier différents cas d'usage afin de déterminer si la mise en place d'un contrôle d'accès permet d'améliorer le niveau de sécurité du système d'information.

Comme nous l'avons détaillé dans les chapitres précédents, la mise en œuvre d'un réseau à accès contrôlé nécessite une infrastructure spécifique, potentiellement complexe à mettre en œuvre (voir chapitres 2 et 3). Certains scénarios d'attaque, détaillés section 3.4 peuvent également mettre en défaut la protection apportée par ce protocole. Par exemple, en l'absence de support de la technologie `MACsec`, le déploiement du protocole 802.1X sur des réseaux locaux filaires ne permet pas de contrer la menace d'un utilisateur légitime malveillant.

Avant tout déploiement, il convient donc de s'assurer que le gain en sécurité est supérieur au coût de déploiement et de maintien en conditions opérationnelles et de sécurité de la solution. Les cas d'usage suivants, non exhaustifs, ont pour objectif d'illustrer des scénarios de déploiement afin d'aider à la décision de mise en œuvre de ce protocole. Il convient de noter que certaines situations peuvent être à l'intersection de plusieurs cas d'usage. Un arbre de décision est présenté dans la figure 5.1.

## 5.1 Déploiement d'un réseau local sans fil

Les réseaux sans fil chiffrent nativement les flux entre les équipements et la borne d'accès. Sur un réseau sans fil *personnel* (`WPA`, `WPA2`), tout équipement ayant légitimement accès au réseau peut déchiffrer les flux en provenance et à destination des autres équipements connectés. De plus, l'authentification d'un équipement ne peut être garantie puisque la clé d'accès est commune. Enfin, il est difficile de maîtriser la portée du réseau sans fil puisqu'elle dépend en grande partie de la sensibilité du récepteur.

Le protocole `WPA2-Enterprise` permet de cloisonner les flux des différents équipements connectés car les clés cryptographiques utilisées par les *supplicants* sont indépendantes entre elles. Sa mise en œuvre nécessite le déploiement d'un réseau à accès contrôlé.

**R22**

### Sécurisation d'un réseau local sans fil

Dès lors qu'un réseau sans fil doit être déployé, il est recommandé de mettre en œuvre le protocole 802.1X et d'appliquer les recommandations présentées §3.1.3.

## 5.2 Réseau filaire sans accès libre et non accessible à des individus potentiellement malveillants

On suppose ici que les équipements sont branchés suivant un plan de cablage précis et que les collaborateurs ne peuvent pas les brancher sur des prises en libre accès. Par ailleurs, les locaux étant sécurisés, le réseau n'est pas accessible physiquement à un individu malveillant.

Dès lors qu'aucun accès au réseau à protéger ne peut être atteint par un individu potentiellement malveillant, et puisque la menace d'un utilisateur légitime malveillant n'est pas retenue, le déploiement du protocole 802.1X n'est pas indispensable. L'application de la recommandation R18 sur la limitation du nombre d'adresses MAC autorisées est cependant indispensable, afin de contrer la menace d'un l'utilisateur légitime non malveillant qui se tromperait de prise réseau.

### Attention

Les prises réseau brassées en avance et non reliées à des équipements doivent être traitées avec la plus grande précaution. En effet, en cas d'apprentissage dynamique des adresses MAC, le commutateur n'a pas encore enregistré d'adresse. Le premier équipement connecté sera donc autorisé à accéder au réseau.

R23

### Déploiement dans des conditions maîtrisés

Lorsqu'aucun accès au réseau à protéger ne peut être atteint par un attaquant, l'application de la recommandation R18 sur la limitation du nombre d'adresses MAC autorisées est indispensable. Les accès brassés en avance et non utilisés doivent être traités avec précaution :

- soit en désactivant l'apprentissage automatique de l'adresse MAC, ce qui nécessite une action d'administration avant le premier branchement ;
- soit en déployant le protocole 802.1X.

La décision de déploiement du protocole 802.1X est du ressort des équipes en charge de la sécurité du réseau à protéger, en fonction des contraintes métier et des services offerts.

## 5.3 Réseau filaire en accès libre aux collaborateurs

On suppose ici que certains ports d'accès au réseau à protéger peuvent être en accès libre et les équipements qui s'y connectent varient. Par ailleurs, les locaux étant sécurisés, le réseau n'est pas accessible physiquement à un individu malveillant.

Dans ce cas, la recommandation R18 (limitation du nombre d'adresses MAC) n'est pas applicable et la recommandation R17 (affectation statique de VLAN) peut être inadaptée car elle restreint la connectivité de chaque prise d'accès à un seul réseau virtuel.

La configuration des commutateurs doit alors s'adapter rapidement pour fournir l'accès aux services réseau à la personne qui se connecte. La mise en œuvre du protocole 802.1X et de la recom-

mandation R17- (affectation dynamique de VLAN) apporte ici une souplesse d'utilisation tout en limitant l'exposition des services aux seuls postes authentifiés.

### Attention

Considérer que tous les ports d'un système d'information sont en accès libre et activer globalement l'affectation dynamique de VLAN n'est pas une bonne pratique. Cela confère au serveur RADIUS un rôle critique qu'il ne doit pas porter en raison de l'absence de sécurité dans les protocoles de communication qu'il utilise.
Cette mauvaise pratique rend également dynamique la configuration des commutateurs du système d'information et peut amener à l'utilisation de protocoles dangereux, non recommandés par l'ANSSI [10] et à la perte de maîtrise du système d'information.

R24

### Gestion des prises en accès libre

Il est recommandé de mettre en œuvre le protocole 802.1X sur les ports de connexion en accès libre aux collaborateurs. Dans ce cas, il est nécessaire d'appliquer la recommandation R17- portant sur l'affectation dynamique de VLAN et de se conformer aux recommandations du document [10].

## 5.4 Réseau filaire accessible à des individus potentiellement malveillants

On suppose ici que des prises réseau inoccupées sont accessibles à un individu malveillant. En revanche, ce dernier ne peut manipuler aucun équipement authentifié. Ce cas est donc sensiblement différent de celui présenté 5.2. Il est dans ce cas essentiel de limiter l'accès aux seuls équipements authentifiés afin de limiter l'exposition du réseau.

R25

### Connexion possible d'individus malveillants

Si la sécurité physique de certains accès au réseau à protéger ne peut pas être garantie, il est recommandé de déployer le protocole 802.1X pour restreindre son accès aux seuls équipements authentifiés.

### Information

La recommandation R25 peut être par exemple utilisée pour limiter l'accès au réseau d'entreprise dans les salles de réunion. Certaines prises sont ainsi laissées en accès libre aux visiteurs alors que d'autres, bien identifiées, permettent la connexion au réseau de l'entreprise après authentification.

## 5.5 Accès temporaire d'un attaquant à un équipement authentifié

Contrairement au cas présenté section 5.4, on suppose ici qu'un attaquant peut accéder temporairement à un équipement authentifié. Dans ce cas, cet attaquant peut piéger les branchements, ce qui peut entrainer l'interception, voire la modification des communications. En l'absence de support du protocole `MACsec`, aucune mesure technique liée au protocole 802.1X ne permet de contrer cette menace.

La mise en place du protocole 802.1X est donc un choix de l'équipe en charge de l'exploitation et de la sécurité du réseau. En revanche, plusieurs précautions permettent de limiter les risques associés à cette menace.

**R26**

### Lutte contre le piégeage des accès réseau

Il est recommandé de procéder à une inspection visuelle régulière des câbles réseau.

**R27**

### Réduction des risques liés au piégeage des accès réseau

Il est recommandé d'appliquer les recommandations R18 (limitation du nombre d'adresses MAC autorisées), R19 (cloisonnement et supervision des réseaux utilisateurs) et R20 (restriction des services accessibles en authentification automatique) pour réduire les risques liés au piégeage des accès réseau.

## 5.6 Synoptique de décision

L'arbre de décision présenté figure 5.1 reprend les différents cas d'usage présentés dans ce chapitre et indique les actions à mener en priorité pour protéger l'accès au réseau local.

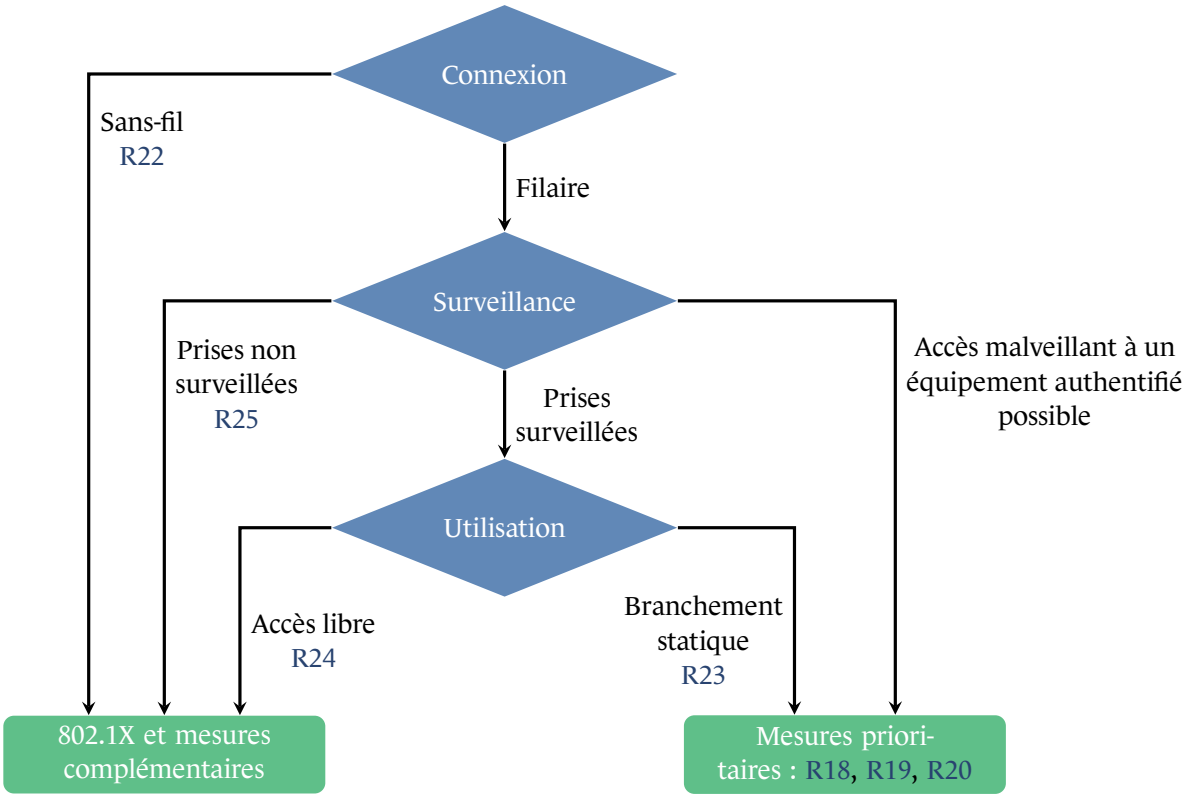


FIGURE 5.1 – Synoptique de décision de mise en œuvre du 802.1X.

# Liste des recommandations

# Bibliographie


[1] *IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control*.
*IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004)*, février 2010.

[2] *IEEE Standard for Information technology – Bridges and Bridged Networks*.
*IEEE Std 802.1Q-2014 (Bridges and Bridged Networks)*, août 2014.

[3] *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.
*IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, décembre 2016.

[4] *[MS-PEAP] : Protected Extensible Authentication Protocol (PEAP)*.
Open Specification Documentation v20160714, Microsoft Corporation, juillet 2016.
http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/%5BMS-PEAP%5D.pdf.

[5] *IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security - Amendment 3 : Ethernet Data Encryption devices*.
*IEEE Std 802.1AEcg-2017 (Amendment to IEEE Std 802.1AE-2006 as amended by IEEE Std 802.1AEbn-2011 and IEEE Std 802.1AEbw-2013)*, mai 2017.

[6] *Extensible Authentication Protocol (EAP)*.
B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz.
RFC 3748, RFC Editor, juin 2004.
https://tools.ietf.org/html/rfc3748.

[7] *RADIUS (Remote Authentication Dial In User Service) Support For Extensible authentication Protocol (EAP)*.
B. Aboba and P. Calhoun.
RFC 3579, RFC Editor, septembre 2003.
https://tools.ietf.org/html/rfc3579.

[8] *Recommandations de sécurité relatives à un système GNU/Linux*.
Note technique DAT-NT-002/ANSSI/SDE/NP v1.1, ANSSI, juillet 2012.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[9] *Déploiement et configuration centralisés d'EMET pour le durcissement des postes de travail et des serveurs Microsoft Windows*.
Note technique DAT-NT-027/ANSSI/SDE/NP v2.1, ANSSI, octobre 2016.
https://www.ssi.gouv.fr/emet.

[10] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://www.ssi.gouv.fr/nt-commutateurs.

[11] *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous windows*.
Note technique DAT-NT-013/ANSSI/SDE/NP v2.0, ANSSI, janvier 2017.
https://www.ssi.gouv.fr/windows-restrictions-logicielles.

[12] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*.
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/.

[13] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[14] *Recommandations de sécurité relatives aux réseaux WI-FI*.
Note technique DAT-NT-005/ANSSI/SDE/NP v1.0, ANSSI, septembre 2013.
https://www.ssi.gouv.fr/nt-wifi.

[15] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[16] *Guide TLS*.
Guide SDE-NT-035 v1.1, ANSSI, août 2016.
https://www.ssi.gouv.fr/nt-tls.

[17] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v2.0, ANSSI, avril 2018.
https://www.ssi.gouv.fr/securisation-admin-si.

[18] *RGS : Annexe B1 Mécanismes cryptographiques*.
Référentiel Version 1.0, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[19] N. Asokan, Valtteri Niemi, and Kaisa Nyberg.
*Man-in-the-Middle in Tunnelled Authentication Protocols*.
*IACR Cryptology ePrint Archive*, 2002 :163, 2002.

[20] *802.1X Authentication Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*.
Page web, CISCO, oct 2016.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xe-3se/3850/sec-user-8021x-xe-3se-3850-book/config-ieee-802x-pba.html.

[21] *Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE*.
Page web, CISCO, aug 2017.
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/sw8021x.html#79758.

[22] *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*.
P. Congdon, B. Aboba, A. Smith, G. Zorn, and J. Roese.
RFC 3580, RFC Editor, septembre 2003.
https://tools.ietf.org/html/rfc3580.

[23] *A Bridge Too Far – Deafeating Wired 802.1X with a Transparent Bridge Using Linux*.
Alva Duckwall.
Publication scientifique, août 2011.
https://www.defcon.org/images/defcon-19/dc-19-presentations/Duckwall/DEFCON-19-Duckwall-Bridge-Too-Far.pdf.

[24] *Licence ouverte / Open Licence*.
Page Web v2.0, Mission Etalab, avril 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

[25] *Diameter Base Protocol*.
V. Fajardo, J. Arkko, J. Loughney, and G. Zorn.
RFC 6733, RFC Editor, octobre 2012.
https://tools.ietf.org/html/rfc6733.

[26] *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)*.
P. Funk and S. Blake-Wilson.
RFC 5281, RFC Editor, août 2008.
https://tools.ietf.org/html/rfc5281.

[27] *How to configure 802.1X authentication on ProCurve switches*.
Page web, HP, jul 2008.
https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02642107.

[28] *802.1X Network Access Contrl and Bypass Techniques*.
Valérian Legrand.
Publication scientifique, juin 2017.
https://hackinparis.com/data/slides/2017/2017_Legrand_Valerian_802.1x/Network_Access_Control_and_Bypass_Techniques.pdf.

[29] *Datagram Transport Layer Security Version 1.2*.
E. Rescorla and N. Modadugu.
RFC 6347, RFC Editor, janvier 2012.
https://tools.ietf.org/html/rfc6347.

[30] *RADIUS Accounting*.
C. Rigney.
RFC 2866, RFC Editor, juin 2000.
https://tools.ietf.org/html/rfc2866.

[31] *Remote Authentication Dial In User Service (RADIUS)*.
C. Rigney, S. Willens, A. Rubens, and W. Simpson.
RFC 2865, RFC Editor, juin 2000.
https://tools.ietf.org/html/rfc2865.

[32] Bruce Schneier, Mudge, and David A. Wagner.
*Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)*.
In *CQRE*, volume 1740 of *Lecture Notes in Computer Science*, pages 192–203. Springer, 1999.

[33] *The EAP-TLS Authentication Protocol*.
D. Simon, B. Aboba, and R. Hurst.
RFC 5216, RFC Editor, mars 2008.
https://tools.ietf.org/html/rfc5216.

[34] *Transport Layer Security (TLS) Encryption for RADIUS*.
S. Winter, M. McCauley, S. Venaas, and K. Wierenga.
RFC 6614, RFC Editor, mai.
https://tools.ietf.org/html/rfc6614.

ANSSI-PA-043
Version 1.0 - 07/08/2018


**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN