HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Groupe Sécurité Unix et Réseau
14 Juin 2005

WPA / WPA2
Une sécurité fiable pour le Wi-Fi ?

Guillaume Lehembre
<Guillaume.Lehembre@hsc.fr>

Plan

- Rappels 802.11, WEP et 802.1x
- Les nouvelles technologies en sécurité : WPA et 802.11i
  - WPA
  - 802.11i
  - Phase opérationnelles du 802.11i
    - Négociation de la politique de sécurité
    - Authentification 802.1x
    - Échange de clé sous EAP
      - Hiérarchie PMK / GMK
      - Les différents HandShake : 4-Way Handshake, Group Key Handshake et STAKey Handshake
    - Chiffrement et intégrité des données : TKIP, CCMP, MIC
  - Faiblesses ?
  - Itinérance
- Conclusion

Principe du 802.11

- Composants :
  - Borne ou point d'accès (AP)
    - Concentrateur sans fil, potentiellement aussi un pont et un routeur
  - Carte réseau (NIC)
    - Interface Ethernet sur l'équipement
- Deux modes
  - Mode '*ad-hoc*' : dialogue direct entre deux interfaces (point à point)
    - IBSS : Independant Basic Service Set
    - Réseau maillé
  - Mode '*infrastructure*' : dialogue entre une interface et une borne (multi-point)
    - BSS : Basic Service Set
    - Réseau en étoile
- 14 canaux
  - Plusieurs réseaux peuvent cohabiter au même endroit sur des canaux différents

Principe du 802.11

- Chaque réseau est identifié par un SSID : identificateur du réseau
  - Plusieurs réseaux avec des SSID différents peuvent cohabiter au même endroit sur le même canal
- Une interface Ethernet sans fil 802.11 est similaire à une interface Ethernet filaire 802.3
  - 802.11b : CSMA/CA, 802.3 : CSMA/CD
  - Vision identique pour les ordinateurs et pour TCP/IP
  - Adressage MAC identique
    - Adresses des bornes en plus : 4 adresses MAC au lieu de 2 dans la trame
- WEP (*Wired Equivalent Privacy*)
  - Permet (en théorie) d'assimiler un réseau Ethernet sans fil à un réseau Ethernet filaire en assurant une sécurité équivalente à celle d'un câble
  - Implémentation faite sans consultation préalable avec des cryptographes

Eléments d'architecture

- BSS : *Basic Service Set*
  - Ensemble de services de base
- IBSS : *Independant Basic Service Set*
  - Stations communicant entre elles, pas de planification, éphémère
- DS : *Distribution System*
  - Représente l'interconnexion de plusieurs BSS
- AP : *Access Point*
  - Donne accès au DS en fournissant des services, STA commes les autres
- STA : *Station*
- ESS : *Extended Service Set*
  - DS + ensemble BSS du même SSID

MPDU / MSDU

- MSDU : Mac Service Data Unit
  - paquet de données envoyé par l'applicatif à la couche MAC
- MPDU : Mac Protocol Data Unit
  - paquet de données envoyé par la couche MAC à l'antenne

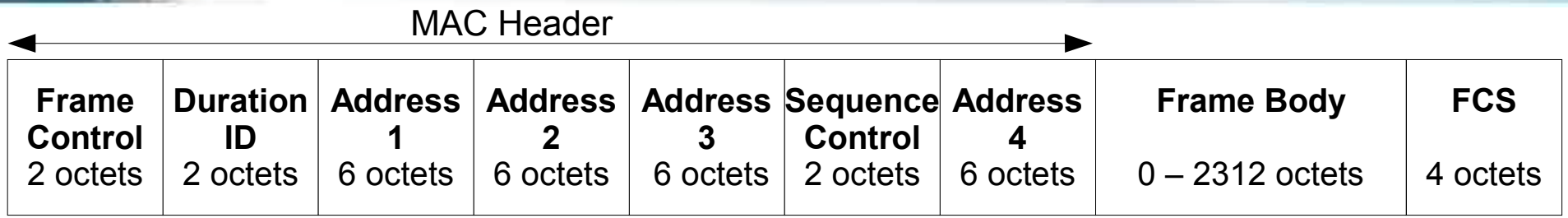
- Point important : Un MSDU peut être fragmenté en plusieurs MPDU

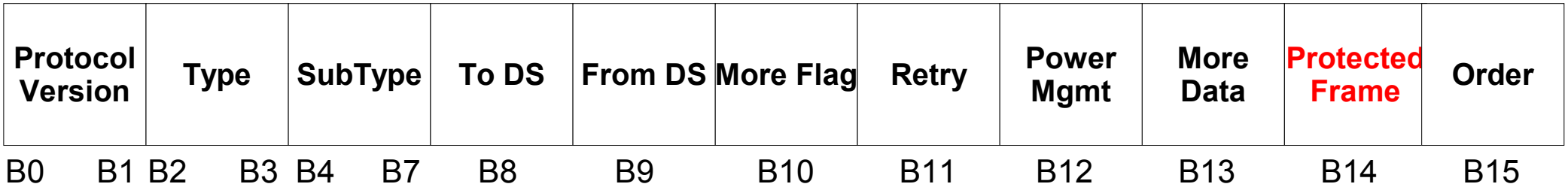
- Cette distinction a son importance pour TKIP (WPA) et CCMP (WPA2)
  - Pour TKIP, le MIC est calculé sur le MSDU
  - Pour CCMP, le MIC est calculé sur chaque MPDU

Association / Authentification

- Association
  - Enregistre la station auprès de l'AP
  - Obtention d'une AID (*Association Identity*) partagée entre chaque AP de l'ESS, permettant la ré-association transparente au sein de l'ESS
  - Toujours inititiée par la station
  - Equivalent de la connexion physique pour le filaire
- Authentification
  - Action de prouver son identité afin de faire partie du BSS ou ESS
  - Deux méthodes d'authentification :
    - ouverte (*Open Authentication*) : authentification nulle
    - à clef partagée (*Shared Key Authentication*) : utilise la clé WEP pour chiffrer un défi en clair envoyé par la borne - **A NE JAMAIS UTILISER**
  - La dé-authentification peut être inititée par la station ou l'AP

Trame 802.11





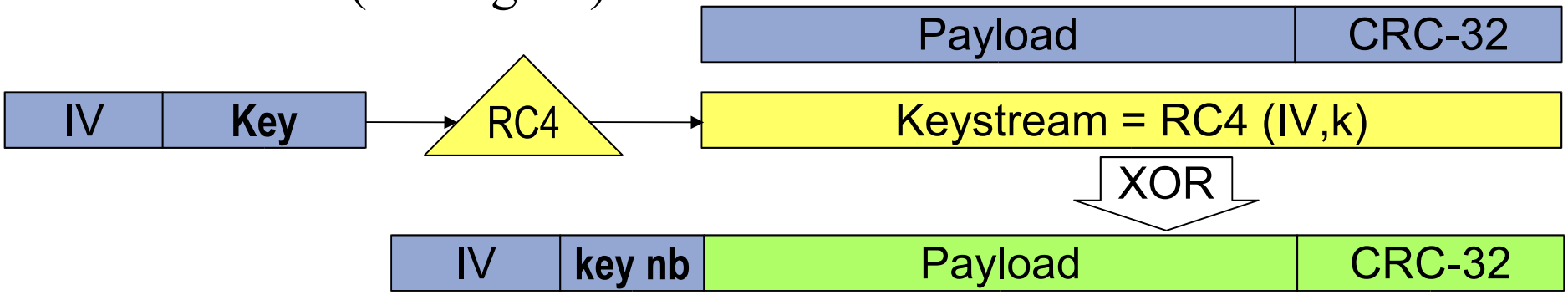
- **Frame Control** : L'ancien champ WEP a été renommé Protected Frame pour indiquer qu'un chiffrement est utilisé (sans le préciser)
- **Address 1-4** : Adresse de la source (SA) = MAC Source, Adresse destination (DA) = MAC destination, Adresse de la station émettrice (TA), Adresse de la station réceptrice (RA)
- **Sequence Control** : comprend le numéro de séquence et le numéro de fragment
- **FCS** : CRC de 32 bits sur l'en-tête MAC et le corps de la trame

WEP (Wired Equivalent Privacy)

- Basé sur l'algorithme de chiffrement RC4

	Vecteur d'initialisation	Clef partagée	Clef RC4 K=IV,k
WEP	24 bits	40 bits (x4)	64 bits (x4)
WEP2	24 bits	104 bits (x4)	128 bits (x4)

- Confidentialité (+ intégrité) des données



- Également utilisé pour l'authentification des stations (en mode clef partagée)

Vulnérabilités

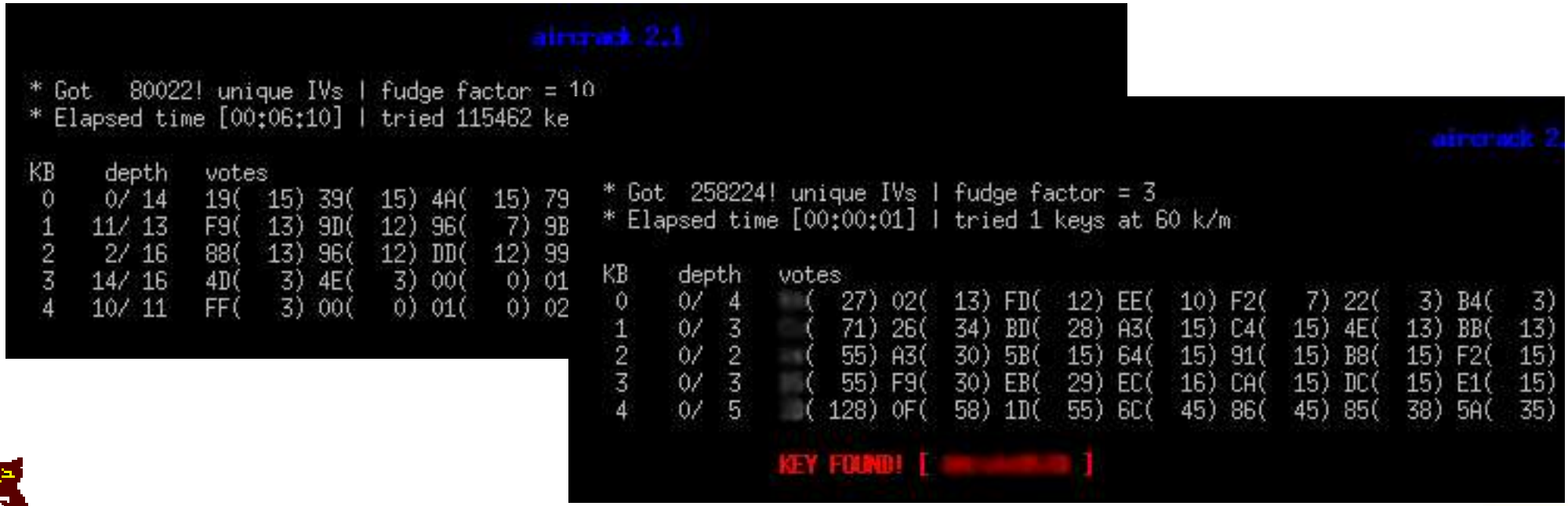
- Contre la confidentialité
  - Réutilisation de la suite chiffrante (*keystream reuse*)
  - Faiblesse de RC4 (*key scheduling algorithm weakness)*
  - Attaque exhaustive (clé dérivée d'une *passphrase*)
  - Attaque statistique
- Contre l'intégrité
  - Modification de paquets (*bit flipping*)
  - Injection de faux paquets
- Contre l'authentification auprès de l'AP
  - Fausse authentification (*authentication spoofing*)

Attaque statistique

- Attaque découverte par un hacker nommé KoreK
  - http://www.netstumbler.org/showpost.php?p=89036
- Ne nécessite plus la capture de millions d'IV mais se base juste sur le nombre d'IV uniques capturés.
- Utilisation des cas résolus exceptionnels (> 5% de réussite)
- Ecriture d'une PoC : chopper
- L'injection de trafic permet d'accélérer grandement la capture des trames
  - 1. Tronque le message chiffré d'un caractère (1 octet) => message invalide
  - 2. Suppose une valeur V pour le dernier octet (0 =< V =< 255), corrige le message et réinjecte la trame vers l'AP
  - 3. L'AP rejete toute les trames sauf celle ayant le dernier octet valide (répéter 1 - 3)
- Décryptage des paquets ARP/IP : chopchop
  - http://www.netstumbler.org/showthread.php?t=12489

Cassage du WEP – Aircrack (1)

- Aircrack – Christophe Devine – version actuelle : 2.1 (Unix & Windows)
  - Exemple
    - `aircrack -f 4 -n 128 packets.pcap`
  - Très rapide et performant (cassage de la clé < 10s avec un nombre de trames suffisant)
  - Implémente la nouvelle attaque statistique développée par KoreK
    - Nécessite un nombre d'IV unique pour pouvoir casser la clé
  - Source: http://www.cr0.net:8040/code/network/aircrack/



Cassage du WEP – Aircrack (2)

- Nécessite 150 000 IV uniques pour une clé de 64 bits et 500 000 pour une clé de 128 bits
- La version 2.2 permettra l'injection de paquet après rejeu d'une trame arp-request générant des IV uniques au niveau de la borne.
- Nécessite une mise à jour des pilotes (HostAP, Atheros, Prism54, wlan-ng)
- Méthodes :
  - `iwpriv <iface> mode 2`
  - `iwconfig <iface> mode Monitor channel <channel>`
  - `ifconfig <iface> up`
  - `airodump <iface> <name> <bssid>`
  - `aireplay -x <nb_packet> <iface>`
- Version aireplay 2.2 (beta) permettant l'injection disponible
  - http://www.cr0.net:8040/code/network/aireplay-2.2.tgz

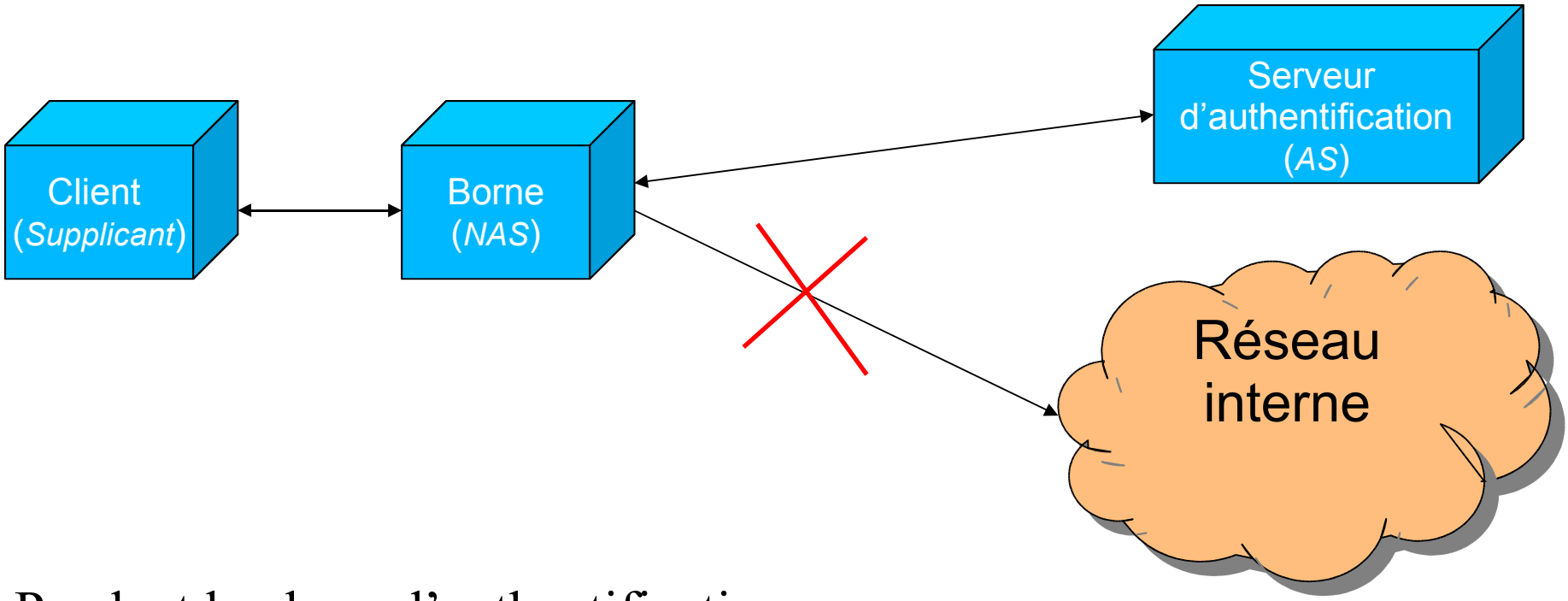
Composants de 802.1x

- Demandeur
  - En anglais : *Supplicant*
  - C'est l'entité qui souhaite accéder aux ressources, et qui va donc devoir prouver son identité
- Serveur d'accès
  - En anglais : *Network access server* (NAS) ou *Authenticator*
  - Commutateur
  - Borne sans fil
- Serveur d'authentification
  - En anglais : *Authentication server* (AS)
  - C'est celui qui vérifie les accréditations présentées par le demandeur.
  - Il dialogue avec le serveur d'accès.

Notion de port 802.1x

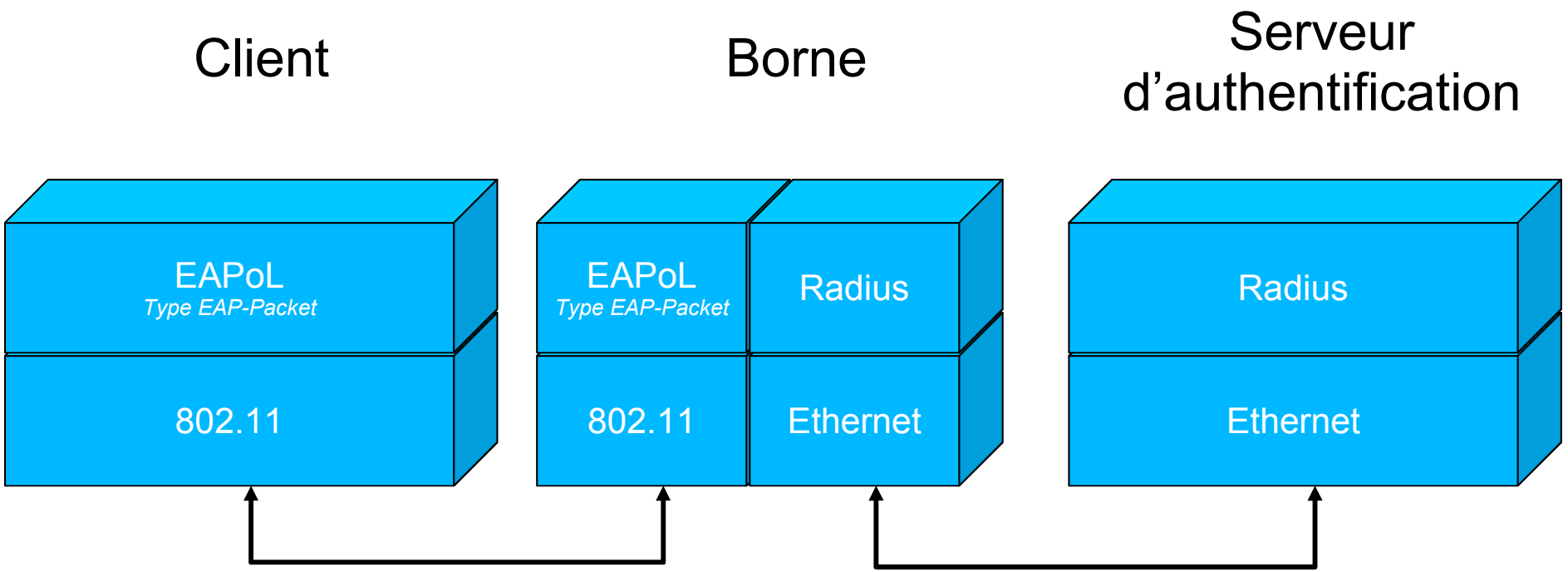
- Sur un réseau filaire commuté
  - Chaque station est reliée à un port du commutateur
  - Chaque station s'authentifie en 802.1x sur ce port
- Sur un réseau sans fil
  - Par la nature du support, toutes les stations accèdent à l'AP via le même support
  - Il faut pouvoir distinguer chaque « port logique »
  - L'AP donne à chaque client qui s'est authentifié une clé de session qui lui est propre
  - Toute trame n'utilisant pas de clé de session est ignorée par l'AP

Architecture 802.1x



- Pendant la phase d'authentification
  - La station ne peut accéder qu'au serveur d'authentification
  - Tous les autres flux sont bloqués par l'AP

EAPoL & Radius



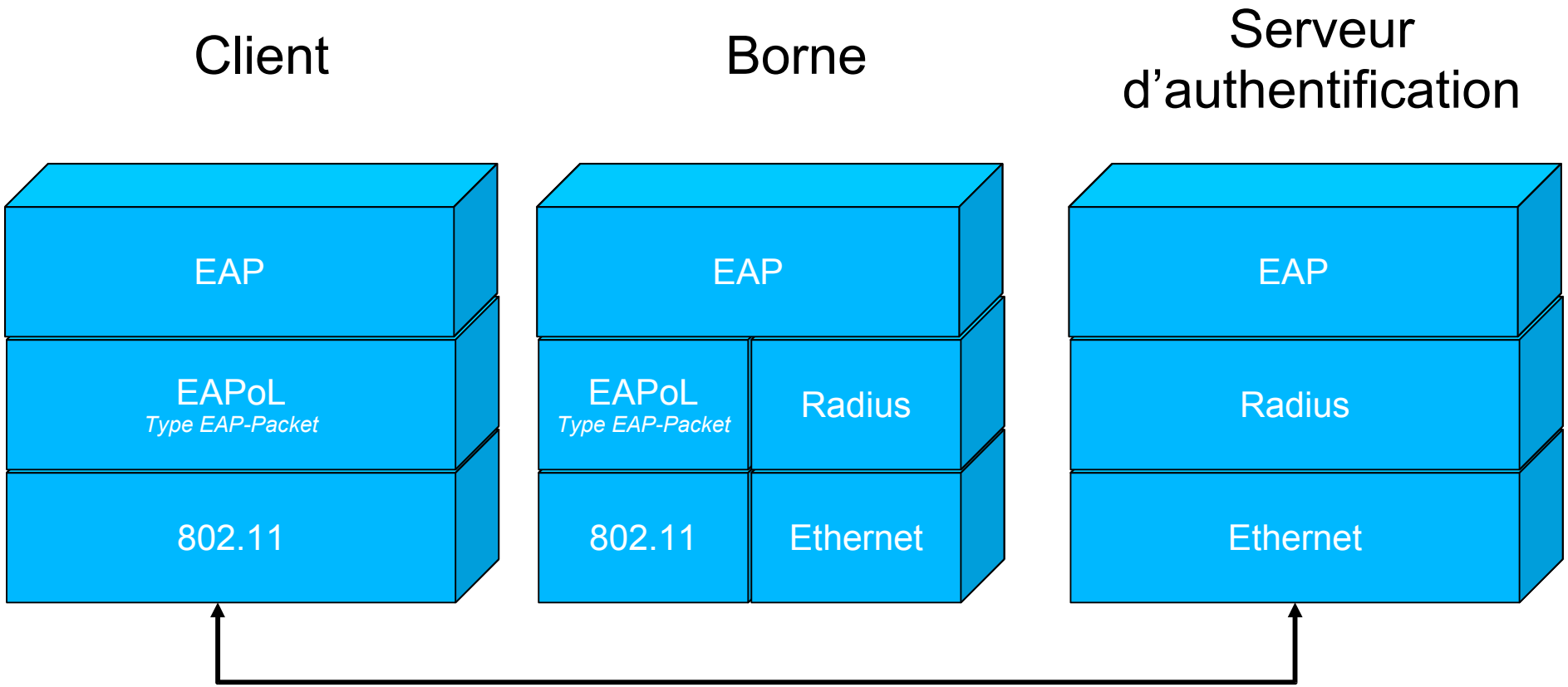
EAPoL
Transport de l'authentification de « *point à point* »
Entre le client et la borne
Sur 802.11

Radius
Transport de l'authentification de « *point à point* »
Entre la borne et le serveur d'authentification
Sur Ethernet

Généralités EAP

- *Extensive Authentication Protocol* (RFC 2284)
- Initialement conçu pour PPP
- Objectif
  - Permettre l'ajout de nouveaux protocoles d'authentification
- EAP est un protocole de transport d'authentification
  - Spécialisé dans les flux d'authentification (n'est pas un protocole d'authentification)
  - Il repose sur des méthodes pré-existantes
- Les AP ne servent qu'à relayer les messages EAP entre le client et le serveur d'authentification
- L'AP n'est pas obligée de connaître la méthode d'authentification utilisée entre le client et le serveur
  - Pratique pour l'évolutivité

EAP



EAP
Transport de l'authentification de bout en bout
Entre le client et le serveur d'authentification

Pourquoi de nouveaux mécanismes ?

- WEP : ne peut plus garantir la sécurité 802.11
- Janvier 2001 : Début des travaux du groupe de travail 802.11i (anciennement 802.11e qui a ensuite été divisé) au sein de l'IEEE pour développer des spécifications de sécurité au niveau de la couche 2 du modèle OSI pour l'authentification et le chiffrement des données.
- Avril 2003 : Recommandation WPA de la Wi-Fi Alliance (anciennement WECA) fondée sur un sous ensemble de la norme 802.11i – depuis la mi-2003 tous les produits certifiés au label WiFi doivent supporter cette recommandation.
- 23 Juin 2004 : Publication de la norme 802.11i
- Référence : http://grouper.ieee.org/groups/802/11/

Le WPA

- WPA : *Wireless Protected Access*
  - Solution du WECA pour corriger les erreurs du WEP
- Profil de 802.11i promu par le WECA
  - Permet de combler une partie des problèmes du WEP
  - Utilisation du mécanisme TKIP
    - Changement des clefs de chiffrement de façon périodique
      - 10ko de données échangées
    - Clef à 128 bits
  - Vecteur d'initialisation de 48bits (281 474 976 710 656 possibilités)
  - Impossibilité de réutiliser un même IV avec la même clef
  - Utilisation du MIC qui est un contrôle d'intégrité de tout le message
- 2 modes de fonctionnement
  - Mode PSK (*PreShared Key*) : secret partagé
  - Mode à base de 802.1X pour une authentification centralisée

Le WPA

- Le WPA n'intègre pas les sécurisation que le 802.11i apporte :
  - La sécurisation des réseaux multi-point Ad-Hoc
  - N'implémente pas AES comme algorithme de chiffrement
- Nécessite des équipements capables de l'implémenter
  - Les anciens équipements ont la plupart du temps la possibilité de mettre à jour leur software
  - Infrastructure à base de Radius (sauf en mode PSK)
    - C'est du 802.1X
- Références :
  - Document du WECA : http://www.wi-fi.org/opensection/protected_access.asp
  - Livre Blanc sur le Wi-Fi : http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf

Le WPA2

- Définition d'un RSN (*Robust Security Network*) permettant de garantir :
  - Sécurité et mobilité
    - Authentification du client indépendamment du lieu où il se trouve
  - Intégrité et Confidentialité
    - Garantie d'une confidentialité forte avec un mécanisme de distribution dynamique des clefs
  - Passage à l'échelle et flexibilité
    - Ré-authentification rapide et sécurisée en cas de « handover », séparation du point d'accès et du processus d'authentification pour le passage à l'échelle, architecture de sécurité flexible

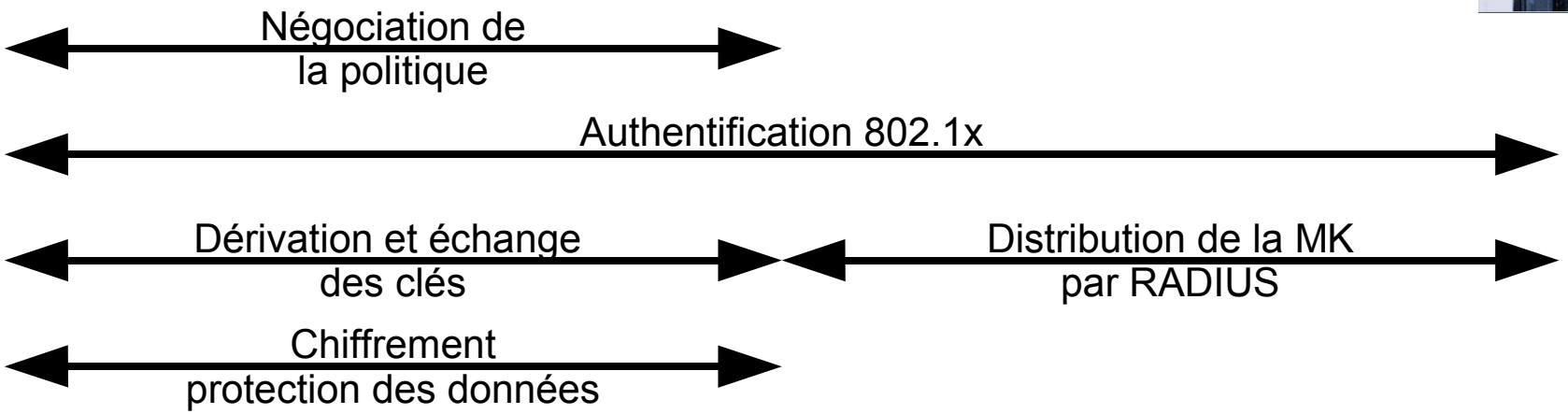
Le WPA2

- Associations construites autour d'authentifications fortes : RSNA (Robust Security Network Association) – dépendantes de 802.1x
  - PMKSA : Pairwise Master Key Authentication Security Association (contexte post 802.1x)
  - PTKSA : Pairwise Transient Key Security Association (contexte post 4 Way Handshake)
  - GTKSA : Group Transient Key Security Association (contexte post Grouk Key Handshake)
  - STAKeySA : Station Key Security Association (contexte post STAKey Handshake)

- Sécurité au niveau MAC :
  - TKIP (*Temporal Key Integrity Protocol*) - Optionnel
  - CCMP (*Counter-mode/CBC-MAC-Protocol*) - Obligatoire
  - Le TSN (*Transition Security Network*) permet une compatibilité avec les anciens mécanismes (*Open Authentication, Shared Key Authentication, WEP)*

Phase opérationnelles du 802.11i

- Phases opérationnelles
  - Négociation de la politique de sécurité
  - Authentification 802.1x
  - Échange des clefs sous EAP
  - Chiffrement des données



802.11i

- Phase 1 : Négociation de la politique de sécurité
  - L'AP diffuse dans les Beacons les RSN IE (*Information Elements*)
    - Liste des authentification supportées (802.1x)
    - Liste des protocoles de sécurité (CCMP, TKIP, ...)
    - Liste des méthodes de chiffrement pour la diffusion des clefs de groupes (GTK)
  - Le choix du client est alors précisé dans un élément d'information de sa trame Association Request

Probe Request

Probe Response + RSN IE
CCMP Mcast, CCMP Ucast, 802.1x auth

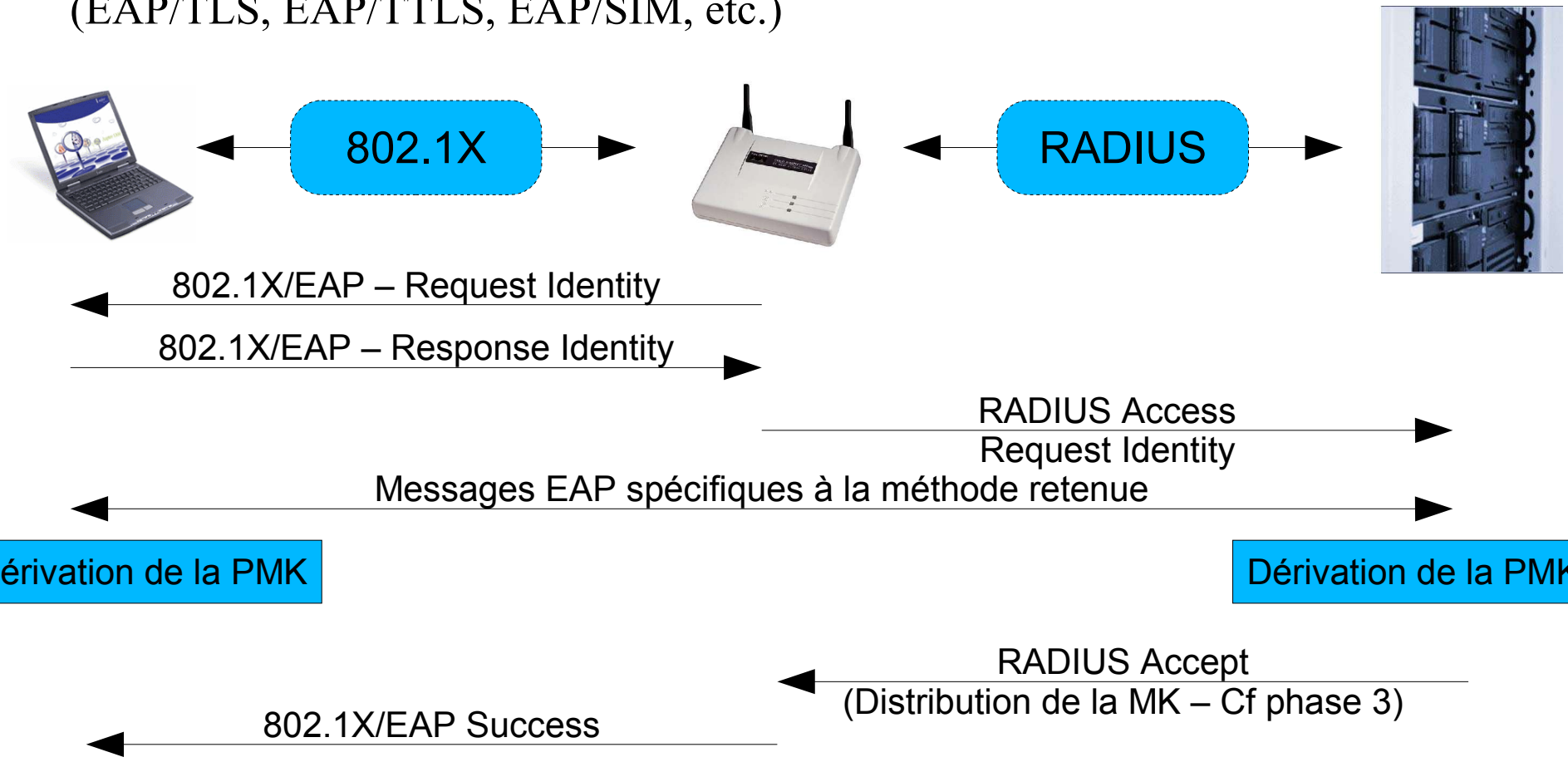
802.11 Open System Authentication

802.11 Open System Authentication - *Success*

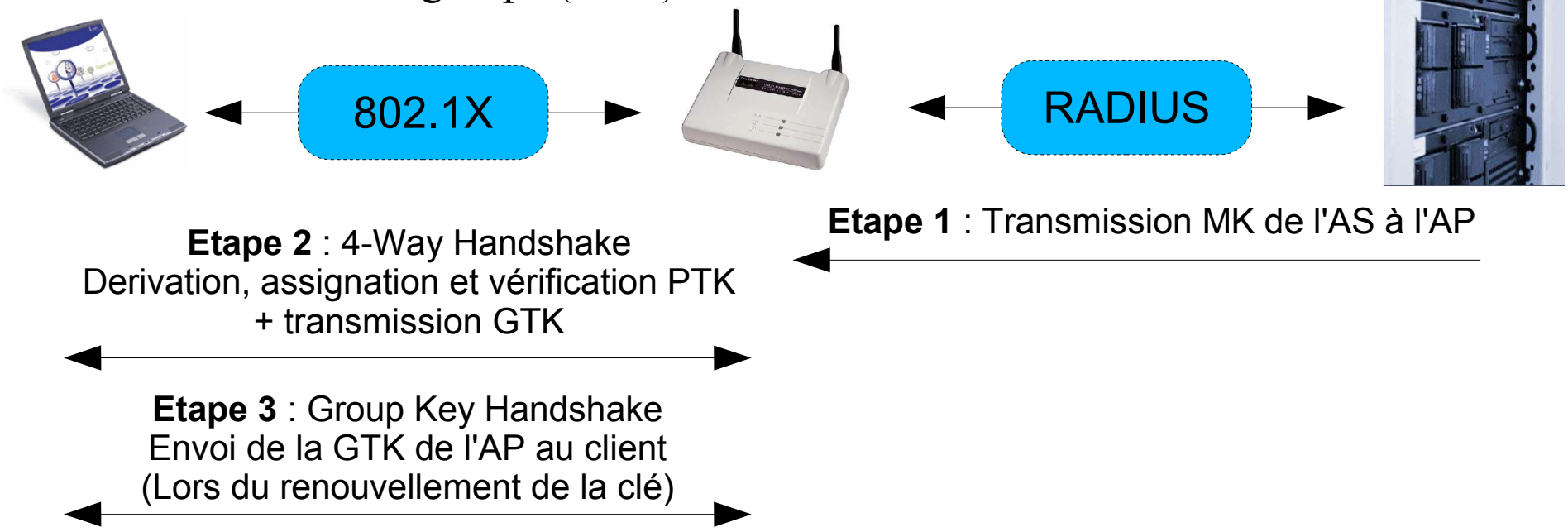
Association Request + RSN IE
STA request CCMP Mcast, CCMP Ucast, 802.1x auth

Association Response - *Success*

- Phase 2 : Authentification 802.1x
  - Définition de concert de la MK (*Master Key*) basé sur la méthode EAP choisie (EAP/TLS, EAP/TTLS, EAP/SIM, etc.)



- Phase 3 : Échange des clefs sous EAP en 3 étapes
  - Transmission de la MK du serveur d'authentification (AS) à l'AP
    - Message radius avec l'attribut MS-PPE-RECV-KEY
    - Dérivation de la PMK à partir de la MK
  - Calcul de la PTK (*Pairwise Transient Key*) grâce au *4-Way Handshake*
  - Envoi de la clef de groupe (GTK) en utilisant la KEK



Clef PTK – Pairwise Transient Key

- La PTK est dérivée de la PMK et permet l'authentification et le chiffrement des données unicast et la distribution sécurisée de la clé de groupe.

- Deux modes d'obtention d'une PMK (256 bits)
  - Si utilisation d'un serveur d'authentification : dérivation à partir de la MK (*Master Key*) obtenue par les échanges 802.1x entre ce serveur et le client

```
PMK = TLS-PRF(MasterKey, «client EAP encryption» ||
                         clientHello.random || serverHello.random)
```

  - Sinon, PMK = PSK
    - clef de 256 bits
    - clef dérivée d'une passphrase de 8 à 63 caractères (haché 4096 fois)

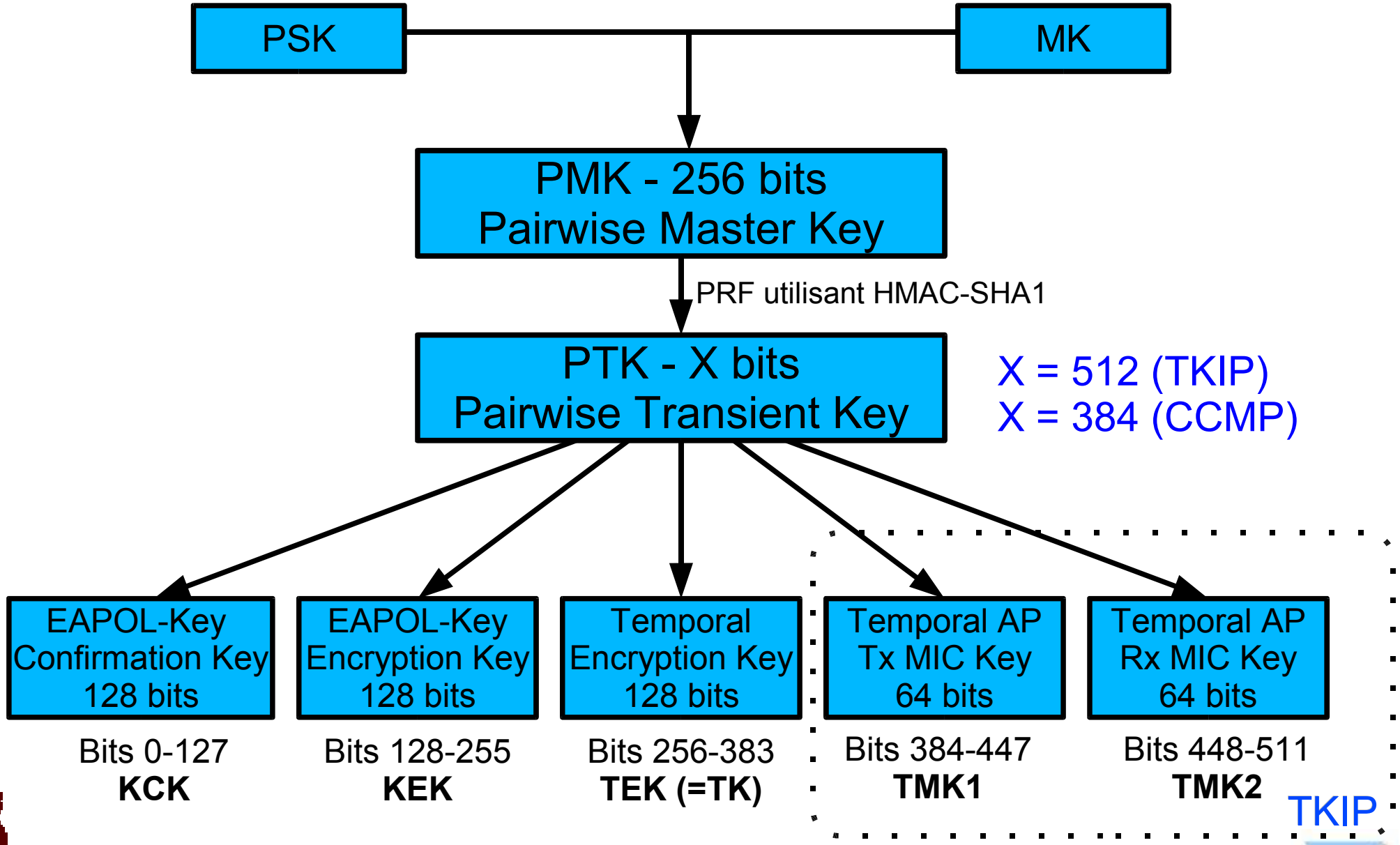
```
PMK = PSK = PBKDF2(passphrase, SSID, ssidLength, 4096, 256)
```

PBKDF2 est une fonction de dérivation de clef défini dans PKCS #5 v2

Clef PTK – Pairwise Transient Key

- La PTK (512 bits) est calculée grâce à :
  - la PMK, des aléas, les adresses MAC du point d'accès et du client ainsi que la chaine de caractère « Pairwise Key Expansion »
  - `PTK = PRF-X(PMK, « Pairwise Key Expansion »,`
    `Min(AP_Mac, STA_Mac)||Max(AP_Mac, STA_Mac)||`
    `Min(ANonce, SNonce) ||Max(ANonce, SNonce) )`
  - La fonction PRF-X est une fonction pseudo aléatoire basée sur HMAC (RFC 2104) utilisant SHA1 comme méthode de hachage dont la sortie à un nombre d'octets définis :
    - 512 bits en mode TKIP (PRF-512)
    - 384 bits en mode CCMP (PRF-384)
  - De la PTK on obtient :
    - KCK : Clef assurant l'authenticité des données dans le 4-Way Handshake et Group Key Handshake (*Key Confirmation Key* – 128 bits)
    - KEK : Clef assurant la confidentialité des données dans le 4-Way Handshake et Group Key Handshake (*Key Encryption Key* – 128 bits)
    - TK : Clef assurant le chiffrement des données (*Temporal Key* – 128 bits)
    - TMK : Deux clefs assurant l'intégrité des données (une dans chaque sens) lors de l'utilisation de TKIP (*Temporal MIC Key* – 2x64 bits)

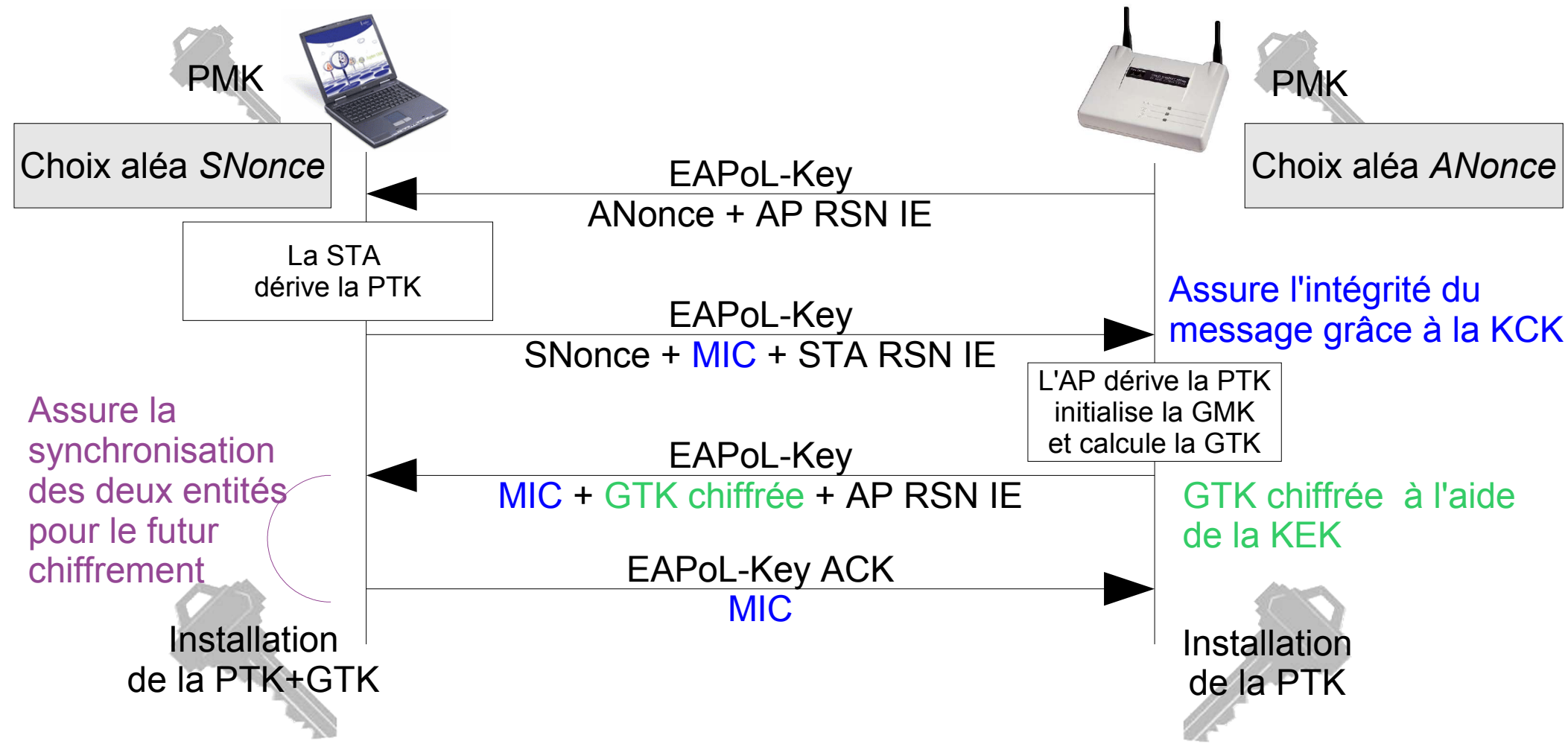
Décomposition des Pairwise Keys



4-Way Handshake : Obtention de PTK

- Le 4-Way Handshake, initialisé par l'AP, permet :
  - La confirmation de la connaissance de la PMK par le client
  - La génération d'une PTK à partir de la PMK
  - L'installation des clés d'intégrité et de chiffrement
  - Le transport sécurisé de la GTK
  - La confirmation de la suite de chiffrement utilisée

4-Way Handshake : Obtention de PTK




```
PTK = PRF-X(PMK, « Pairwise key expansion »,
  Min(AP_Mac, STA_Mac) || Max(AP_Mac, STA_Mac) || Min
  (ANonce, SNonce) || Max(ANonce, SNonce))
```

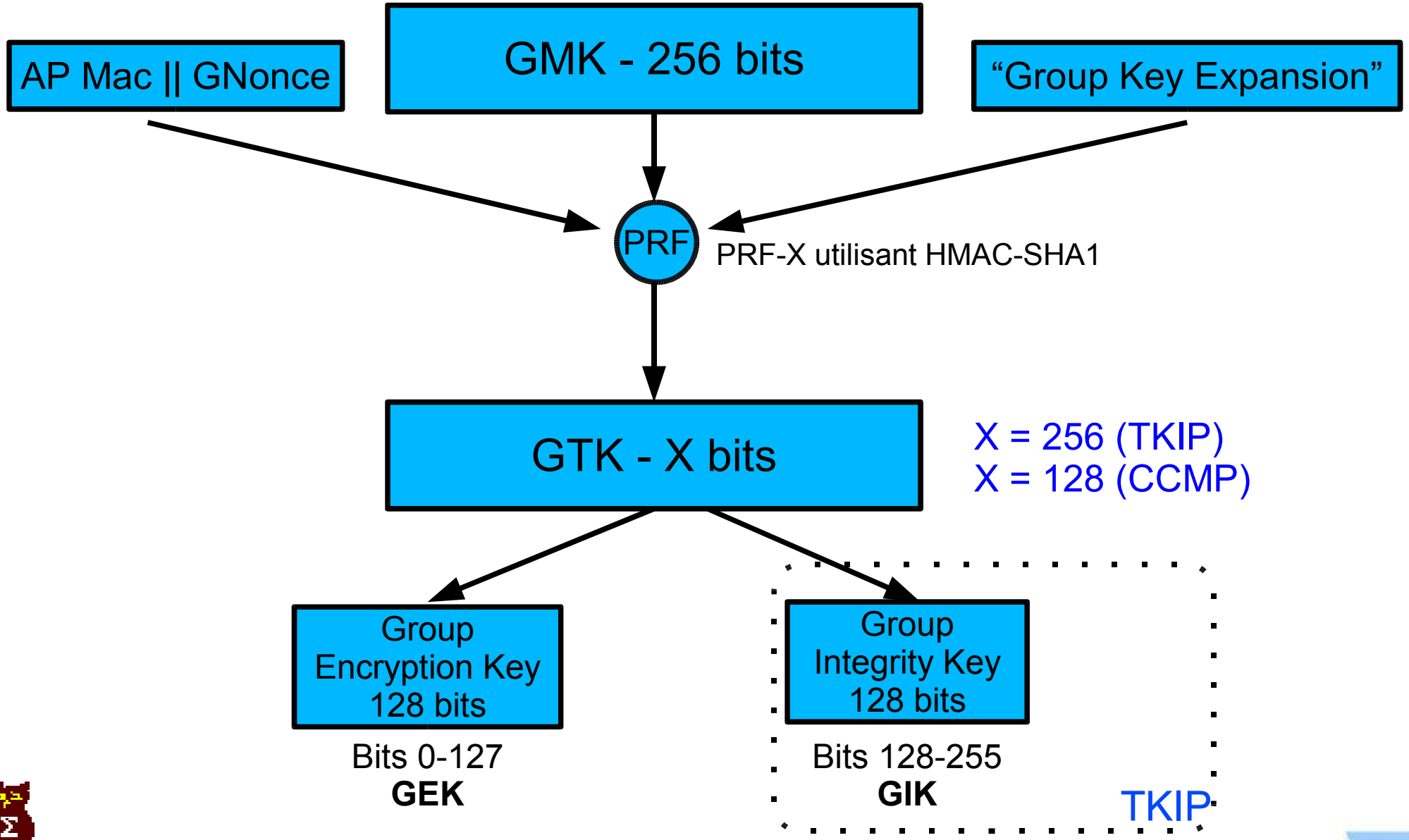
Clef GTK – Group Transient Key

- La GMK est une clef définie par la borne
- La GTK est dérivée de la GMK et sert à chiffrer et authentifier les trames à destination de plusieurs stations (broadcast ou multicast), elle doit être renouvellée quand un client quitte le réseau (plusieurs clefs possibles).

```
GTK = PRF-X(GMK, «Group Key Expansion », AP_Mac || GNonce)
```

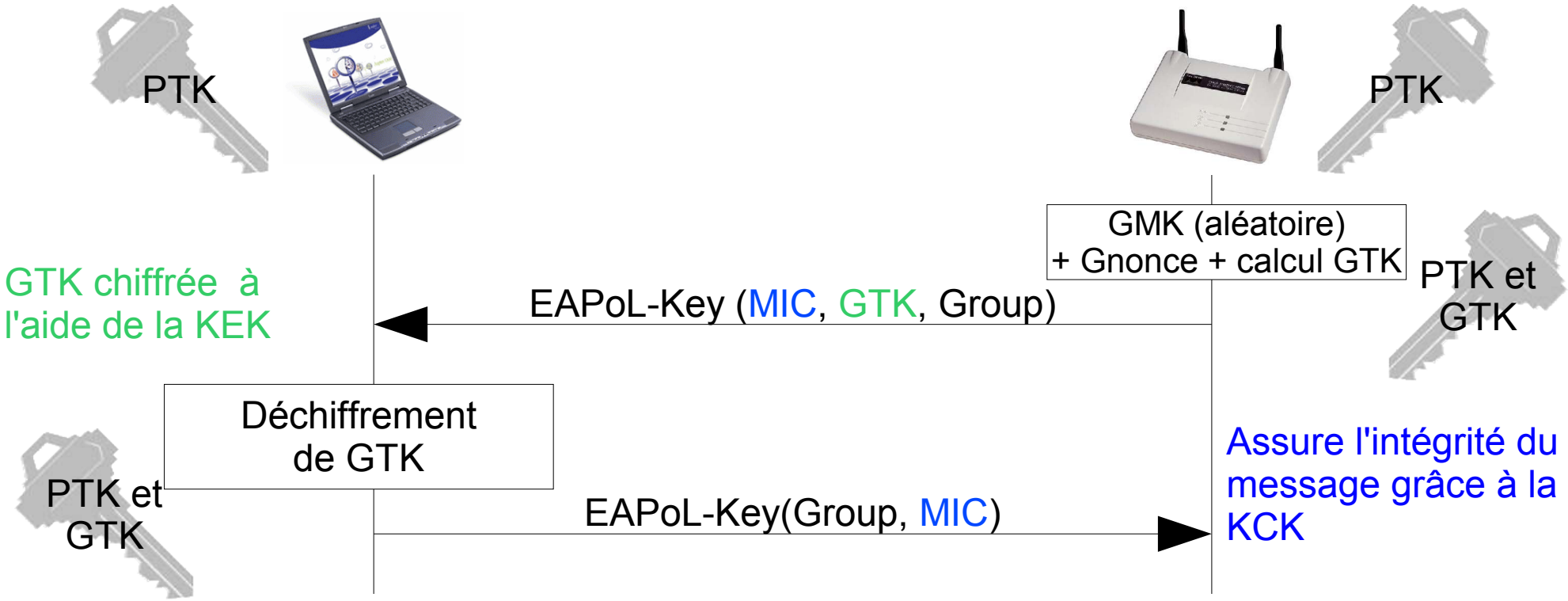
  - La fonction PRF-X est une fonction pseudo aléatoire basée sur HMAC (RFC 2104) utilisant SHA1comme méthode de hachage dont la sortie à un nombre d'octets définis :
    - 256 bits en mode TKIP (PRF-256)
    - 128 bits en mode CCMP (PRF-128)
  - De la GMK on obtient :
    - GEK : Clef assurant le chiffrement du trafic (*Group Encryption Key* – 128 bits) – dans le cas de CCMP cette clef assure aussi l'intégrité
    - GIK : Clef assurant l'intégrité du trafic lors de l'utilisation de TKIP (*Group Integrity Key* – 128 bits)

Décomposition des Group Keys



Group Key Handshake : Obtention GTK

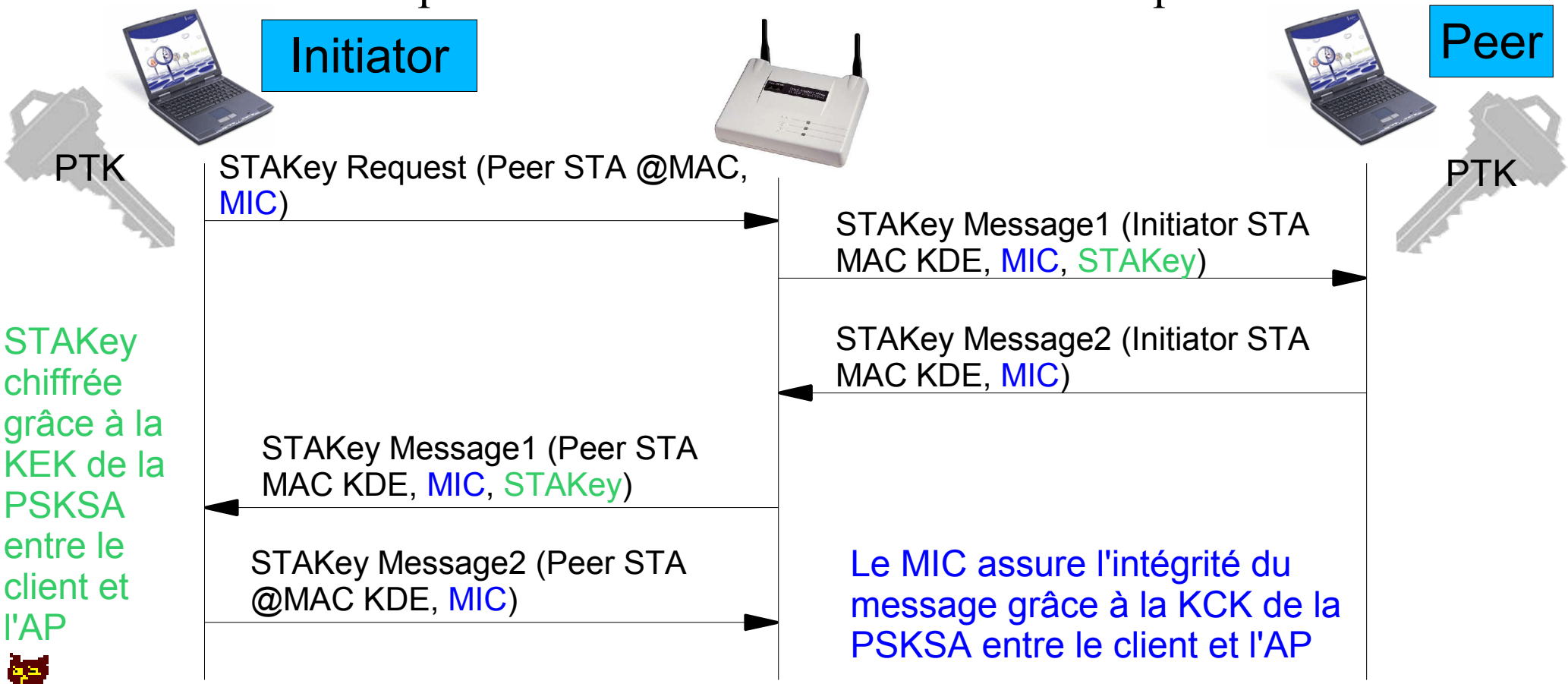
Renouvellement de la clé de groupe pour des clients ayant déjà une association de sécurité




```
GTK = PRF-256(GMK, «Group Key Expansion », AP_Mac || GNonce)
```

STAKey Handshake

- Créé une association de sécurité (STAKeySA) entre une station initiatrice (*initiator*) et une station distante (*peer*) au sein d'un même BSS
- Handshake initié par la station contrairement aux deux précédents



Solutions de chiffrement du 802.11i

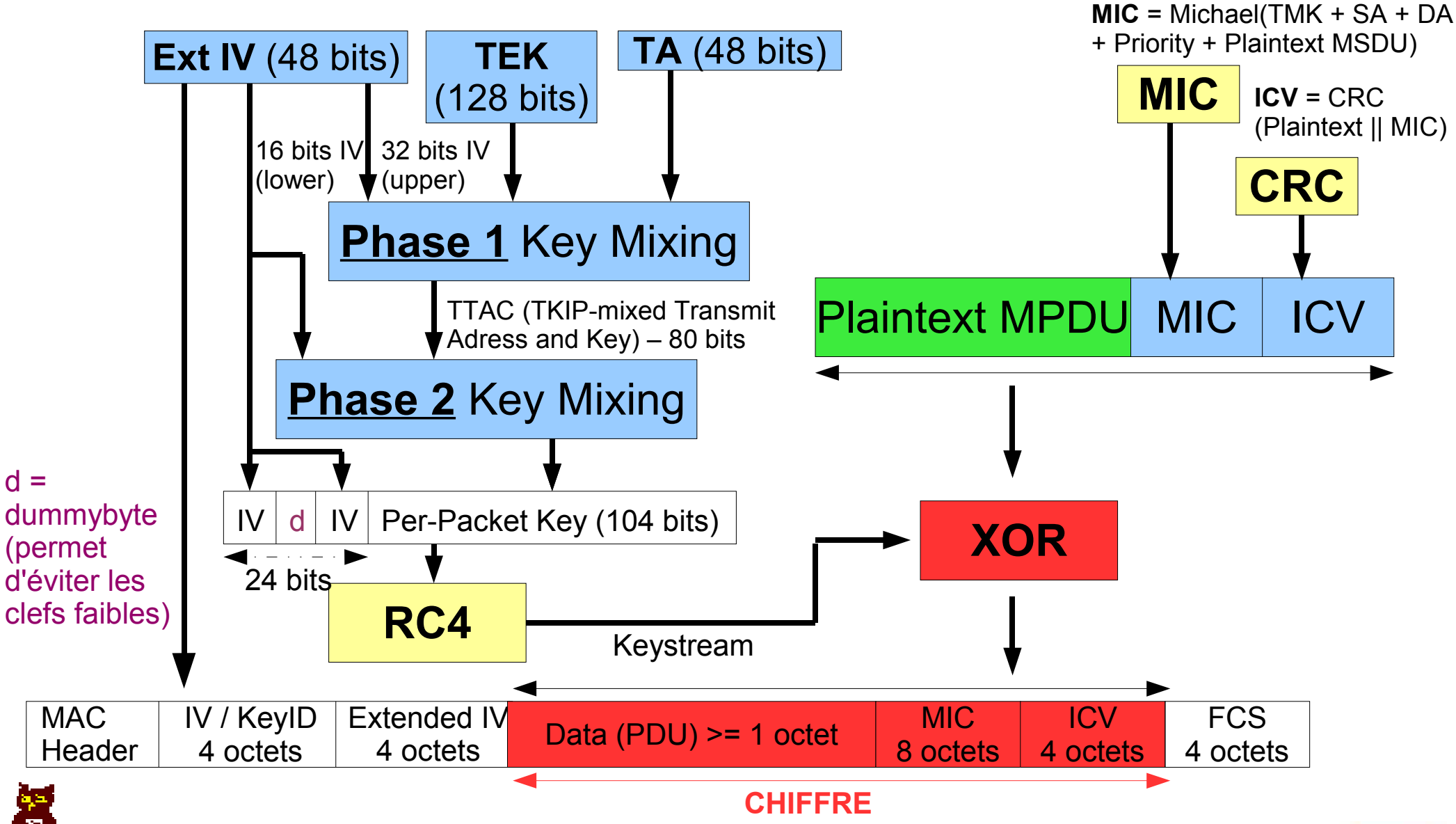
- Phase 4 : Chiffrement des données
- Le WEP inchangé ne permet pas d'assurer la sécurité des réseaux 802.11 de troisième génération, trois mécanismes ont été ajoutés à 802.11i :
  - TKIP
    - *Temporal Key Integrity Protocol*
    - Basé sur un moteur WEP (RC4) et améliorant la méthode de gestion des clefs et le contrôle d'intégrité grâce à MIC (*Message Integrity Control*).
  - CCMP
    - *Counter-Mode/Cipher Block Chaining Message Authentication Code Protocol*
    - Basé sur le chiffrement AES en mode CCM et signature MIC basée sur CBC-MAC
    - Obligatoire dans la norme 802.11i
  - WRAP
    - *Wireless Robust Authenticated Protocol*
    - Basé sur le chiffrement AES en mode OCB (*Offset Code Book*)
    - http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/ocb/ocb-spec.pdf
    - Problème de licence sur cet algorithme : 3 groupes en réclame la paternité.

TKIP – Généralités

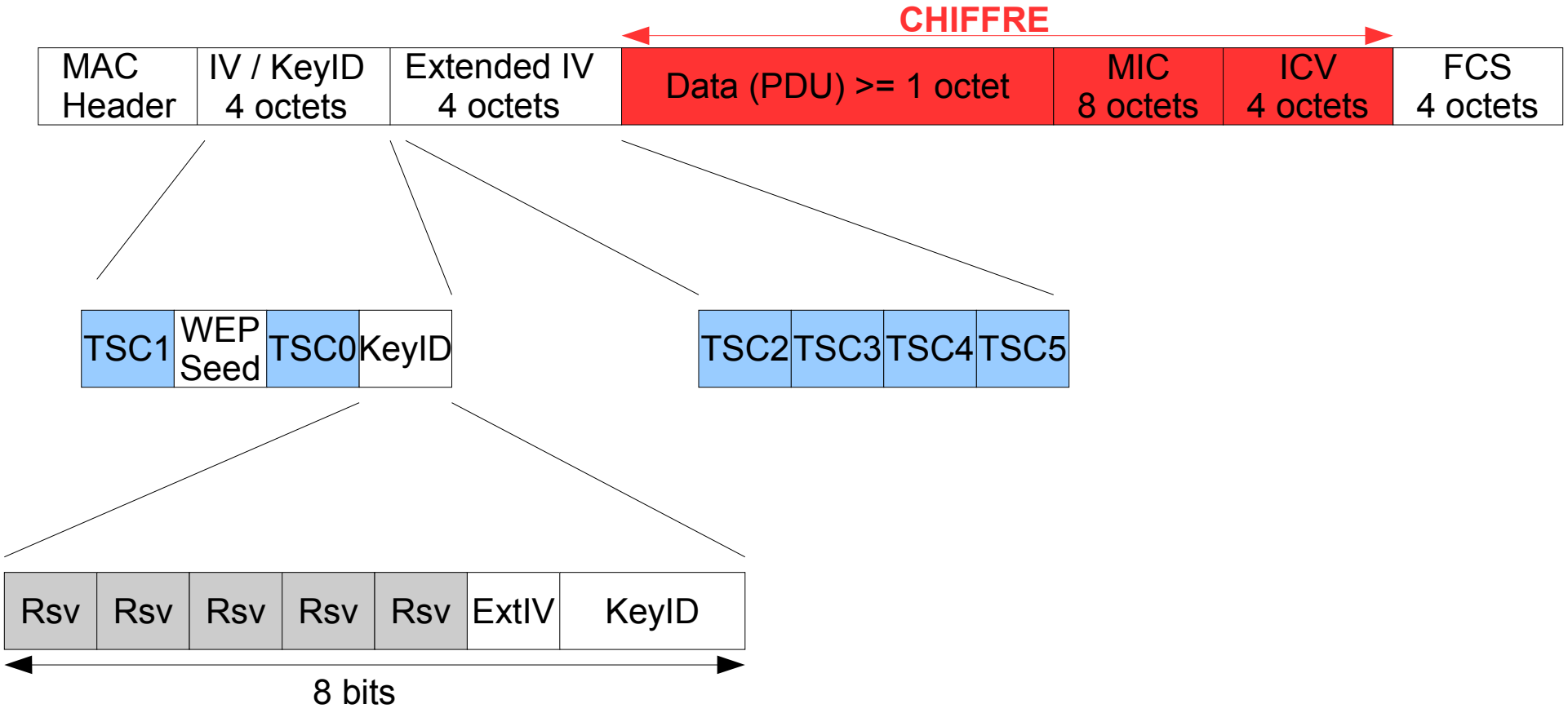
- Algorithme de chiffrement sous jacent : RC4, utilisé correctement (au sens cryptographique du terme)

- Les apports de TKIP par rapport au WEP :
  - Utilisation d'un algorithme de hachage cryptographique non linéaire : MIC (*Message Integrity Code*) basé sur Michael (Niels Ferguson)
  - Impossibilité de réutiliser un même IV avec la même clef (l'IV joue maintenant un rôle de compteur appellé TSC (*TKIP Sequence Counter*)) et augmentation de la taille de l'IV à 48 bits
  - Utilisation de clés de 128 bits (et non 40 ou 104 bits pour le WEP)
  - Intègre des mécanismes de distribution et de changement de clés
  - Utilise une clé différente pour le chiffrement de chaque paquet : PPK (*Per Packet Key*)

TKIP – Fonctionnement détaillé



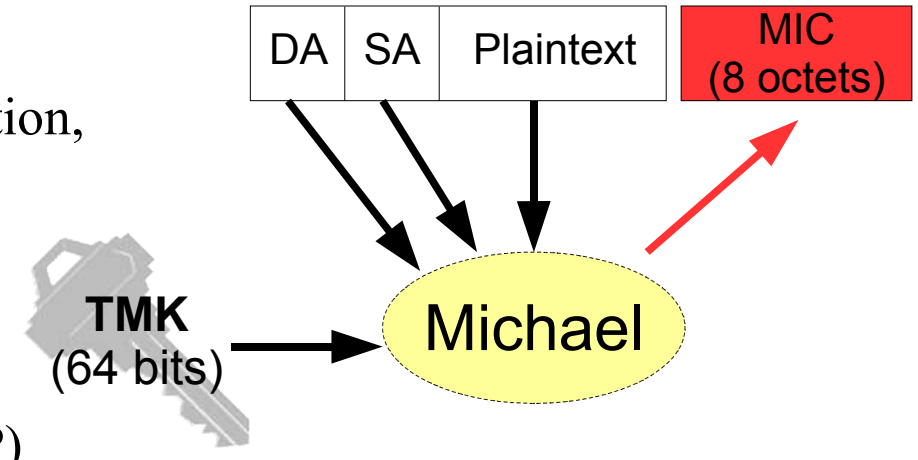
TKIP – En-tête TKIP



Rsv = Bit (ou octet) réservé = 0
ExtIV = 1 (indique la présence d'un IV étendu)
TSC (TKIP Sequence Number) = 6 octets = IV étendu

MIC dit "*Michael*"

- Vrai contrôle d'intégrité basé sur HMAC-SHA1 (clé de 64 bits) crée spécialement pour les besoins de TKIP (contraintes processeurs).
- Authentifie l'émetteur et le destinataire (SA & DA)
- Niveau de sécurité (voulu) : 20 bits (~ 1 Million de possibilités) :
  - Obligation d'implémenter des contre mesures en cas d'attaque visant à forger des MIC
  - Solution choisie : invalider la clef de l'attaquant (induisant une nouvelle négociation 802.1X) + « blackout » 60s
  - Risque de DoS (très difficile à réaliser)
  - N'utilise que des opérations de substitution, rotations, XOR (pas de multiplication)
  - MIC invalide => Renouvellement des clés (EAPoL message (clients), « Four way/Group Key handshake (AP)



Validation d'une MSDU chiffrée par TKIP

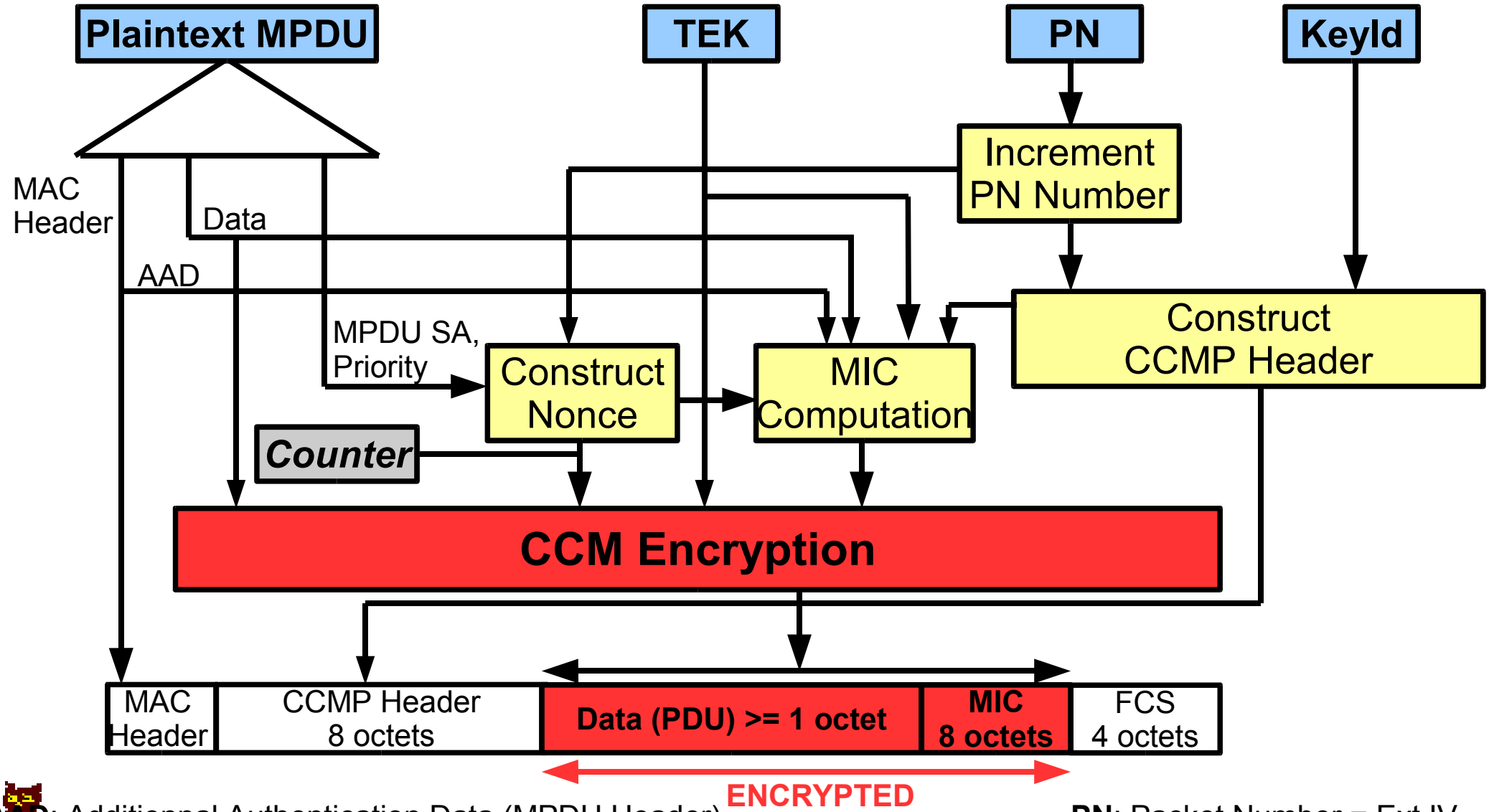
- Ne pas oublier : TKIP utilise toujours WEP (chiffrement RC4)
- Le MIC est calculé sur la MSDU

- La validation d'une MSDU suit les étapes suivantes :
  - Extraction de l'IV étendu et du KeyID, suppression des MPDU ne respectant pas le séquencement obligatoire des IV, construction du WEP seed (WEP IV)
  - Déchiffrement WEP à l'aide de l'IV et de la clé WEP (Per Packet Key)
  - Vérification de l'ICV, réassemblement des MPDU en MSDU puis vérification du MIC
  - Si le MIC est valide, la trame est passée pour traitement aux couches supérieures, sinon des contres mesures sont lancées.

CCMP - Généralités

- Protocole de sécurité basé sur le chiffrement AES (*Advanced Encryption Standard*) en mode CCM (clef et blocs de 128 bits).
- N'est pas un compromis de sécurité comme TKIP mais repose sur une remise à plat complète et un nouveau protocole créé spécialement pour l'utilisation dans 802.11i RSN : CCMP
- CCM combine CTR pour la confidentialité et CBC-MAC pour l'authenticité et l'intégrité
- Mode par défaut en 802.11i
- Ajoute 16 octets au MPDU (8 octets pour l'en-tête CCMP et 8 octets pour le MIC)
- Protection anti-rejeu grâce au PN (le PN est unique pour chaque PTKSA, GTKSA ou STAKeySA)

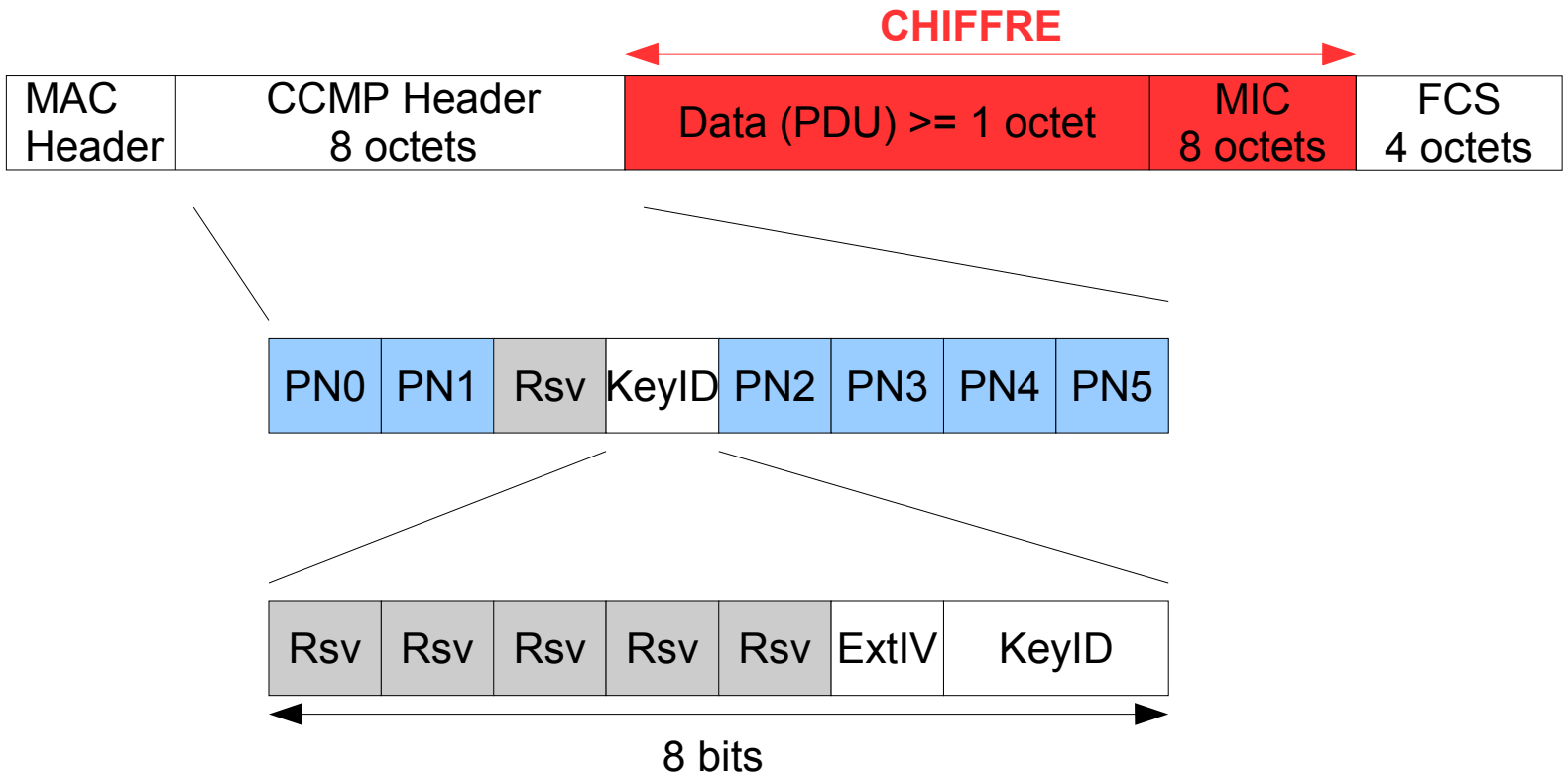
CCMP – Fonctionnement détaillé



AAD: Additionnal Authentication Data (MPDU Header)

PN: Packet Number = Ext IV

CCMP – En-tête CCMP



Rsv = Bit (ou octet) réservé = 0
ExtIV = 1
PN (Packet Number) = 6 octets = IV étendu

Validation d'une MSDU chiffrée par CCMP

- L'ICV n'est plus utilisé (héritage du WEP dans TKIP ...)
- Le MIC est calculé sur chaque MPDU (contrairement à TKIP !)

- La validation d'une MSDU suit les étapes suivantes :
  - Extraction du PN (IV étendu), suppression des MPDU ne respectant pas le séquencement obligatoire des PN
  - L'AAD et le Nonce sont reconstruits à partir du MPDU chiffré. La valeur de l'AAD est vérifiée, en cas de différence le MPDU est rejeté.
  - Le MPDU est déchiffré et le MIC est extrait.
  - Si le MIC est valide, le MPDU en clair est construit à partir de l'en-tête MPDU et du MPDU déchiffré et passé aux couches supérieures, sinon des contres mesures sont lancées.

Récapitulatif des solutions de chiffrement

	WEP	*TKIP*	*CCMP*
Chiffrement	RC4	RC4	AES
Taille de la clé	40 ou 104 bits	128 bits (chiffrement) 64 bits (authentification)	128 bits
Taille IV	24 bits	48 bits	48 bits
Clé par paquet	Non (seul l'IV fait varier la suite chiffrante)	Oui	Pas nécessaire
Intégrité de l'en-tête du paquet	Non	SA et DA protégés par Michael	CCM
Intégrité des données du paquet	CRC32	Michael	CCM
Détection des rejeux	Non	Sequencement des IV obligatoire et rejeu impossible	Sequencement des IV obligatoire et rejeu impossible
Gestion des clés	Aucune	IEEE 802.1X	IEEE 802.1X

Déjà des faiblesses ?

- Attaque sur la PSK (WPA & WPA2)
  - Sécurité basée sur la qualité de la *passphrase* => Attaque par dictionnaires ou Brute force
  - Solutions : Choisir une passphrase de plus de 20 caractères OU entrer la PSK en hexadécimal avec des données aléatoires
  - http://wifinetnews.com/archives/002453.html : Découverte du problème (Nov 2003)
  - http://new.remote-exploit.org/images/5/5a/Cowpatty-2.0.tar.gz : ~ 60 mdp/s
- Attaque sur le protocole 4-Way Handshake (WPA & WPA2)
  - Attaque publiée par ChangHua He et John C. Mitchell intitulée « *1 Message Attack on the 4-Way Handshake* »
    - Faille : Pas d'authentification sur le 1er message
    - Le client se doit de conserver des données entre le 1er et le 3ème message (la signature du 3ième message lui permettant de déduire la bonne PTK)
    - Exploitation : Inondation d'un client par des trames N°1 spoofées
    - Entraine un problème d'espace mémoire ...

Déjà des faiblesses ?

- Attaque sur la TEK (WPA)
  - Une attaque sur la TEK publiée par Vebjorn Moen, Havard Raddum et Kjell J. Hole intitulée « *Weaknesses in the Temporal Key Hash of WPA* » est possible.
    - La complexité de l'attaque est de 2^{105} au lieu de 2^{128} avec une recherche exhaustive. L'attaque permet aussi de déduire les 64 bits de la clé d'authentification avec une complexité de 2^{38}
    - Nécessite la connaissance d'au moins deux clefs RC4 générées à partir de 32 bits de poids fort d'IV identiques
    - Implémentation de l'attaque avec quatre clefs, moins de 7 minutes de calcul (sur PIV 2.5Ghz) pour récupérer la clé de chiffrement TEK !
- Les attaques de bas niveau sont toujours possibles :
  - Couche 802.11
  - Inondation de paquets Dé-authentification et Dé-association
  - Vol de Bande passante
  - Brouillage radio

Itinérance

- Deux mécanismes ont été introduits pour améliorer l'itinérance :
  - **Pre Authentication**
    - Permet à un client de s'identifier avec un autre AP sur lequel il risque de basculer (au sein du même BSS)
    - Comment ? : redirection des trames d'authentification générés par le client vers son futur AP par l'intermédiaire du réseau filaire
    - Avantage : Roaming plus rapide
    - Inconvénient : Accroissement significatif de la charge sur le serveur d'authentification
  - **Key Caching** :
    - Permet de conserver la PMK afin de la réutiliser lors d'une future transaction avec cet AP
    - Utilisation du PMKID (*Pairwise Master Key Identifier*) pour identifier la bonne clef
    - Extension de certains constructeur « Proactive Key Caching » : partage des PMK entre AP

Conclusion

- Le WEP est définitivement à éviter, la durée de vie d'une clé de 128 bits est **inférieur à 1h** avec les nouveaux outils
- Les bornes ne supportant pas WPA doivent implémenter une rotation des clés au maximum toutes les heures
  - protège de l'utilisation frauduleuse des ressources informatiques
  - ne protège pas de la perte de confidentialité des données
- WPA s'impose comme solution pour les bornes ne pouvant pas supporter le WPA2 (mise à jour logiciel possible).
- WPA2 est la solution la plus pérenne
- Le mode PSK ne garantit pas la confidentialité entre utilisateurs d'un même BSS (Utiliser le mode Entreprise – Serveur d'authentification)
- Le chiffrement ne doit pas empêcher l'isolement des réseaux et la mise en place de filtrage

Références

- IEEE 802.11i standard
- IEEE 802.11i Overwiew, Nancy Cam-Winget, Tim Moore, Dorothy Stanley, Jesse Walker – Décembre 2002
- Real 802.11 Security – Wi-Fi Protected Access and 802.11i – John Edney & William A. Arbaugh – Addison-Wesley – ISBN 0-321-13620-9
- Sécurité Wi-Fi – Guy Pujolles – Eyrolles – ISBN 2-212-11528-8
- Analysis of the 802.11i 4-Way Handshake – Changhua He, John C Mitchell – Université de Standford
- 1 Message Attack on the 4-Way Handshake – Changhua He, John C Mitchell – Université de Standford
- Weaknesses in the Temporal Key Hash of WPA – Vebjorn Moen, Havard Raddum, Kjell J. Hole – Université de Bergen – Avril 2004

Merci de votre attention

Questions ?

Retrouvez ces transparents sur www.hsc.fr

Prochains rendez-vous

- **Convention sécurité :** 15 et 16 juin
  - Deux jours de tutoriels et de **conférences gratuites**
  - Programme : **http://www.hsc.fr/conferences/csm05_programme.html**
- **Formation DNS** : 21 juin, **Postfix et anti-spam** : 22 juin
  - **`http://www.hsc.fr/services/formations/`**
- **Formations SecurityCertified** : 5-9 & 19-23 septembre
  - Permettant de passer la **certification SCNP**
  - **`http://www.hsc.fr/services/formations/`**
- **Formation BS7799 Lead Auditor** : octobre 2005
  - Certifiée par **LSTI** et reconnue par l'**IRCA**
  - **`http://www.hsc.fr/services/formations/`**
- Sur **`http://www.hsc-news.com/`** vous pourrez vous abonner à la **newsletter HSC**