# Les nouvelles normes

Apparition de nouvelles normes ➔

- IEEE 802.1x (fourniture de clé par un serveur d'authentification RADIUS)
- WPA (IEEE802.11 i transitoire)
- WPA2 (IEEE802.11 i)
- WPA3

# WPA (802.11 i transitoire)

## *Wi-Fi Protected Access*

- Authentification:
  - WPA définit deux modes:
    - WPA-PSK: utilisation de clé partagée (Pre Shared Key)
    - WPA-Entreprise: utilisation de serveur RADIUS
- Chiffrement:
  - TKIP (Temporal Key Integrity Protocol):
    - RC4 avec une clé de 128 bits
    - IV de 48 bits (au lieu de 24 bits).
    - Génération de clés de session.
    - Changement automatique de clés.
- Intégrité:
  - MIC (Message Integrity Check):
    - Champ de longueur 8 octets
    - Nouvel algorithme (léger, n'est pas consommateur de puissance).

# IEEE 802.1 x

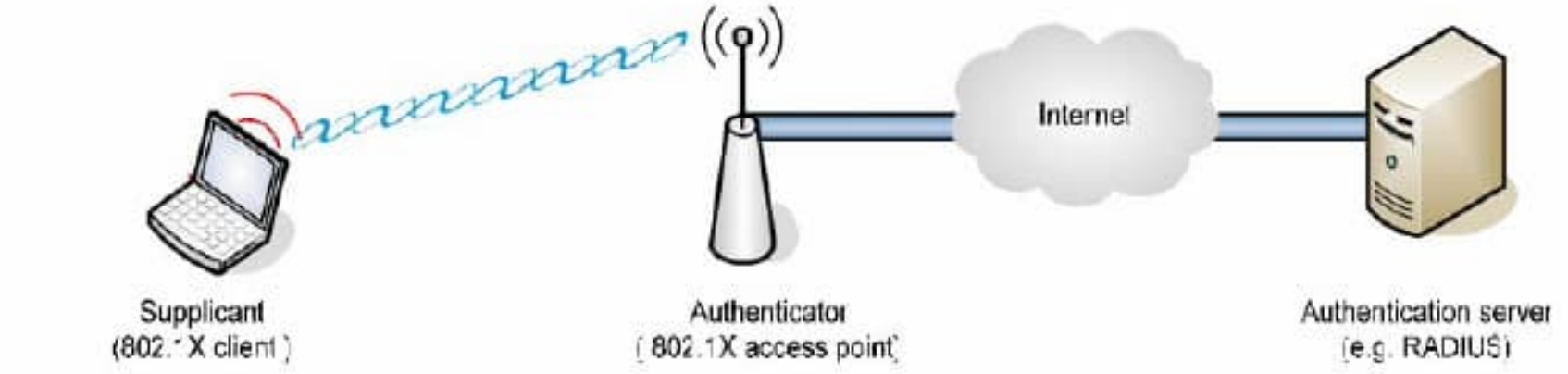
- Datant de 2001, est l'évolution de différents protocoles (PPP, RADIUS, EAP, 802.3, 802.5) développés pour l'authentification.
- Est une réponse au besoin d'authentifier les machines ou les utilisateurs connectés sur un réseau local
- Repose sur le protocole EAP (*Extensible Authentification Protocol*).
- Également appelé EAPOL (EAP Over Lan).

- Permet de changer les clés de chiffrement des utilisateurs de manière sécurisée.

# Acteurs 802.1x

Le protocole 802.1X définit trois catégories d'acteurs:

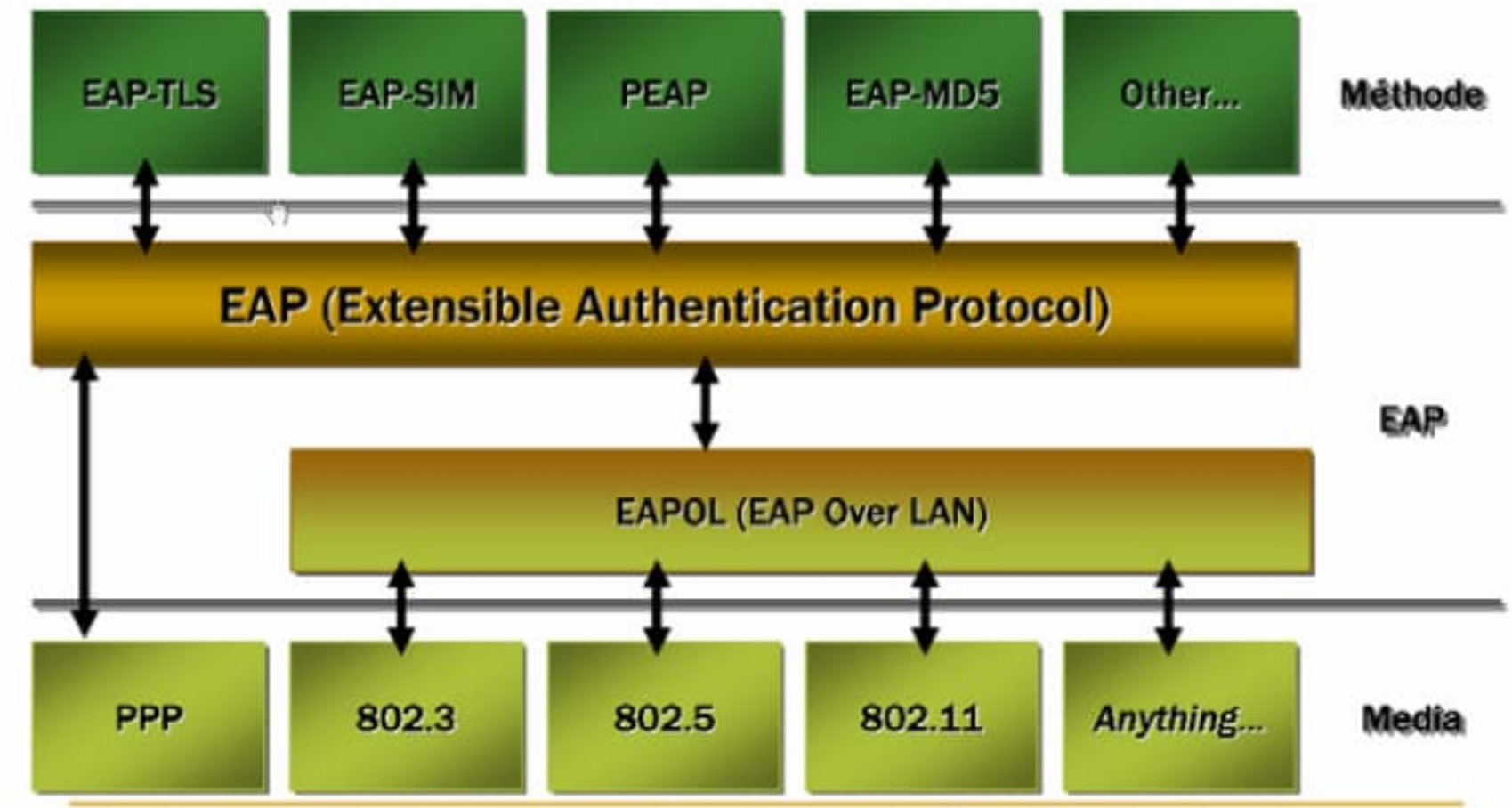
- Le supplicant : il s'agit du poste de travail qui demande à accéder au réseau.
- L'authenticator : c'est le dispositif Wi-Fi (client Radius) fournissant la connexion au réseau. Se comporte comme un contrôleur de port (autorisé/ non autorisé). C'est le point d'accès.
- Le serveur d'authentification : Il s'agit d'un serveur implémentant une solution Radius.



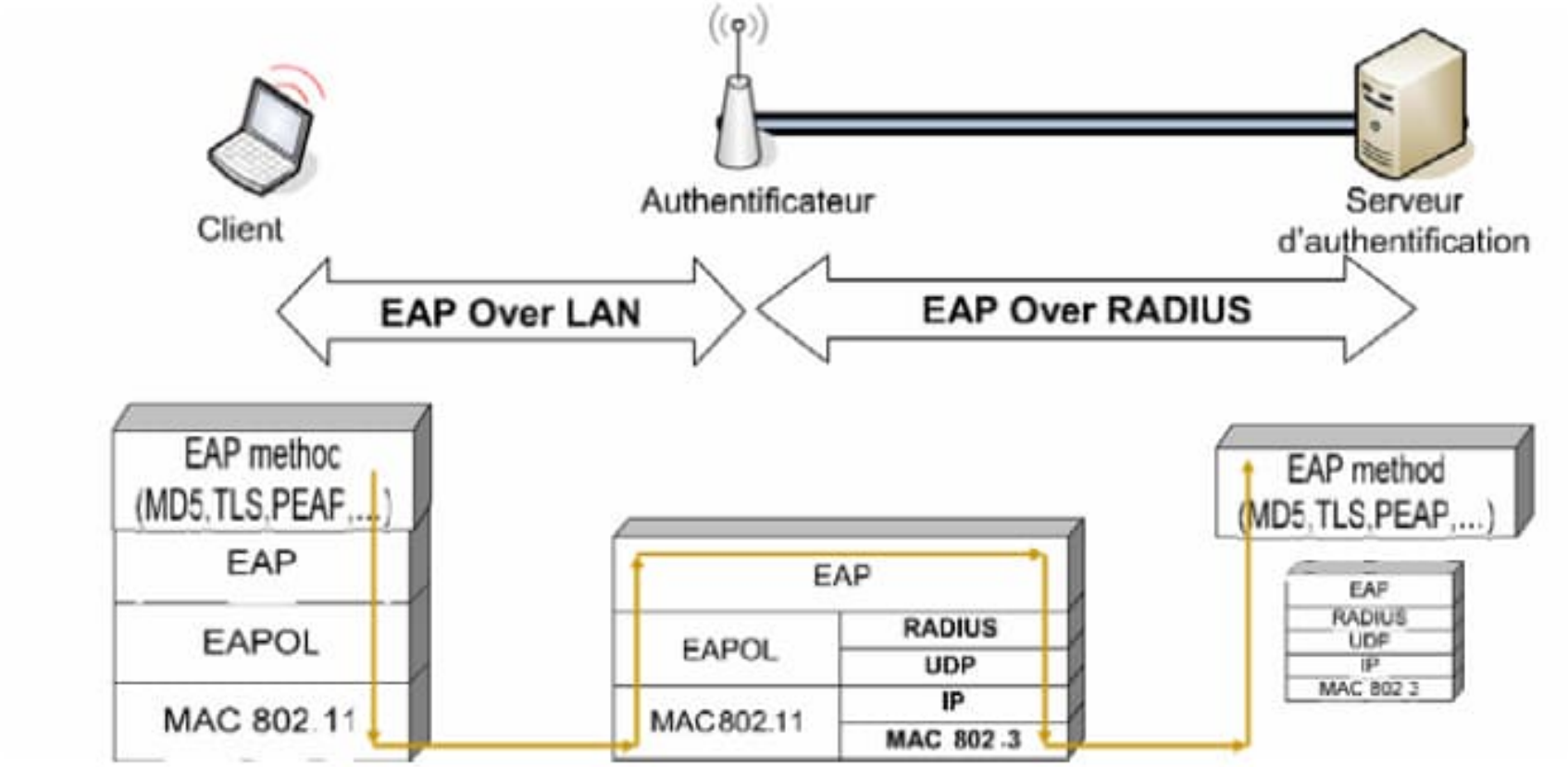
# Le protocole EAP

- Standardisé par l'IETF.
- EAP (Extensible Authentification Protocol).
- Protocole d'encapsulation pour l'authentification. Définit une infrastructure permettant d'héberger des méthodes d'authentification pour l'accès au réseau.
- Propose un format d'échange de messages afn de procéder à l'authentifcation d'un utilisateur auprès d'un serveur.
- Plusieurs méthodes EAP sont définies par l'IETF

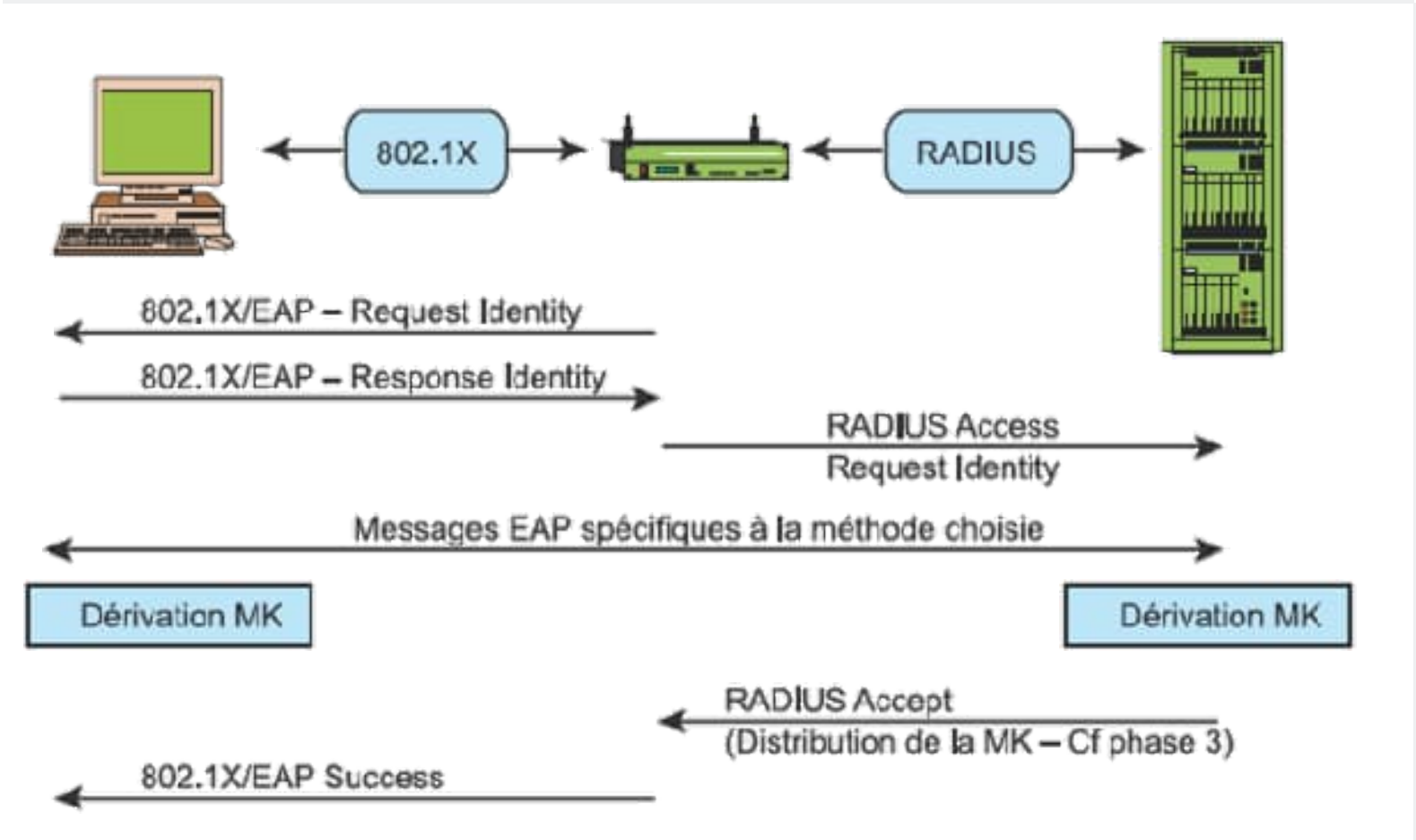
# Le protocole EAP (2)



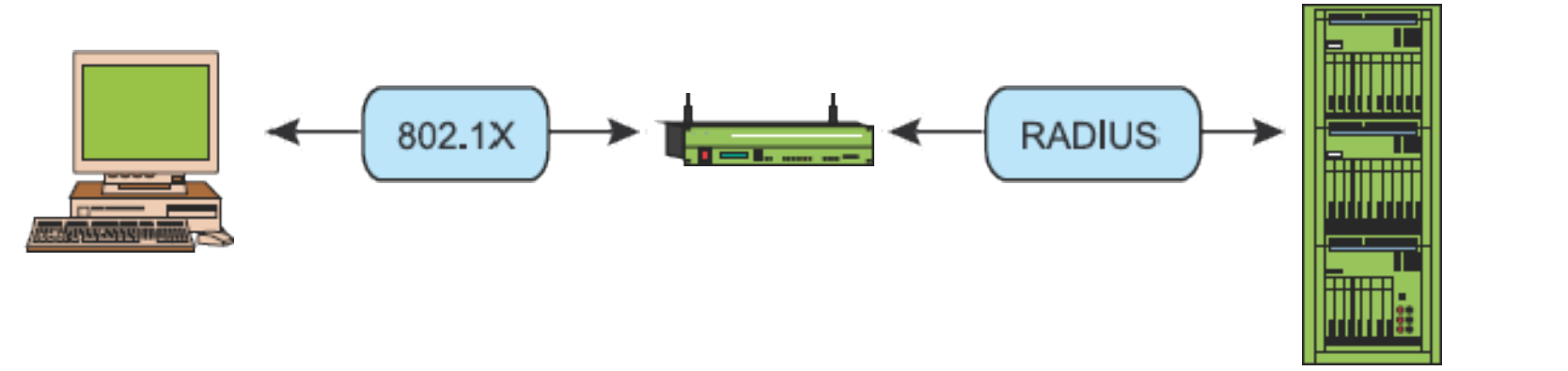
# Usage de EAP dans les réseaux 802.11



# Authentification IEEE802.1X



# Dérivation et Distribution de Clés




Pas 1 : Transmission de la MK de l'AS à l'AP

Pas 2 : 4-Way Handshake
Dérivation et distribution de la PTK et de la GTK

Pas 3 : Group Key Handshake
Dérivation et distribution de la GTK
(pour le renouvellement de la GTK)

# EAPOL

- Défini dans le standard 802.1X
- Spécifie la manière d'encapsuler EAP au dessus de la couche LAN (Ethernet, 802.11, …).
- Les 5 types de messages EAPOL sont:
  - EAPOL-Start
  - EPAOL-Key
  - EAPOL-PAcket
  - EAP-Logoff
  - EAPOL-Encapsulated-ASF-Alert

# RADIUS (Remote Access Dial-In User Service)

- 4 types de messages utilisés dans RADIUS:
  - Access-Request (NAS → AS)
  - Access-Challenge (NAS ← AS)
  - Access-Accept (NAS ← AS)
  - Access-Reject (NAS ← AS)

# EAP over RADIUS

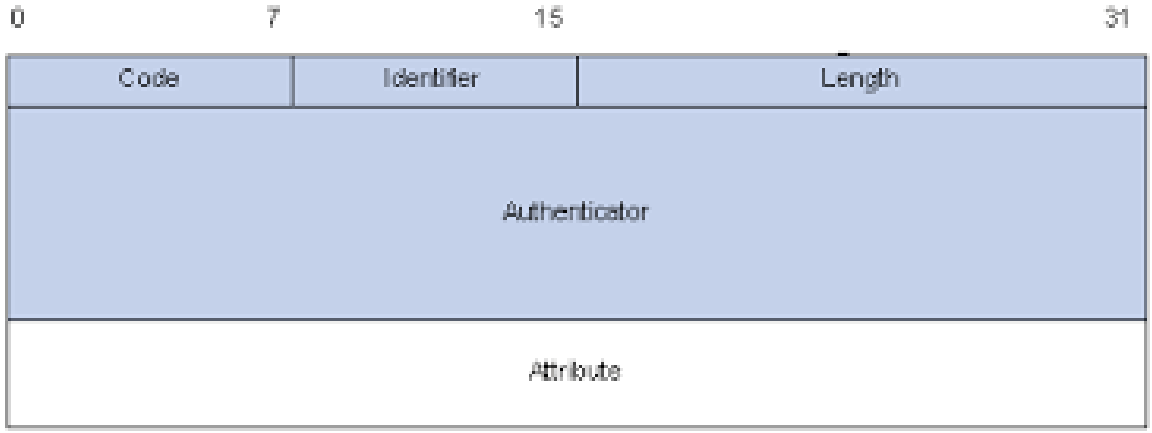
- Spécifie l'encapsulation de EAP au-dessus de RADIUS
- Les messages EAP-Request et EAP-Response sont encapsulés dans les messages Access-Request et Access-Challenge respectivement.

# Les alternatives

## Protocoles AAA (Authentification – Autorisation – Accouting)

- TACAS (Terminal Access Controller Access Control System)
- TACAS+
- Diameter

# Les paquets RADIUS



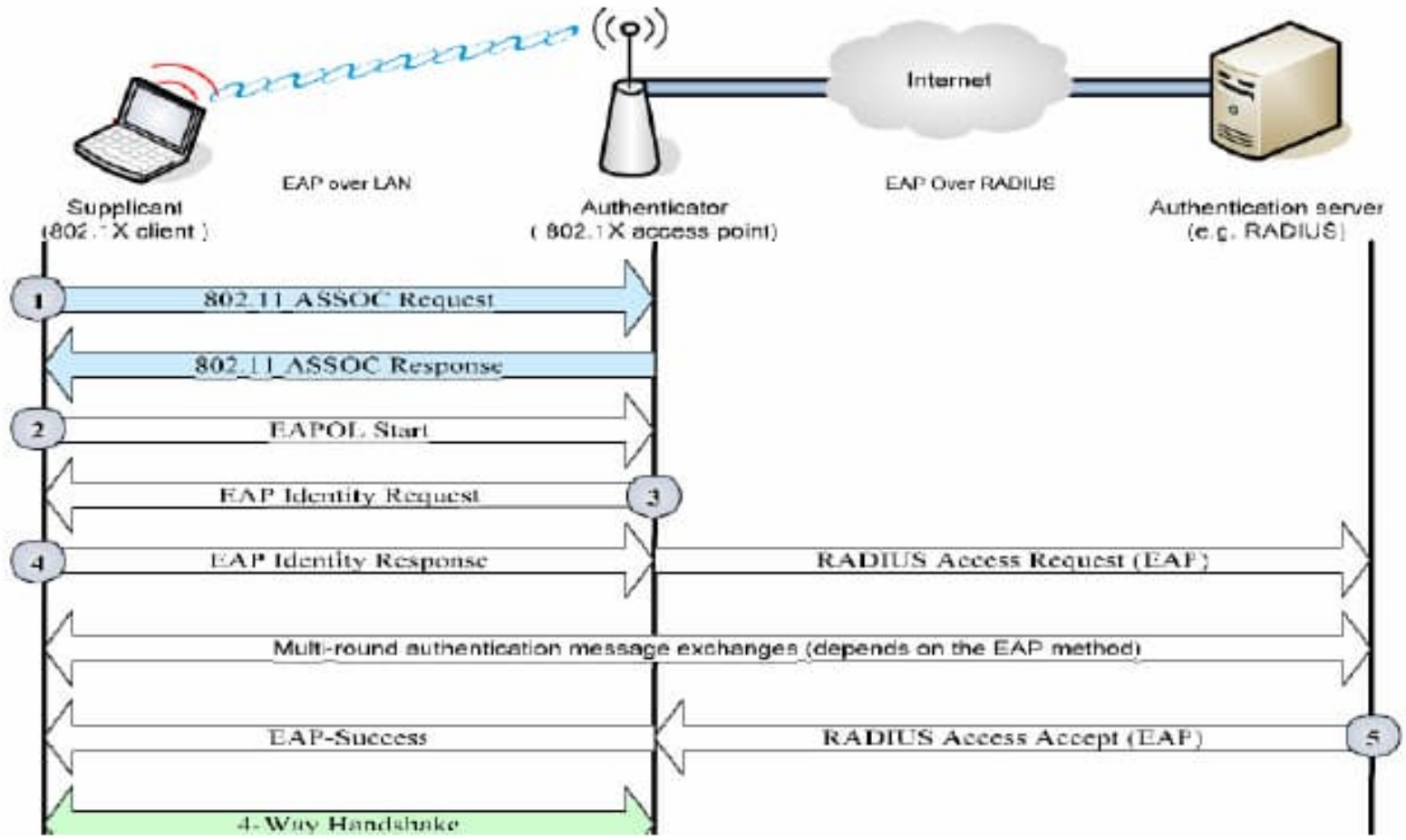

- 63 attributs
- Un attribut  Radius contient les 3 parties suivantes:

  Type: 1 Octet, identifie divers types d'attributs. Les codes d'attributs sont listés plus loin.

  Length: 1 Octet, longueur d'un attribut

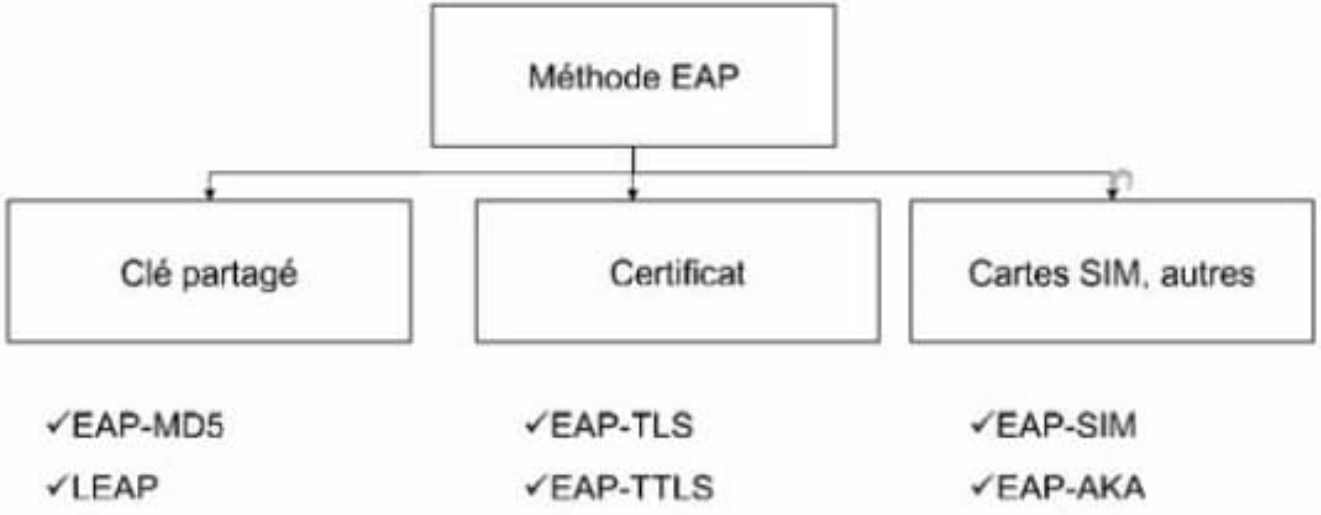
  Value: 0 ou+, contient les informations specifiques à l'attribut

# Processus d'uthentification 802.1X/EAP



# Les méthodes EAP

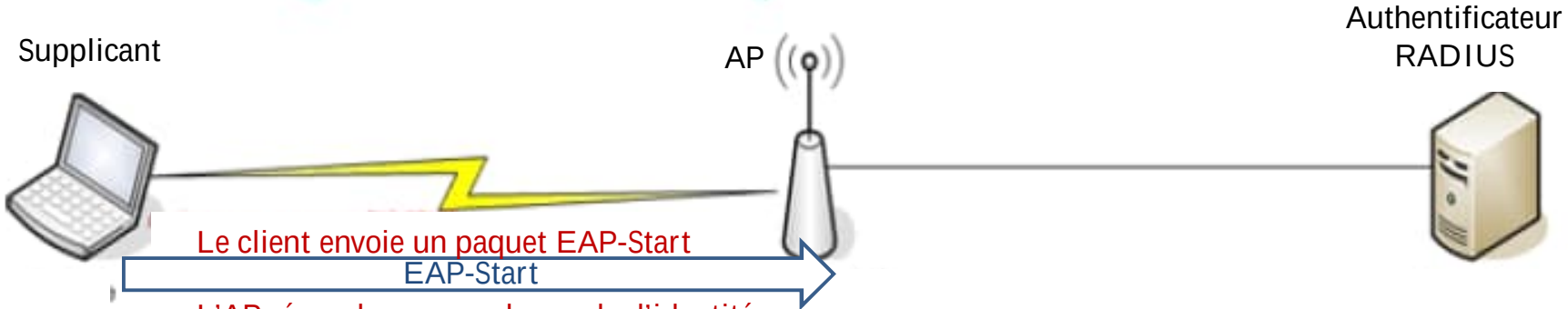
- EAP permet le transport des messages d'auhentification.
- Les méthodes EAP définissent :
  - Le processus d'authentification
  - Le format et les paramètres de ces messages
  - Les paramètres cryptographiques utilisés



# Les méthodes EAP (2)

- EAP-MD5: Le client est authentifié en envoyant le hach MD5 d'un challenge.
- LEAP (*Lightweight EAP*): propre à Cisco. Basé sur l'échange de défi et réponse.
- EAP-TTLS (*tunneled* Transport Secure Layer) : utilise TLS comme un tunnel pour échanger des couples attribut valeur à la manière de RADIUS11 servant à l'authentification.
- PEAP (*Protected EAP*): semblable à EAP-TTLS. Elle est développée par Microsoft. Elle se sert d'un tunnel TLS pour faire circuler de l'EAP.
- EAP-TLS(*Extensible Authentication Protocol-Transport Layer Security*): Le serveur et le client possèdent chacun leur certificat qui va servir à les authentifier mutuellement.

# Exemple d'échange EAP-TLS




Le client envoie un paquet EAP-Start

EAP-Start

L'AP répond avec une demande d'identité

EAP Request Identity

Le client envoie son identité (login, hostname,…)

EAP-Response

L'AP transfère la requête EAP-Response dans une demande d'accès RADIUS

Radius Access Request

Le serveur envoie son certificat

Radius X509 Certificate

Le client vérifie le certificat serveur et envoie son certificat

Client X509 Certificate

Le client génère une clé aléatoire et l'envoie en la chiffrant avec la clé publique du serveur Radius

Random Session Key

Le serveur génère une clé MK et l'envoie au client

Derive Key

Dérivation de la PMK À partir de MK

Dérivation de la PMK À partir de MK

Le serveur envoie un Radius Accept et installe la PMK chez l'AP

Radius accep & PMK

L'AP envoie un EAP Success

EAP-Success

# Comparaison des méthodes EAP

https://www.securew2.com/blog/eap-tls-vs-eap-ttls-pap

# WPA-PSK

- Repose sur des clés partagés : PMK (Pairwise Master Key) sur 256 bits .
- WPA accepte l'AP comme authentificateur.
- Une passphrase est alors configurée au niveau de chaque client.
- Ce mode d'authentification est utilisé pour les petits réseaux sans fil personnels.
- Utilise le même processus d'authentification basé sur les challenge que le WEP.

# TKIP

- WPA utilise le même moteur de cryptage WEP en modifiant la méthode de gestion des clés par l'utilisation du *Temporal Key Integrity Protocol.*
- Le changement de clé grâce à TKIP ➔ + de confidentialité.

- La gestion de clé passe par 3 étapes:
  - Echange des clés aléatoires et les adresses MAC entre les 2 nœuds sur EAPOL (*4-way handshake*)
  - La PMK sert de générateur des clés nécessaires pendant toute la session ➔ 3 clés Temporal Keys
  - Chiffrement

# TKIP (2)

## 1. Echange de clés aléatoires

A-nonce aléatoire

A-nonce

S-nonce aléatoire

Dérivation de la PTK

S-nonce + MIC

Dérivation de la PTK et calcul de la GTK

Message authentifié grâce à la KCK

GTK chiffrée + MIC

GTK cryptée avec la KEK

ACK MIC

Installation de la PTK et de la GTK

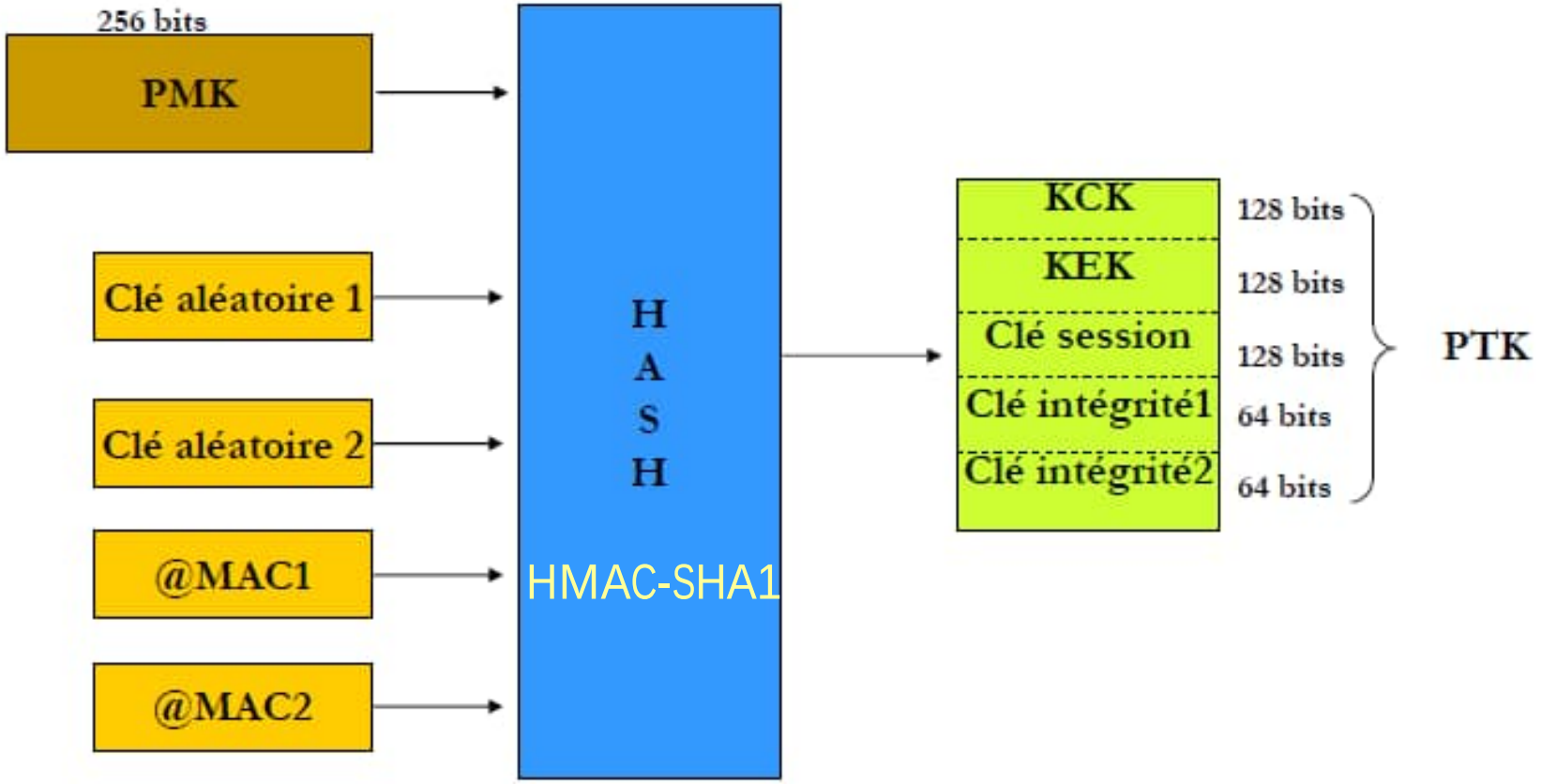
Installation de la PTK et de la GTK

# TKIP (3)

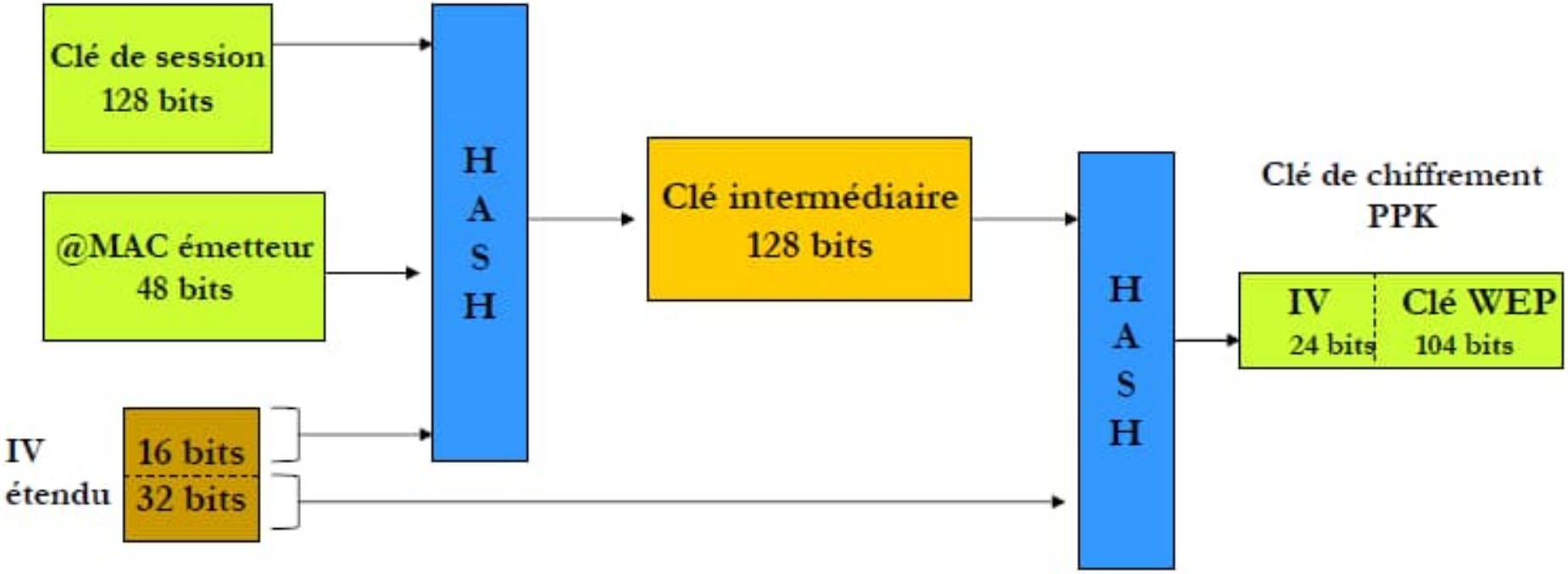
2. Génération des clés

- Obtention d'une clé *Parwise Transcient Key* (PTK) de 512 bits qui fournit:
  - Une *Key Confirmation Key* (KCK) qui sert à une partie de prouver à l'autre qu'elle possède la bonne PMK. C'est elle qui est utilisée pour l'authentification.
  - Une *Key Encryption Key* (KEK) qui sert à assurer la distribution de la clé de groupe,
  - Une clé de session, qui servira pour le chiffrement.
  - Deux clés d'intégrité : une pour chaque sens d'envoi d'informations .

## *Génération des clés*



## 3. Génération de la clé WEP (PPK: *Per Packet Key*)



# Le contrôle d'intégrité MIC *(Message Integrity Code/Check)*

- Remplace le contrôle CRC du WEP.
- Il est calculé sur toute la trame, y compris l'entête ➔ meilleure protection de l'entête contre ajout/ modification.

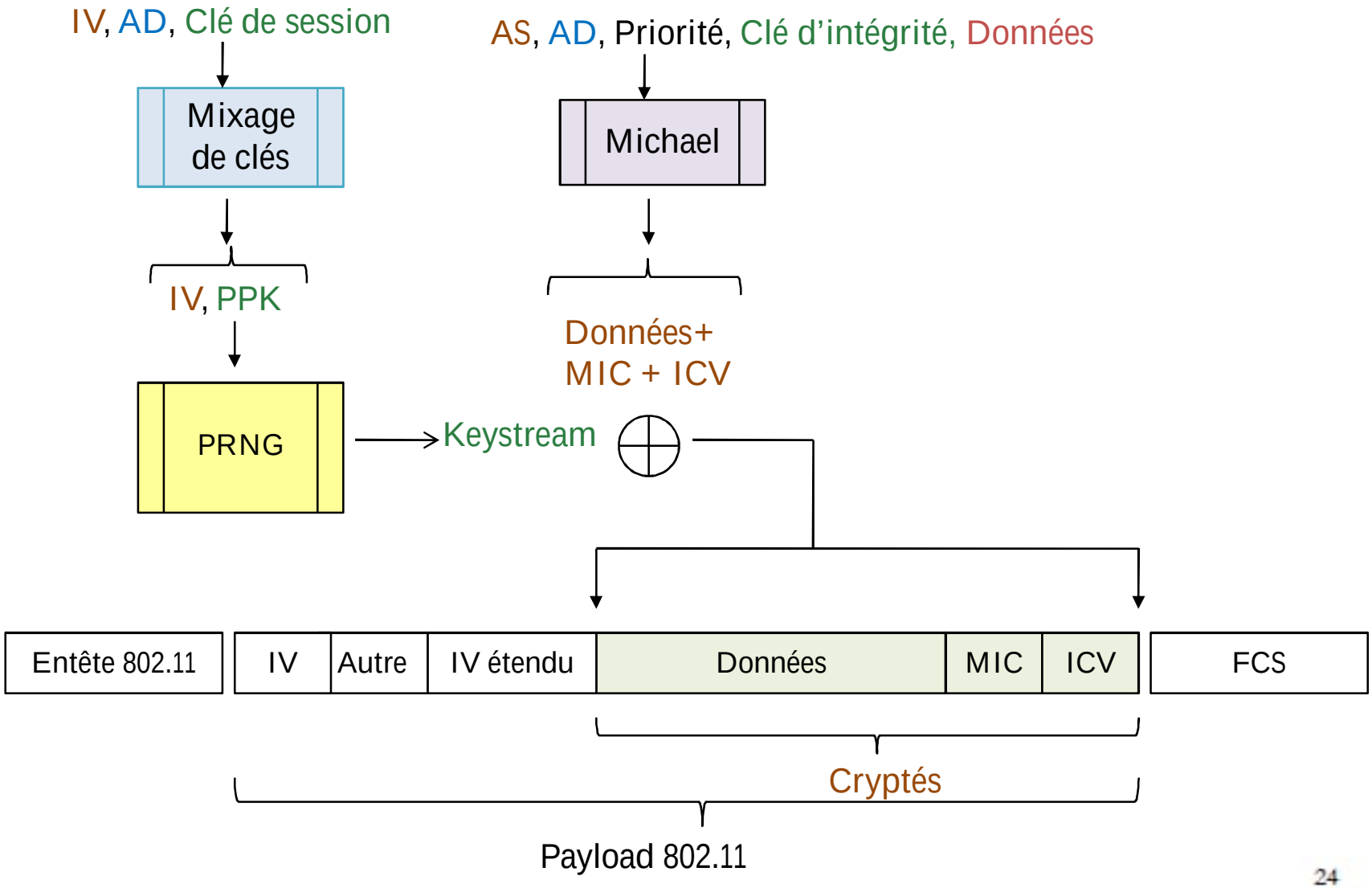
## Calcul du MIC

1. Calculer le MIC à partir de la trame claire complète et d'une des deux clés d'intégrité,
2. Le résultat est concaténé à la trame puis le tout est envoyé au moteur de chiffrement WEP (Un CRC32 est aussi calculé ).

# Cryptage WPA

1. Le IV, l'AD et la clé de session sont entrés dans une fonction de mixage de clés WPA qui calcule la clé de cryptage par paquet (PPK).
2. L'AD, l'AS, la valeur du champ Priorité, les données et la clé d'intégrité de données sont entrées dans l'algorithme Michael pour produire MIC.
3. La valeur de contrôle d'intégrité (ICV) est calculée à partir du total du CRC-32.
4. Le IV et la PPK sont entrés dans le PRNG RC4 pour produire une *keystream* de même taille que les données, le MIC et le ICV.
5. Un OU exclusif est défini entre la keystream et la combinaison Données + MIC + ICV pour produire la partie cryptée de la charge utile 802.11.
6. Le IV est ajouté à la partie cryptée de la charge utile 802.11 dans les champs de IV et de IV étendu, et le résultat est encapsulé avec un en-tête et un code de fin 802.11.

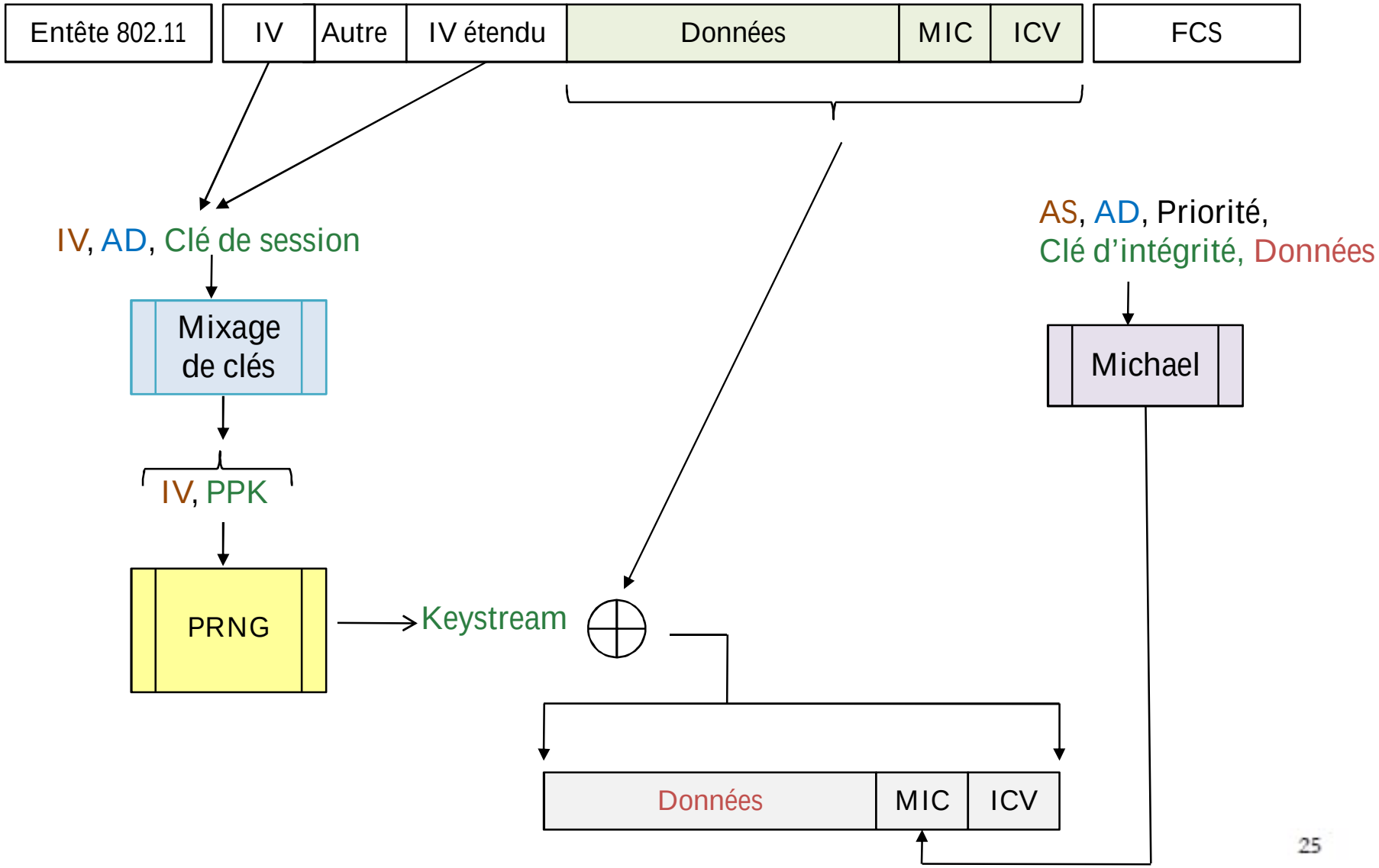
# Cryptage WPA



# Décryptage WPA

1. La valeur de IV est déduite des champs de IV et de IV étendu de la charge utile de la trame 802.11 et est entrée, avec l'AD et la clé de session, dans la fonction de mixage de clés, produisant la PPK.
2. Le IV et la PPK sont entrés dans le PRNG RC4 pour produire une *keystream* de même taille que les données, le MIC et la ICV cryptés.
3. Un OU exclusif est défini entre la *keystream* et les données, le MIC et la ICV cryptés pour produire les données, le MIC et la UCV non cryptés.
4. La ICV est calculée et comparée avec la ICV non cryptée. Si ces valeurs divergent, les données sont silencieusement rejetées.
5. L'AD, l'AS, les données et la clé d'intégrité de données sont entrées dans L'algorithme Michael pour produire le MIC.
6. La valeur calculée du MIC est comparée avec celle du MIC non crypté. Si ces valeurs divergent, les données sont rejetées. Si elles correspondent, les données sont transmises aux couches réseau supérieures pour traitement.

# Décryptage WPA



# Failles du WPA

- Possibilité de casser la clé PSK par « attaque dictionnaire » ou par « force brute » (Aircrack ou autre).
- Vulnérable à l'attaque DoS : envoyer des paquets non valides cause l'interruption de toutes les connexions (mécanisme de défense supplémentaire dans WPA) ➔ bloquer tout le réseau sans fil.
- Le SSID n'est toujours pas sécurisé.
- La désassociation n'est toujours pas sécurisée.
- Les faiblesses du cryptage RC4 déjà citées.

# 802.11i (RSN: Robust Security Network)

- Connu sous le nom de WPA2 (norme ratifiée en 2004).
- Supporte toutes les fonctionnalités de WPA
- Utilise un protocole de chiffrement beaucoup plus puissant que le TKIP, à savoir le CCMP (Counter Chaining Block Code-Message Authentication Code Protocol) basé sur AES (Advanced Encryption Standard).
- Se base aussi sur la norme 802.1x, visant à fournir des garanties de confidentialité élevée..
- AES n'est pas compatible avec l'ancien matériel (implémentation RC4).

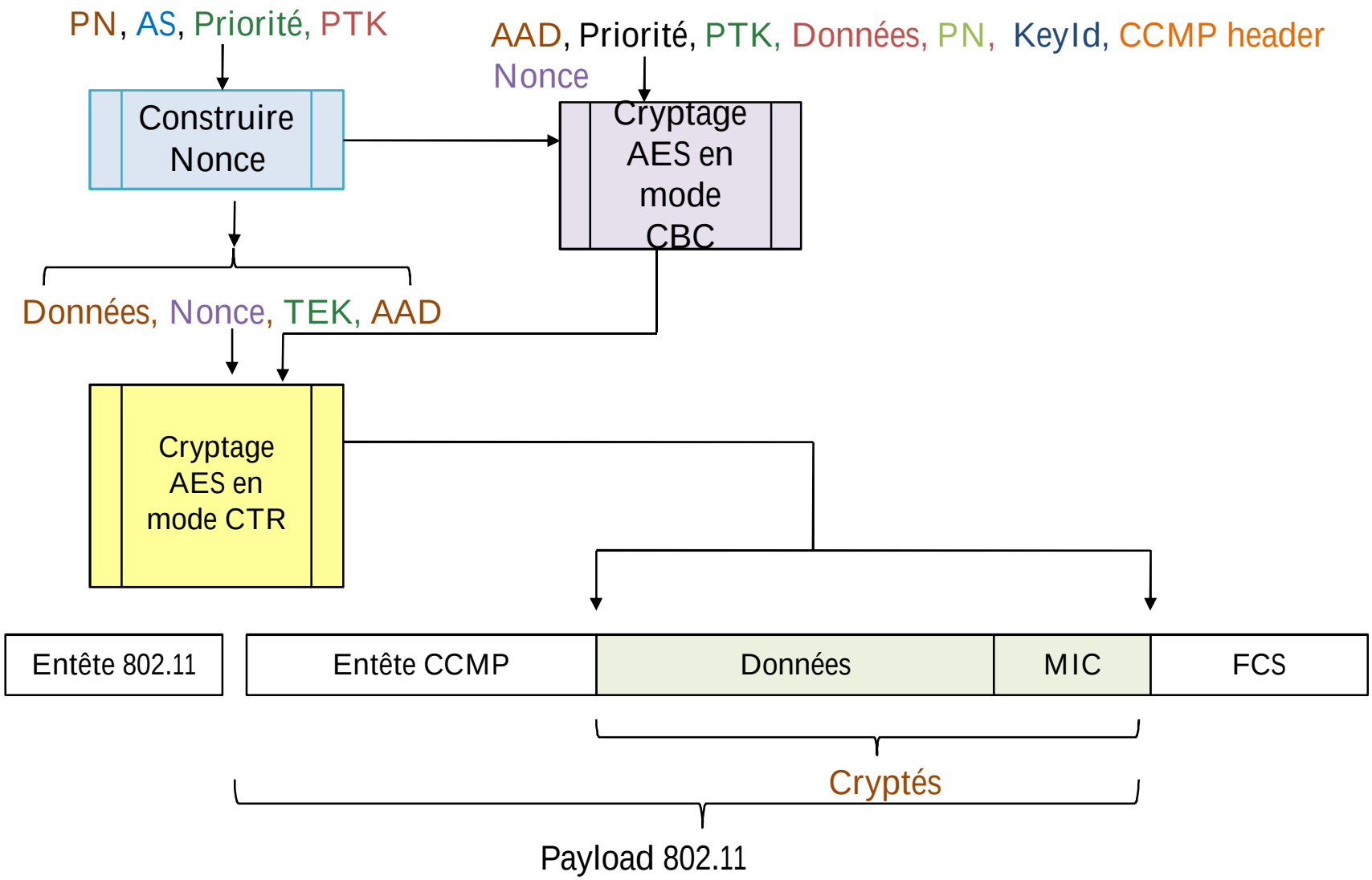
# Fonctionnement de WPA2

- Le fonctionnement de la norme 802.11i s'articule autour de quatre phases :
  1. La négociation de la politique de sécurité : qui s'opère entre le point d'accès et le client demandeur.
  2. L'authentification 802.1x, assuré à l'aide d'un serveur d'authentification, RADIUS par exemple.
  3. Les échanges de clés sous EAP.
  4. Le chiffrement des données, assuré par le protocole CCMP.

# Encapsulation de la trame CCMP

1. Incrémentation du numéro de paquet (PN : *Packet Number* ). Le PN est ainsi unique pour chaque MPDU. Ceci permet d'éviter les attaques de type rejeu. (PN=Ext IV)
2. Cryptage des deux champs d'adresses MAC pour authentifier la trame. Ce sont les informations additionnelles d'authentification (AAD : *Additional Authentication Data*).
3. Construction d'un vecteur d'initialisation (*CCM nonce block*) a partir du PN et du champ priorité dans la MPDU.
4. Cryptage du PN et de l'identifiant de la clef KeyId dans l'en-tête CCMP de huit octets.
5. Exécution du mode CTR de AES utilisant la clef temporaire TEK (*temporary Encryption key*), les AAD, le vecteur d'initialisation, et les données de la MPDU pour former le texte chiffré et le MIC.
6. Obtention de la MPDU chiffrée par concaténation de l'entête de la MPDU en clair, de l'en-tête CCMP, des données et du MIC chiffrés.

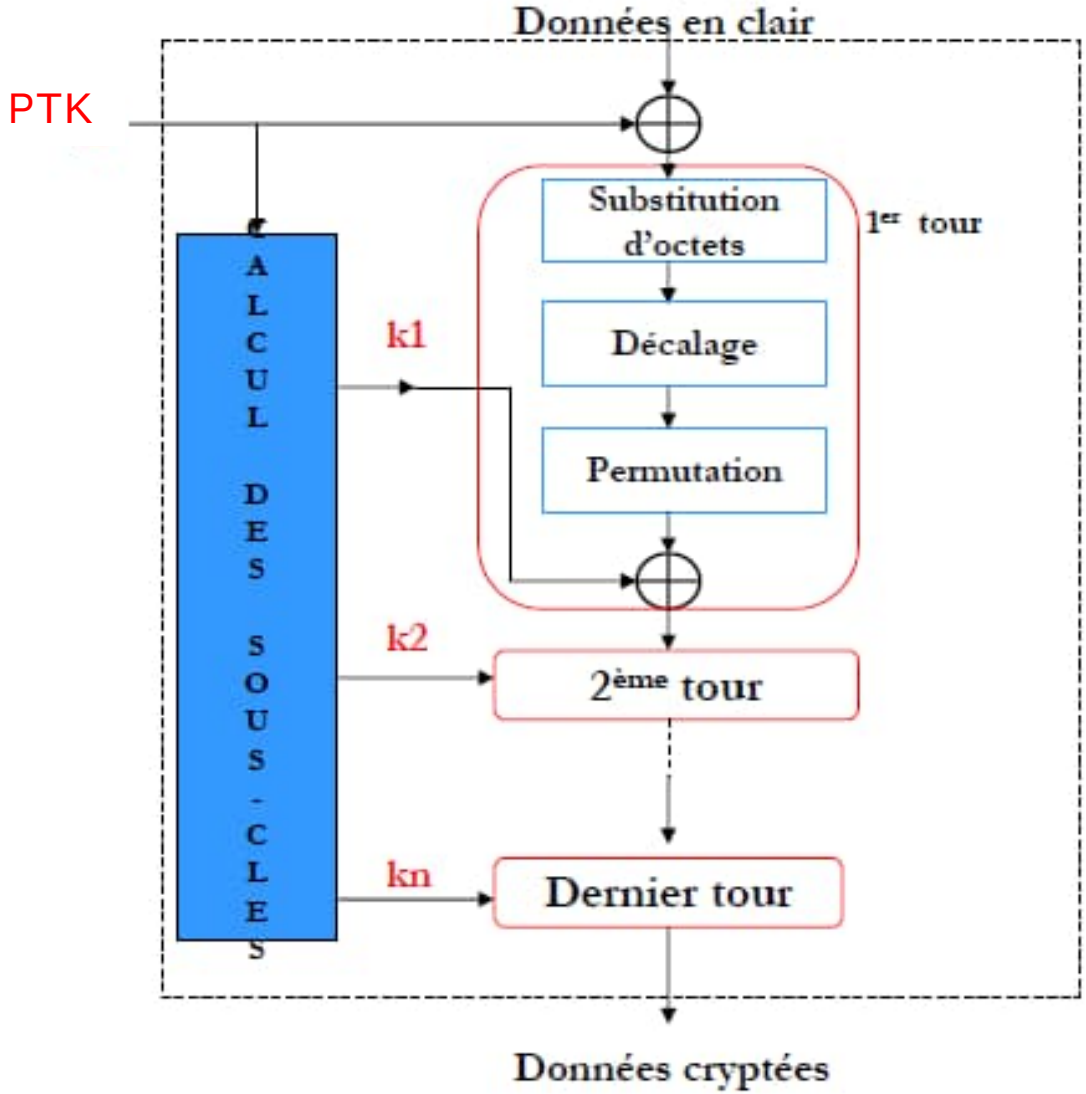
# Encapsulation de la trame CCMP (2)



# Chiffrement AES

- AES se sert pour le chiffrement de la clé de session PTK de façon rétroactive.
- AES fonctionne par chiffrements de blocs de 128 bits en gardant la même clé tout au long de la session. Le chiffrement par AES se fait en suivant une séquence de n opérations à partir de la PTK. La valeur de n sera le nombre de blocs à chiffrer.
- Etapes de chiffrement :
  1. Chaque bloc subit tout d'abord un XOR avec la clé fournie.
  2. Le résultat obtenu est crypté en 10 étapes (tours).
  3. Lors de chaque tour, le bloc passe successivement par une fonction de substitution d'octets, une fonction de décalage et une fonction de permutation.
  4. Le bloc subit enfin un XOR avec une clé dérivée de celle fournie.
  5. Le résultat sera alors prêt pour le tour suivant (ou éventuellement la sortie).

# Chiffrement AES (2)



# Calcul du MIC

Le calcul du MIC s'effectue de la manière suivante :

1. chiffrement du CCM nonce block pour obtenir le vecteur d'initialisation du mode CBC (IV : Initialisation Vector )
2. application d'un XOR entre cet IV et l'adresse source de la couche MAC, puis chiffrement du résultat
3. application d'un XOR entre le résultat précédent et l'adresse destination de la couche MAC, puis chiffrement du résultat
4. puis, pour chaque bloc de données de 128 bits, application de d'un XOR entre le résultat précédent et le bloc de données suivi d'un chiffrement du résultat
5. une fois tous les blocs de données traités, on obtient un bloc de 128 bits dont on ne garde que les 64 premiers pour former le MIC.

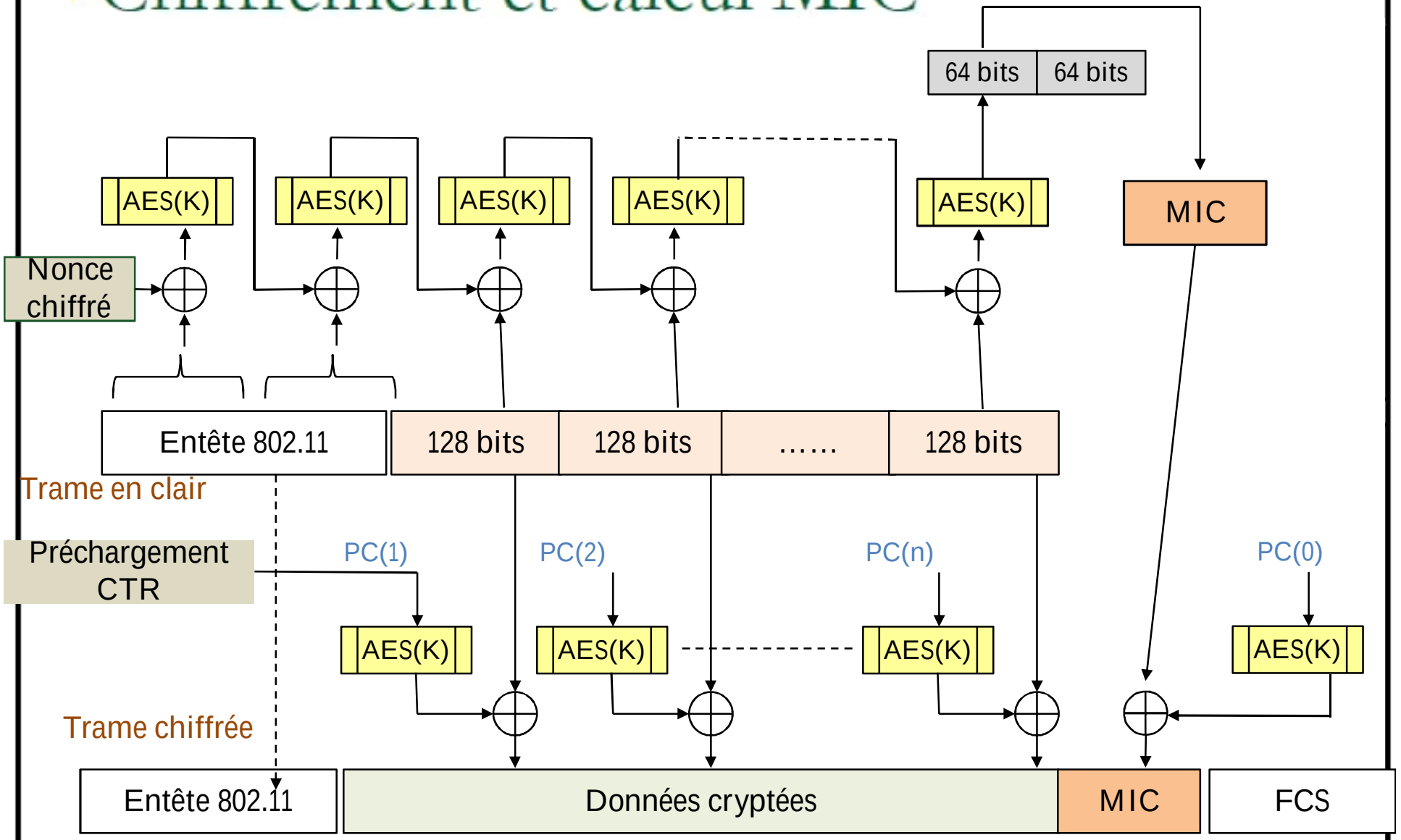
# Chiffrement de la MPDU

L'algorithme de chiffrement prend en entrée :

- la MPDU en texte clair concaténée au MIC
- le PN associé à la MPDU
- la clef temporaire TK.
- le CTR Preload, bloc de données contenant :
  - un octet de flags
  - un octet d'information de qualité de service
  - un champ d'adresse de six octets
  - le PN de la MPDU traitée
  - un compteur initialisé à 1 (PL)

- L'algorithme procède de la manière suivante pour chaque bloc de données de 128 bits de la MPDU :
  - incrémentation du PL
  - chiffrement du CTR Preload obtenu
  - application d'un XOR entre le CTR Preload chiffré et le bloc de données en cours de traitement.
  - Enfin, un XOR est appliqué entre le MIC et le CTR Preload ayant le PL à zéro.

# Chiffrement et calcul MIC



# Adaptabilité des méthodes de sécurité

| Cryptage | Utilisation | | |
|---|---|---|---|
| | Particulier | Petite entreprise | Grande entreprise |
| WEP | Acceptable | Déconseillé | Déconseillé |
| WPA-PSK | Adapté | Adapté | Acceptable |
| WPA-EAP | Excellent | Adapté | Adapté |
| WPA2-PSK | Adapté | Adapté | Acceptable |
| WPA2-EAP | Excellent | Excellent | Excellent |

# Solutions complémentaires pour la sécurité

# Mise en place d'un VPN

- Pour toutes les communications nécessitant un haut niveau de sécurisation, il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel (VPN).
- Les réseaux privés virtuels (VPN : Virtual Private Network) permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées.
- Le principe du VPN est basé sur la technique du tunnelling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. La source peut ensuite éventuellement chiffrer les données (on parle alors de VPN chiffrés) et les achemine en empruntant ce chemin virtuel.
- Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le protocole de tunnelling encapsule les données en rajoutant une entête. Permettant le routage des trames dans le tunnel. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de décapsulation.

# VPN

**Principe de fonctionnement d'un réseau privé virtuel (VPN).**