JRES 2003

La carte à puce EAP* un passeport pour la sécurité des réseaux émergents Wi-Fi

Pascal.Urien@enst.fr

Marc.Loutrel@lip6.fr

Lille, le 20 Novembre 2003.

***Prix de la "Meilleure Innovation Technologique" au concours Sésames du salon cartes'2003.**

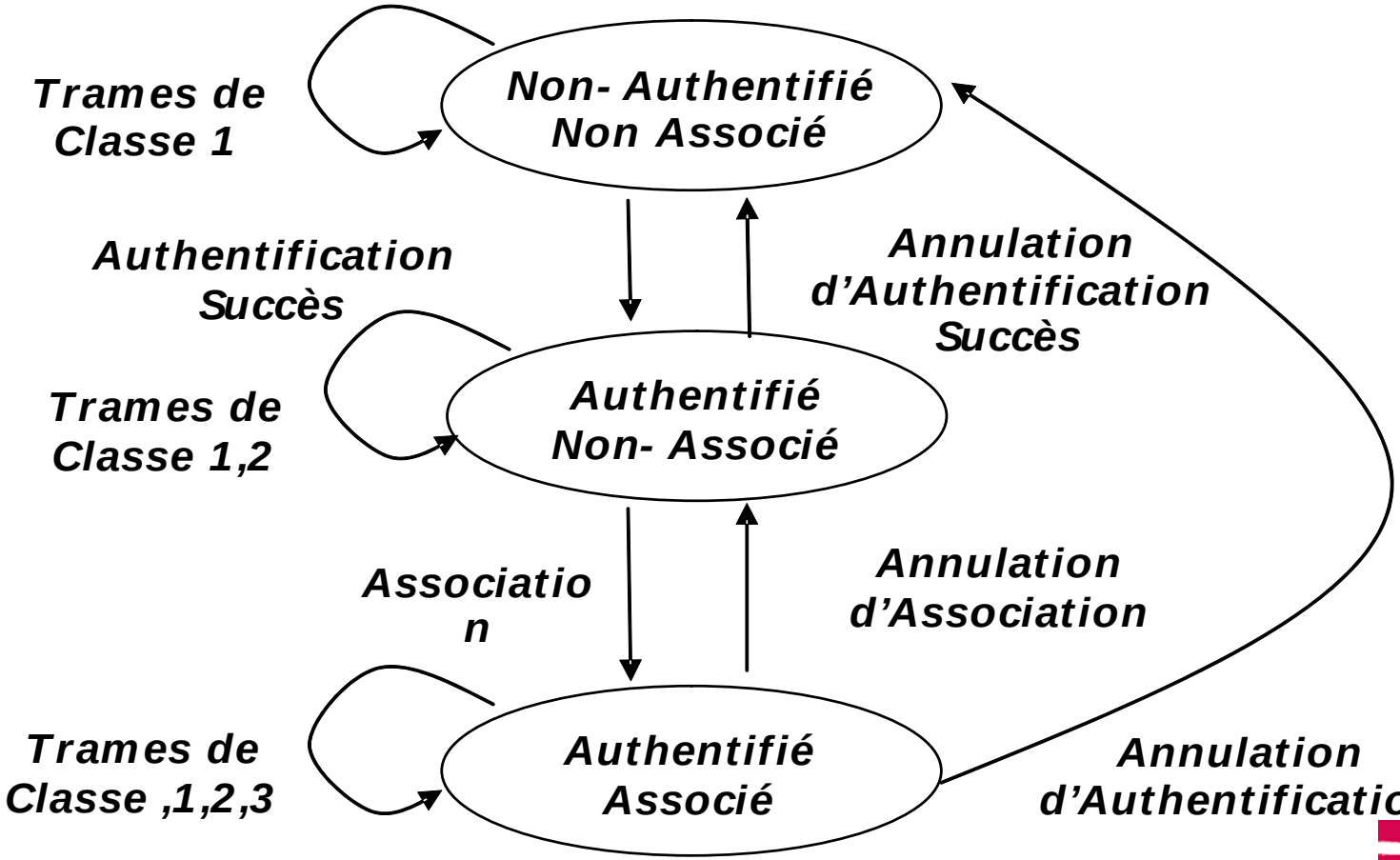
TELECOM PARIS
école nationale supérieure des télécommunications

Introduction

- **L'engouement des marchés informatiques pour les réseaux sans fil 802.11 (ou encore *Wi-Fi*) est freiné par l'absence d'infrastructures de sécurité standardisées et inter opérables.**
- **Les réseaux sans fil paraissent donc *aussi séduisants que dangereux*, et requièrent une analyse attentive des besoins de sécurité préalablement à leur déploiement.**
- **A l'origine, les réseaux 802.11 ne sont que le prolongement naturel de réseaux câblés (Ethernet), l'utilisation de liens radio augmente le temps de connexion des internautes et accroît leur profitabilité économique* .**
- **Cette technologie permet de mettre en place des infrastructures bon marché, mais cependant capables de supporter plusieurs milliers d'utilisateurs.**
- **Cet article fait le point sur les standards en cours de définition, et présente une nouvelle génération de cartes à puce (*les cartes EAP*) renforçant les éléments de sécurité indispensables au déploiement des réseaux sans fil 802.11.**

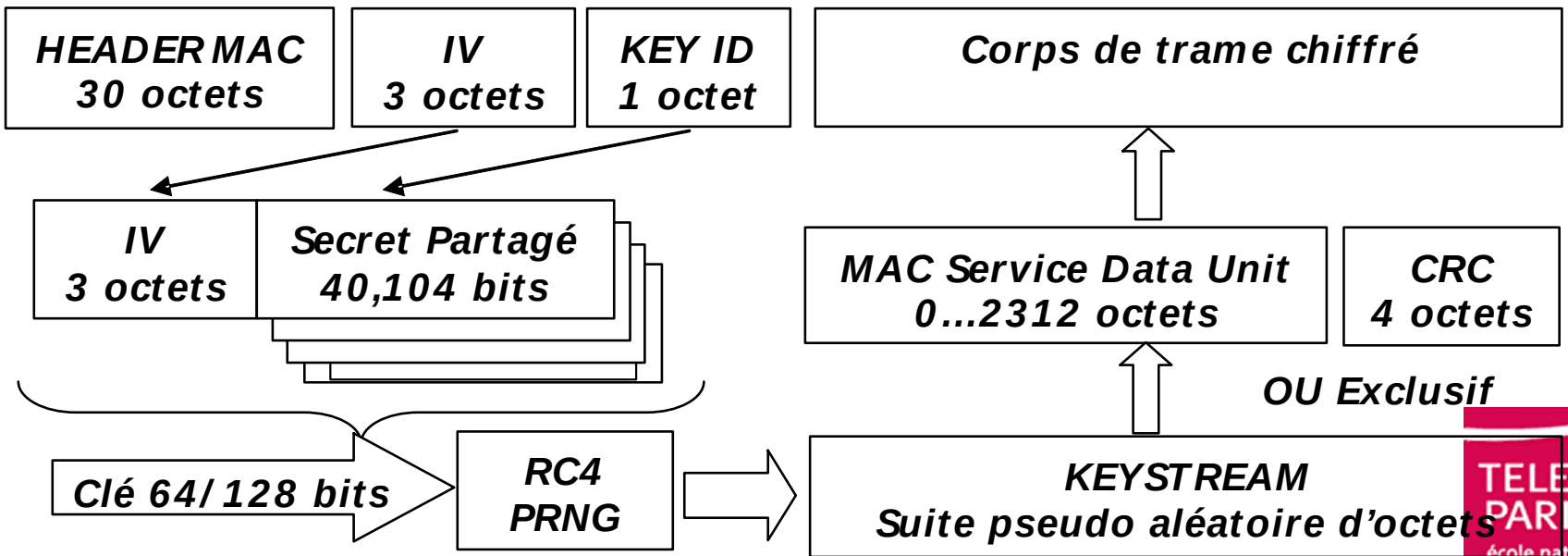
*** Selon www.nopworld.com, un accroissement du temps de connexion de 45 minutes par jour augmente la productivité d'un employé de 20 %.**

802.11: Authentification



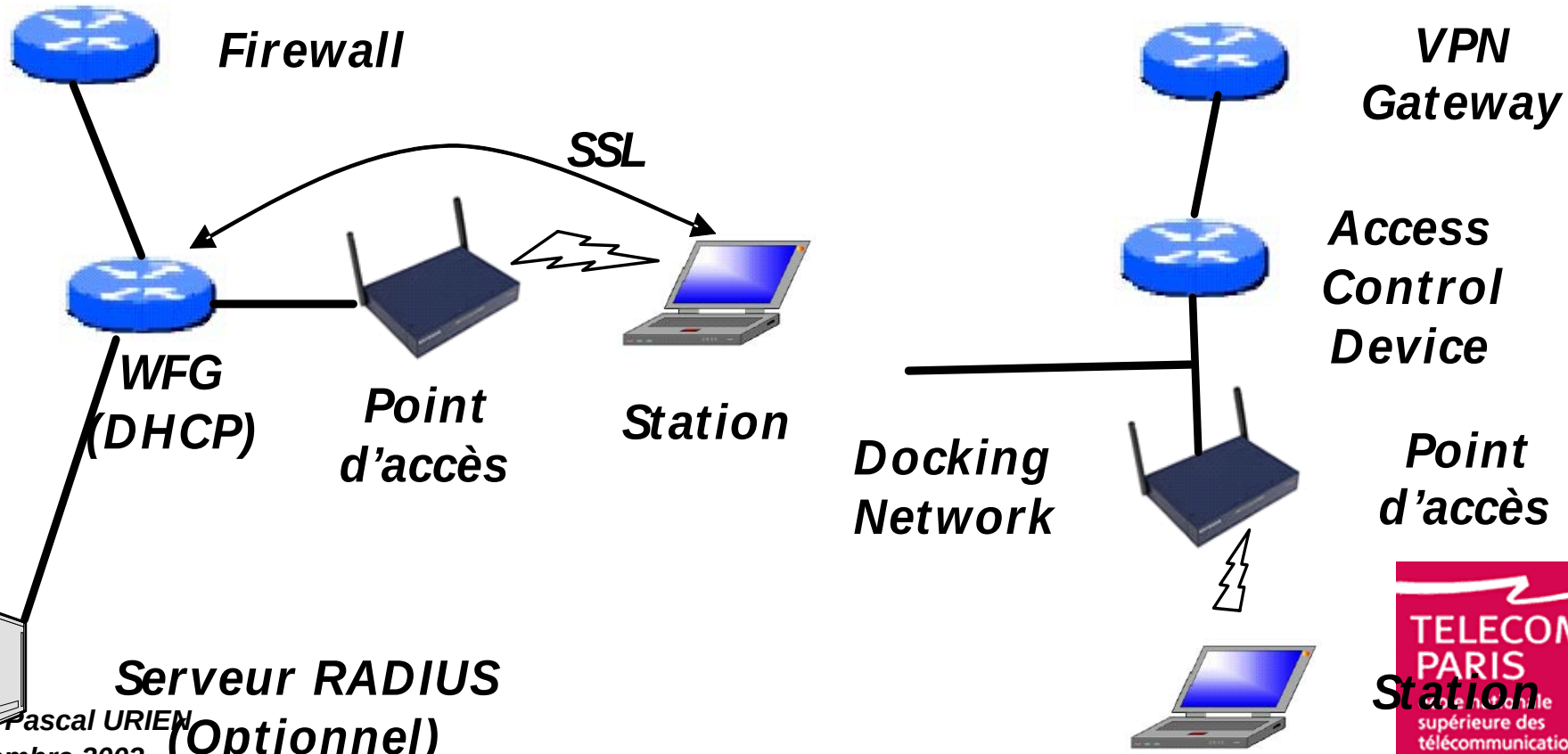
802.11: WEP

- **Un jeu de 4 secrets statiques.**
- **16 millions (2^{24}) de valeurs IV différentes.**
- **Attaque par *Bit Flipping*.**
- **Attaque de *Fluhrer & All***
  - Valeur résolvantes (3+Bi,255,N), environ 4 millions de trames sont nécessaires pour casser un secret partagé de 104 bits.

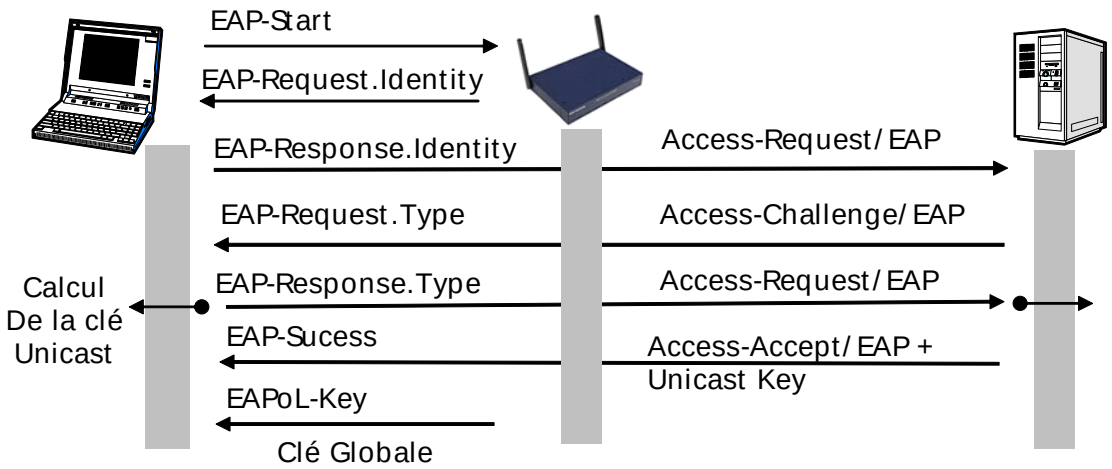


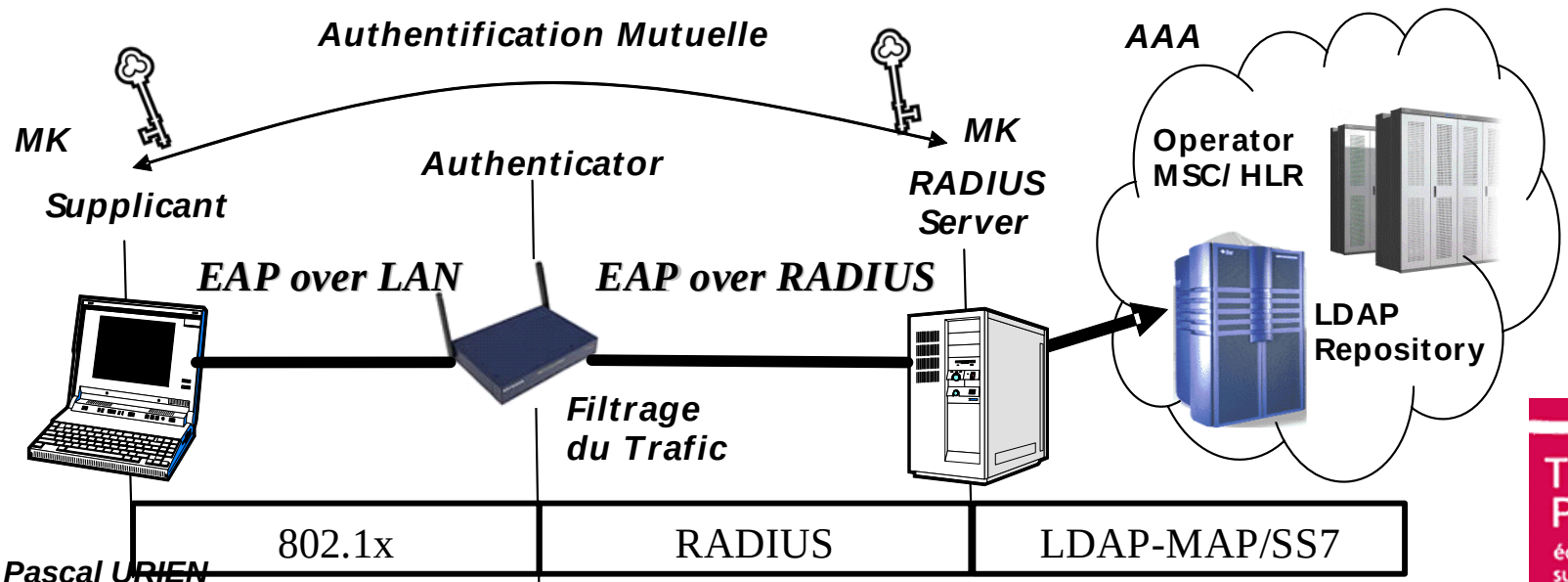
Architectures Alternatives

- Tunnel IPSEC
- WFG – *Wireless Firewall Gateway*
- Switch Mobile, *Access Control List*



- **Authentification Mutuelle entre Supplicant et Authentication Server**
- **Distribution des clés (EAPoL-Key)**

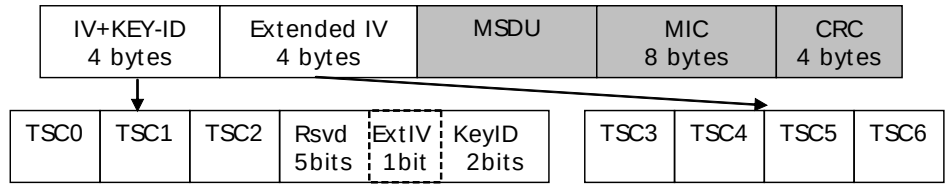




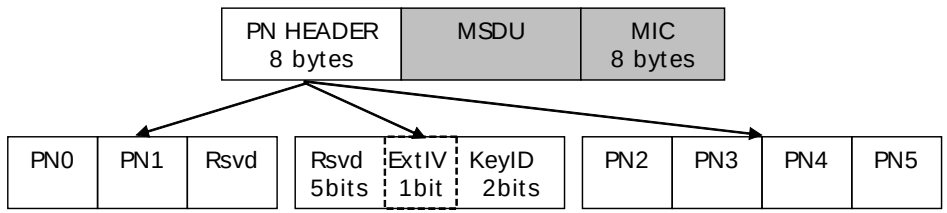
RADIUS

- **Le NAS génère des requêtes *Access-Request*, associées à un nombre aléatoire de 16 octets (le champ *Authenticator*). La réponse du serveur d'authentification est l'un des trois messages suivants**
  - *Access-Challenge*
  - *Access-Reject*
  - *Access-Success.*
- **Elle est signée par un nombre *Response Authenticator* (16 octets), une empreinte MD5 calculée à partir des données de la réponse, du champ *Authenticator* importé de la requête, et d'un *secret partagé* .**
- **De surcroît un paquet RADIUS comporte un attribut de signature (le *Message-Authenticator #80*), qui conformément à la RFC 2104, est déduit du secret partagé et du contenu du message.**

- **Multiples protocoles de sécurité radio**
  - TKIP (=WEP2, RC4)
  - CCMP (AES)



Trame TKIP

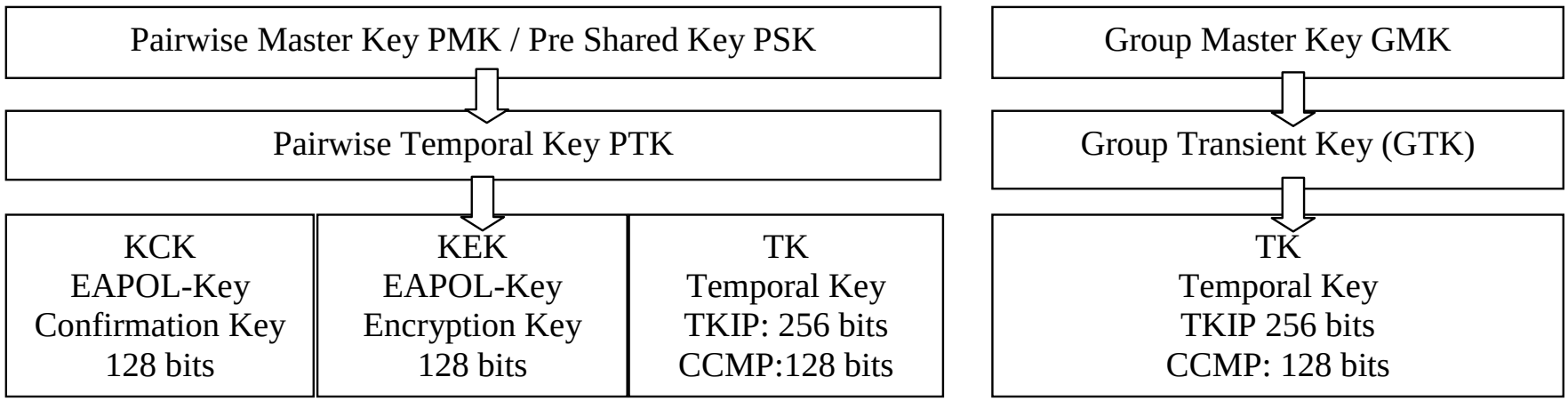


Trame CCMP

- **Eléments d'information IE**
  - Un point d'accès diffuse dans ses trames *Beacon* ou *Probe* des éléments d'information afin de notifier aux nœuds sans fil les informations suivantes,
    - La liste des infrastructures d'authentification supportées (typiquement 802.1X)
    - La liste des protocoles de sécurité disponibles (TKIP, WRAP, CCMP,…)
    - La méthode de chiffrement pour la distribution d'une clé de groupe (GTK).
  - Une station 802.11 notifie son choix par un élément d'information transmis lors de sa demande d'association.
- **Distribution de clés avec mutuelle authentification entre AP et Supplicant.**

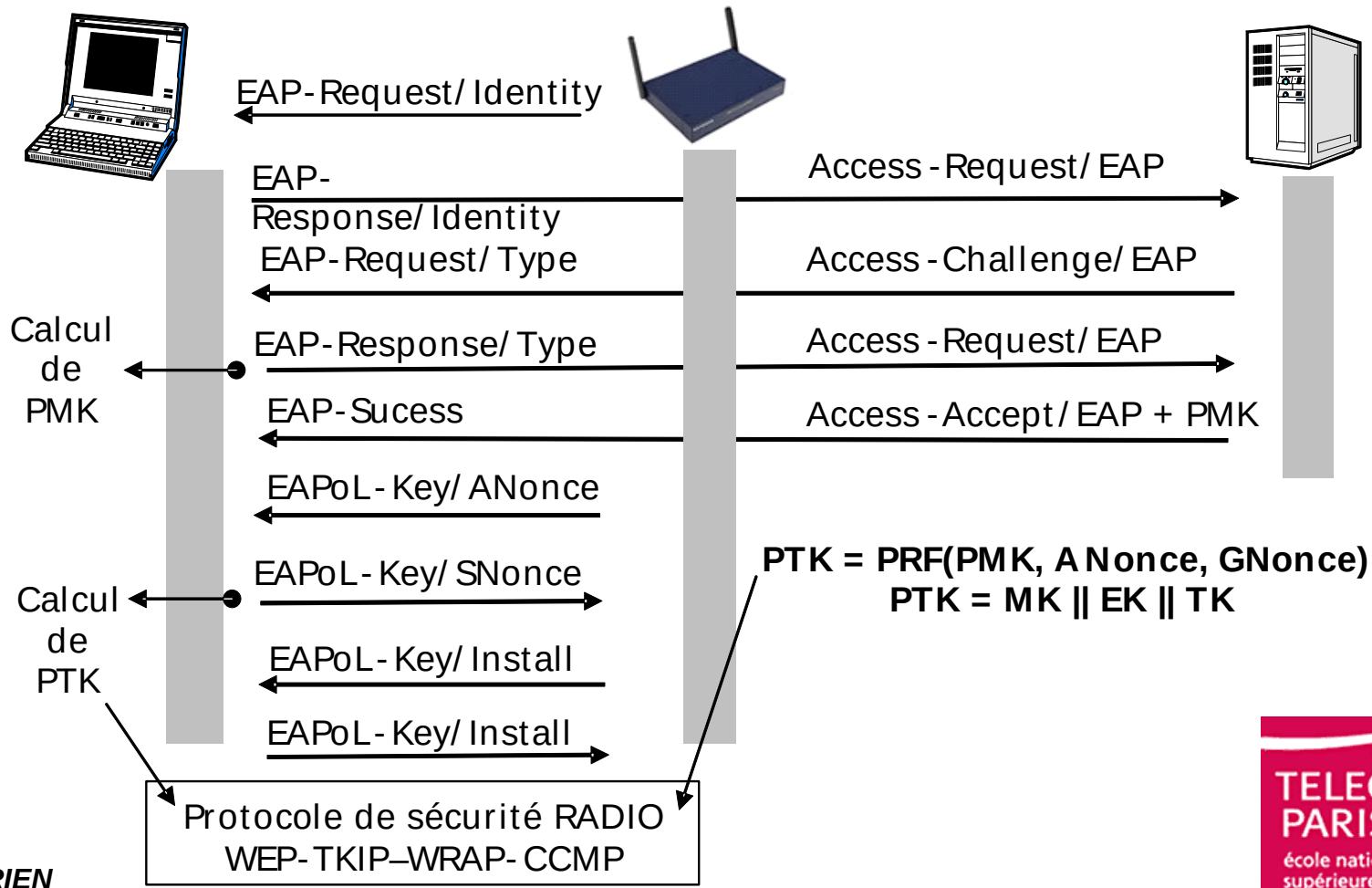
802.11 i: Hiérarchie des clés

- **PMK est déduite de l'authentification EAP.**
- **PSK est une alternative à PMK.**
- **GMK est une clé maître de groupe.**



802.11 i: Distribution des clés

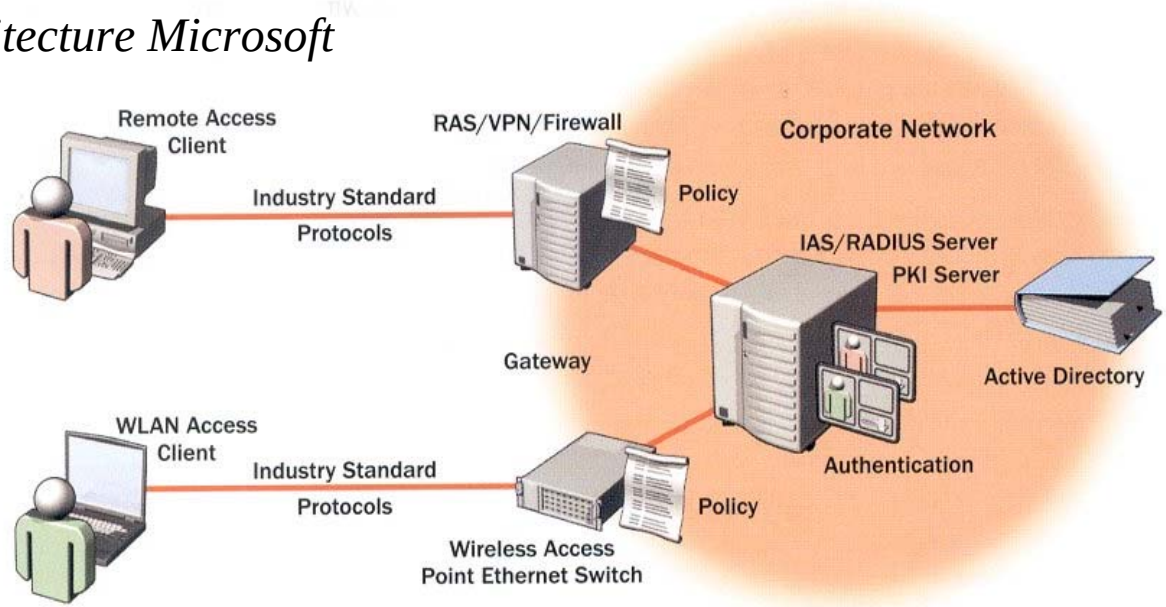
- **Four ways handshake (PTK).**
- **Two ways hanshake (GTK).**



WPA: Wi-Fi Protected Access

- Le *Wi-Fi Protected Access* est une initiative d'un important consortium industriel, destinée à accélérer la diffusion des réseaux sans fil. C'est en fait un sous ensemble de la norme IEEE 802.11i, basé sur le protocole TKIP. Il définit des éléments d'informations spécifiques et des machines d'états de gestion de clés partiellement compatibles avec 802.11i. Le déploiement de cette recommandation implique donc la disponibilité de points d'accès, de cartes réseaux et de *Supplicants* spécifiques.

Exemple d'architecture Microsoft



Le rôle de la carte à puce

- **Les lettres de crédit du réseau sont stockés dans un espace sure et de confiance.**
- **La carte n'est pas clônable.**
- **Le porteur ne connaît pas les lettres de crédit réseaux.**
- **La carte est protégée par deux types de PIN code.**
  - PIN code du porteur.
  - PIN code de l'émetteur.
- **Facteur d'échelle, 1 milliard de cartes produites en 2003.**
- **Plusieurs facteurs de formes, carte de crédit, SIM, interface USB (*token*).**
- **Performances suffisantes, calcul d'une clé RSA 2048 bit en moins d'une seconde.**
- **Capacités mémoire de l'ordre de 64 Ko E^2PROM, ou 1 Mo avec la technologie FLASH.**

TELECOM PARIS
école nationale supérieure des télécommunications

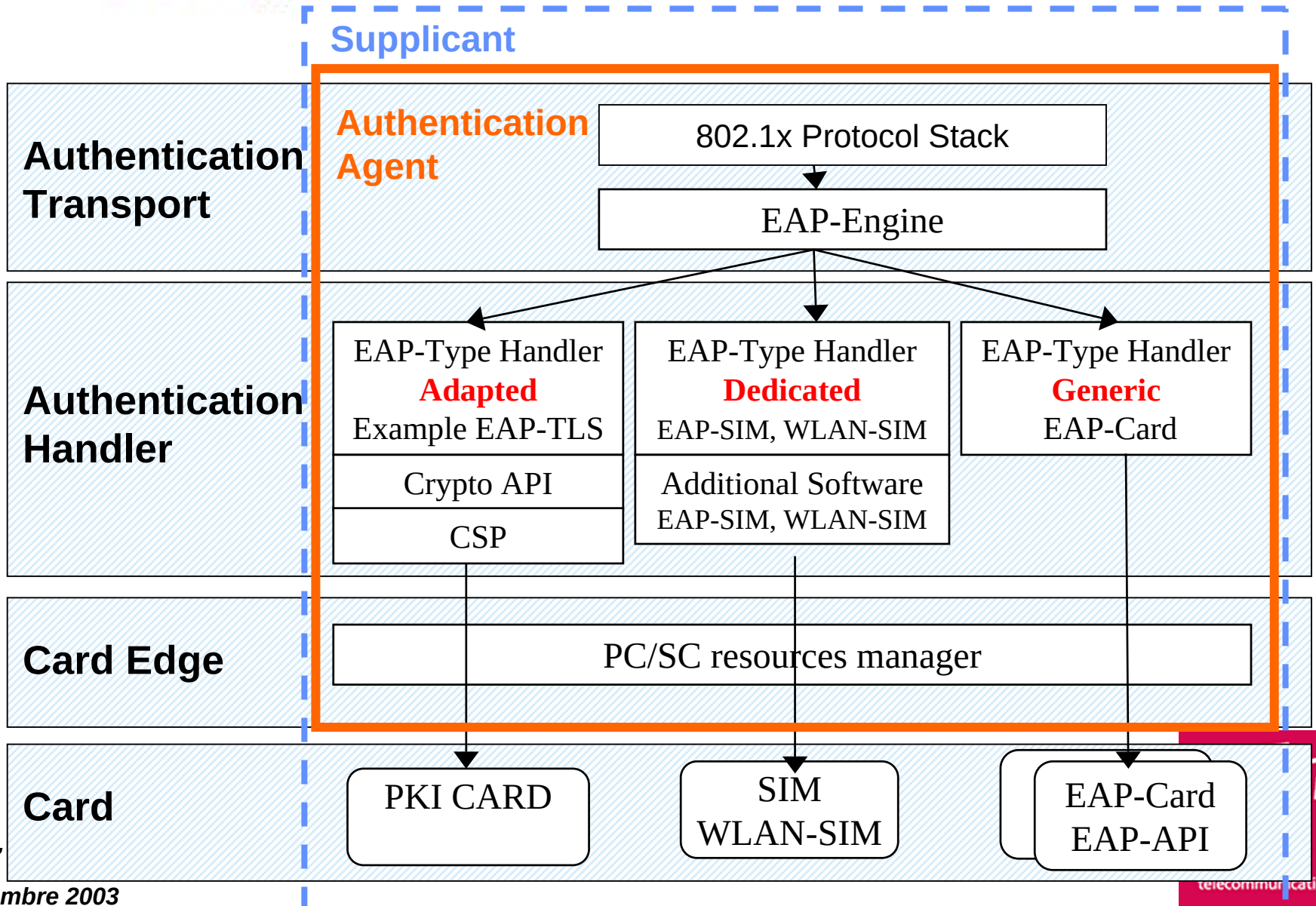
Diverses Approches.

- **L'utilisation de cartes propriétaires, dont l'interface fonctionnelle n'est conforme à aucune norme. Généralement les particularités de tels composants sont masquées par une *API,* c'est-à-dire une interface logicielle offrant des services cryptographiques conformes à des standards par exemple PKCS#11 édité par la société *RSA,* ou CSP déployés sur les systèmes *Microsoft*.**
- **L'utilisation de cartes à puce bien connues, tels que les modules SIM (conformes à la norme GSM 11.11) ou bien des cartes bancaires (BO', EMV…) capables de réaliser des signatures. Par exemple pour implémenter le protocole EAP-SIM [15] il faut disposer d'un composant logiciel additif, qui lorsque nécessaire utilise la carte SIM, c'est-à-dire un ensemble d'ordres ISO 7816-4, nommées APDUs**
- **L'utilisation d'un composant générique, la carte EAP. Dans ce cas une instance logicielle du Supplicant utilise les ressources de la puce sécurisée.**

Le WLAN Smartcard Consortium.

- Active Card
- Alcatel
- Aspects Software Ltd
- Atmel
- Axalto
- BlueWave IP
- Dai Nippon Printing
- ENST
- Gemplus
- Giesecke & Devrient
- Infineon Technologies AG
- Jurgensen & Corcoran Consulting
- Koolspan
- Oberthur Card Systems
- Raak Technologies
- Sagem SA
- SCM Microsystems
- Texas Instruments
- Transat Technologies
- Trusted Logic
- Ucopia
- Visa International

WLAN smartcard – Reference Model

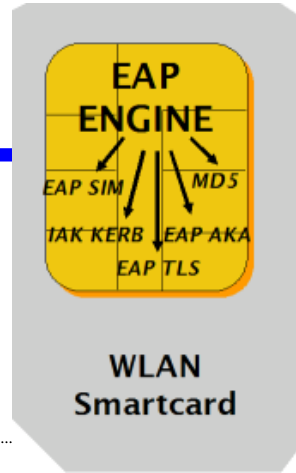


L'API Javacard EAP

- **La carte embarque un moteur EAP qui masque la complexité du protocole.**
- **Une interface java permet l'utilisation simplifiée de ce moteur**

Interface Authenticator	
short	**getAlias**(byte[] buffer, short offset) , Retourne l'Alias de l'interface.
short	**getEAPId**(byte[] buffer, short offset) , Retourne l'identité EAP (***EAP-ID***) de l'interface.
byte	**getEAPType**() , Retourne le type EAP (***EAP-Type***) de l'interface
short	**getRSNMasterKey**(byte[] output, short offset) , Retourne la clé ***PMK***.
short	**init**(javacard.security.Key eapKey) , Initialisation du moteur EAP avec une clé ***eapKey***
short	**processPacket**(byte[] src, short srcofs, short srclen, byte[] dst, short dstofs) Traitement d'un message EAP.
void	**reset**(short session) , Re-Initialisation d'une session d'authentification.
void	**setAlias**(byte[] buffer, short offset, short length), Fixe l'***Alias*** de l'interface.

EAP- API



WISP Applet

Service Provider Interface
EAP-API

Java**C**ard **R**un time **E**nvironment

EAP API

Framework
Classes APIs

Java **V**irtual **M**achine

Smartcard OS

EAP Engine

Files Management

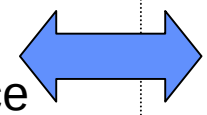
Cryptographic Library

Security Management

IO Management

ISO 7816-4 APDUs
EAP-CARD
WLAN-SIM
SIM

User Interface



La carte EAP: Principes

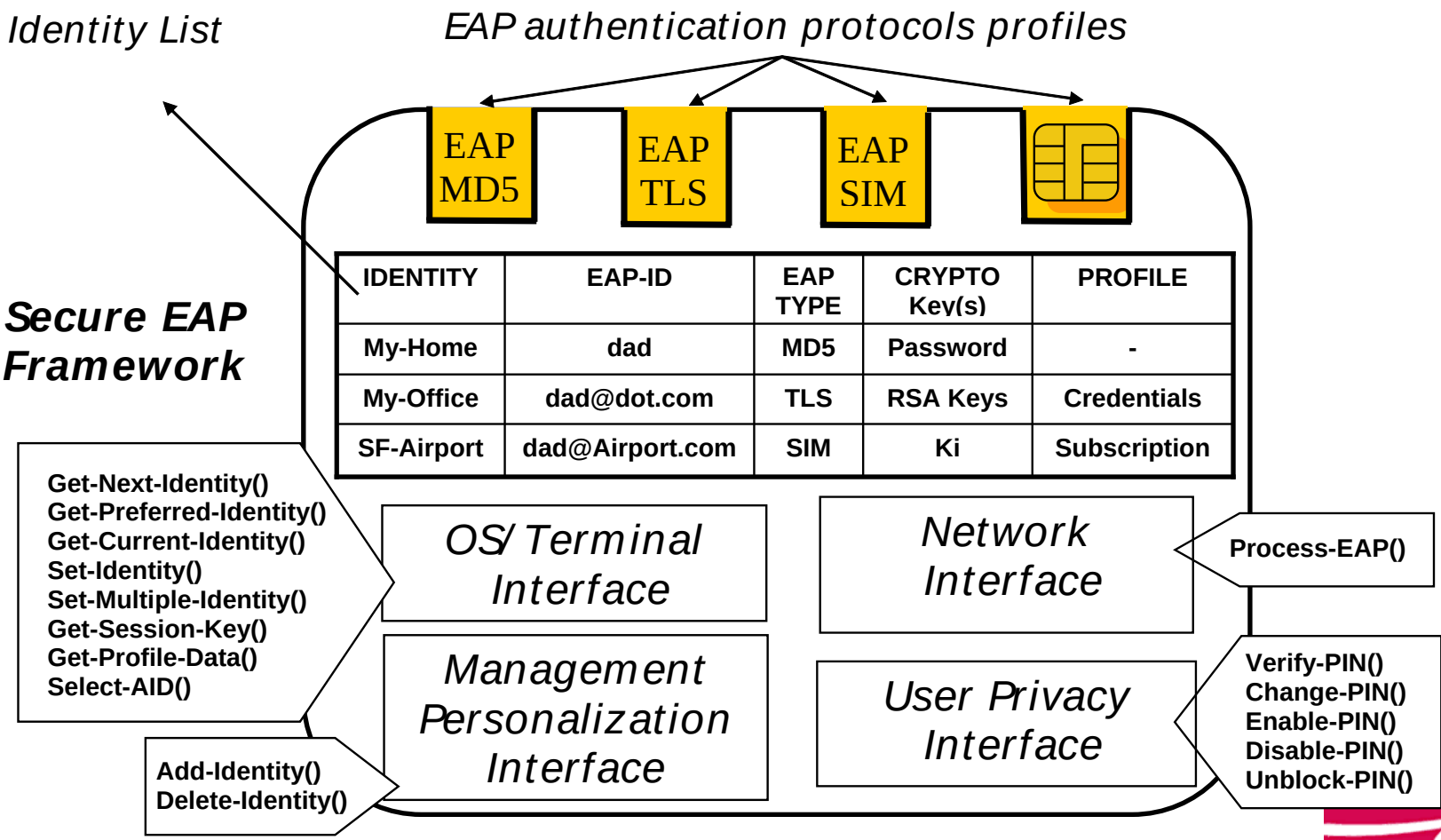
Traitement sécurisés des messages EAP par la carte à puce.

- **Un profile EAP est un guide pour le support d'un protocole particulier.**
  - EAP-SIM
  - EAP-TLS
  - Autres…
- **Une identité est un pointeur sur un triplet (EAP-ID, EAP-Type, lettres de crédit) nécessaire à l'exécution d'une procédure authentification particulière.**
- **La carte gère de multiples protocoles et de multiples identités.**
- **Deux PIN codes :**
  - Utilisateur.
  - Emetteur.

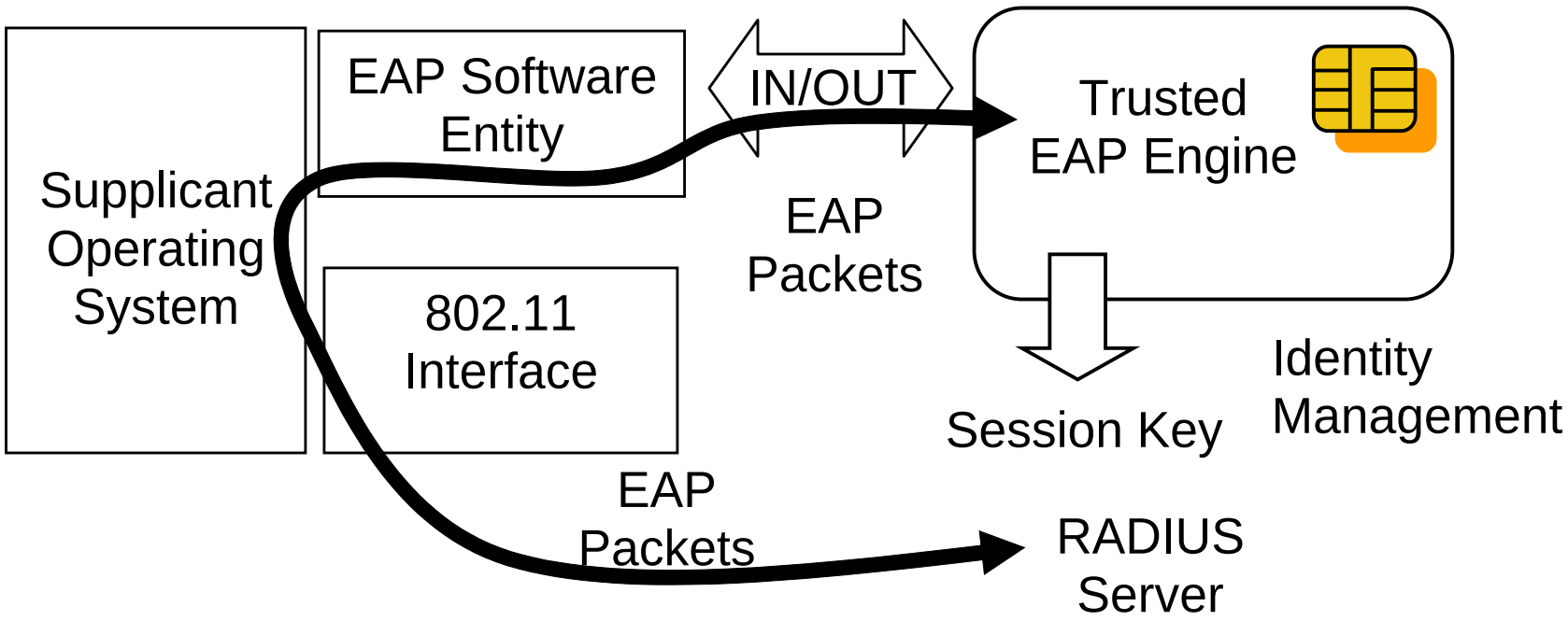
La carte EAP : Services

- **Interface avec le réseau**
  - Traitement des messages EAP
  - Calcul d'une clé de session (PMK …)
  - Profile utilisateur, un ensemble de données utiles au terminal (liste des SSID préférés, certificats X509…)
- **Interface avec le système d'exploitation**
  - Découverte des identités.
  - Sélection d'une identité.
- **Interface de gestion et de personnalisation**
  - Mise à jour des identités et des profiles utilisateur
- **Interface utilisateur et fournisseur de service**
  - PIN codes.

La carte EAP



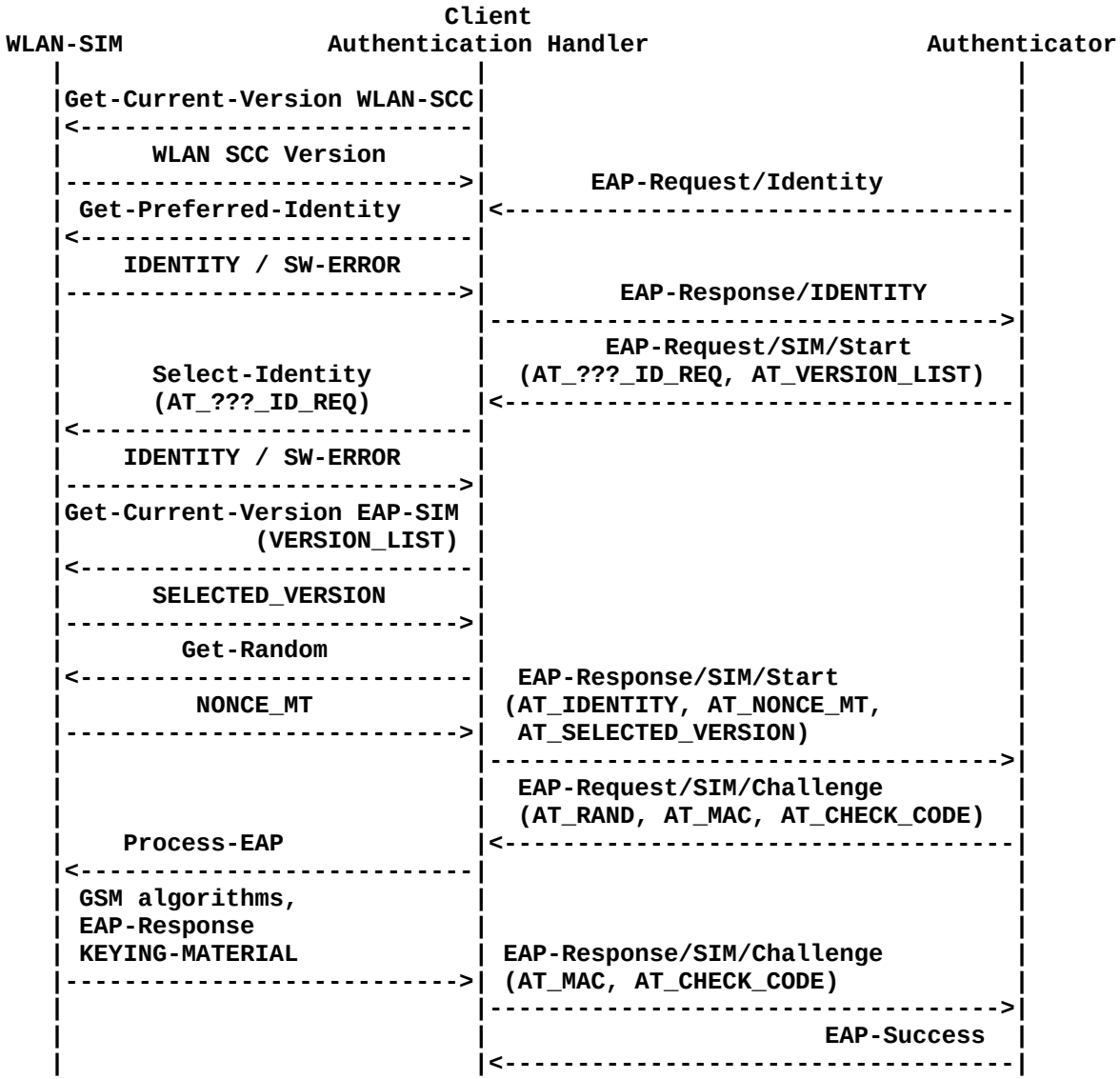
Intégration dans un système d'exploitation



EAP-SIM

- Le point d'accès émet un message EAP-Request/Identity.
- Le Supplicant notifie par un EAP-Response/Identity son identité (EAP-ID).
- Le Serveur d'authentification produit le message EAP-Request/SIM/Start.
- Le Supplicant choisit un nombre aléatoire (NONCE) et l'inclut dans le message EAP-Response/SIM/Start.
- Le serveur d'authentification dispose d'un ou plusieurs triplets GSM (RANDi,SRESi,KCi). Il encapsule dans la requête EAP-Request/SIM/Challenge une liste de valeur RANDi et signe ce message à l'aide d'une empreinte déduite du nombre nonce préalablement reçu (EAP-packet || NONCE). De manière optionnelle, ce message transporte une identité de re-authentification ou un pseudonyme, ces paramètres sont chiffrés.
- Le Supplicant vérifie la signature de la requête. Il produit le message EAP-Response/SIM/Challenge qui contient une empreinte dépendant des valeurs secrètes SRESi (EAP packet || n*SRESi)
- Le serveur d'authentification indique le succès des opérations par un message EAP-Success
- Une clé maître (MK) est déduite d'une empreinte SHA1 (160 bits) réalisée à partir de l'identité courante (EAP-ID) du nombre aléatoire NONCE et de la liste des clés KCi.

La carte WLAN-SIM

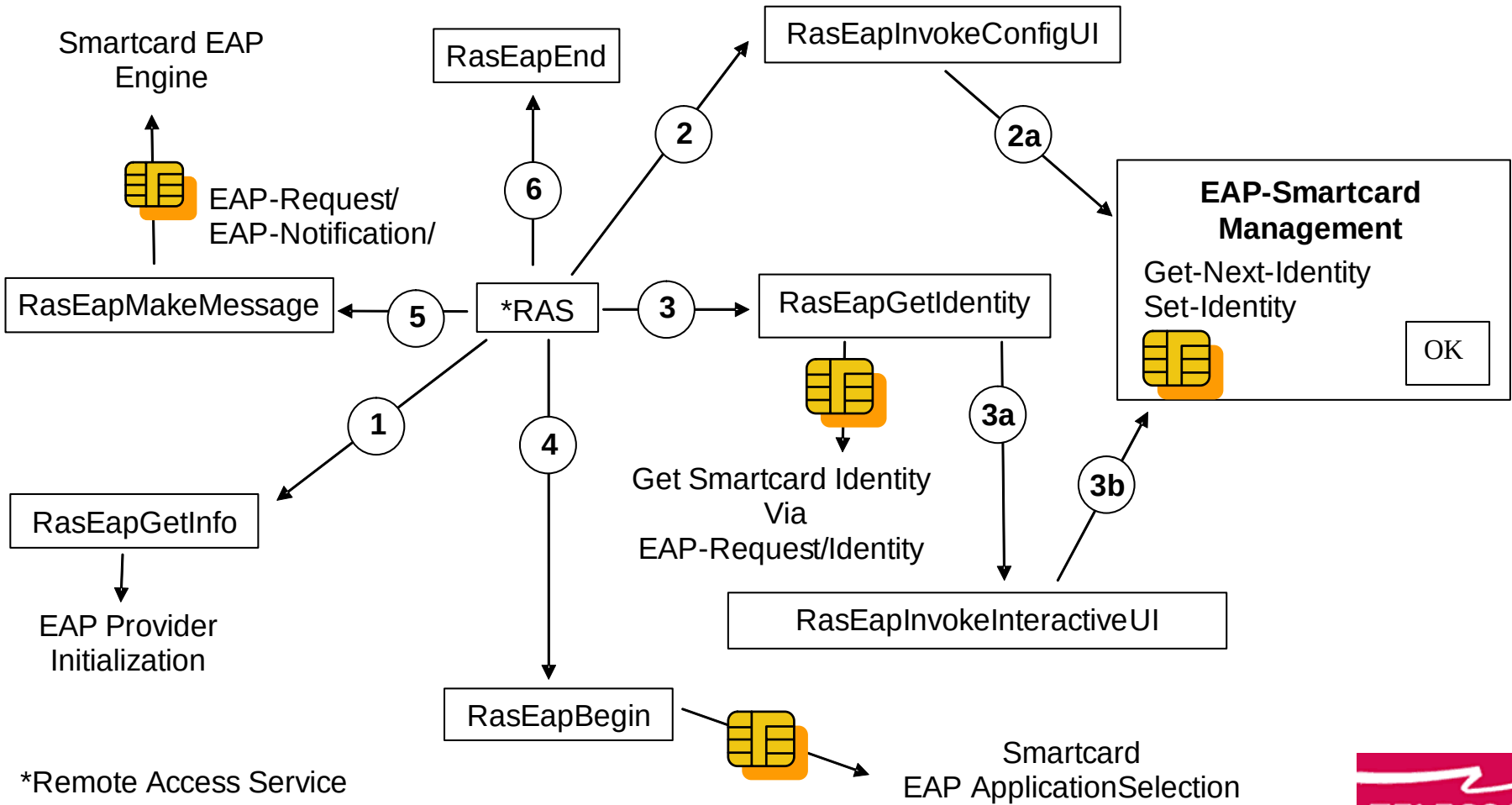


- **Une DLL-EAP par type d'authentification. Une telle librairie supporter plusieurs types d'authentifications.**
- ***DLL CORE***
  - Ras-Eap-GetInfo
  - Ras-Eap-Initialize
  - Ras-Eap-Begin
  - Ras-Eap-MakeMessage
  - Ras-Eap-End
  - Ras-Eap-FreeMemory

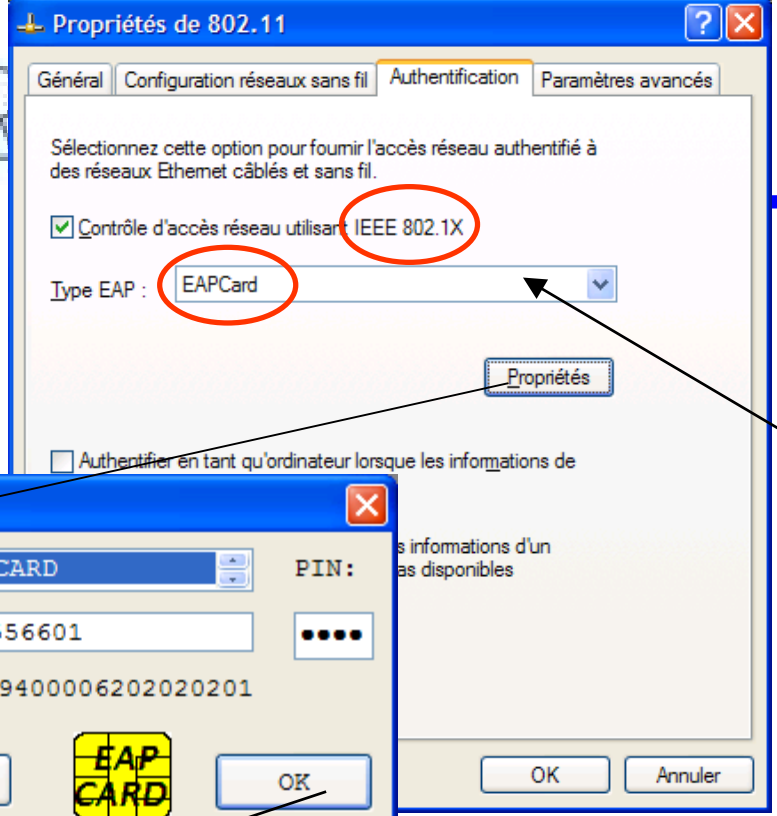
A standard is needed for smartcard interface

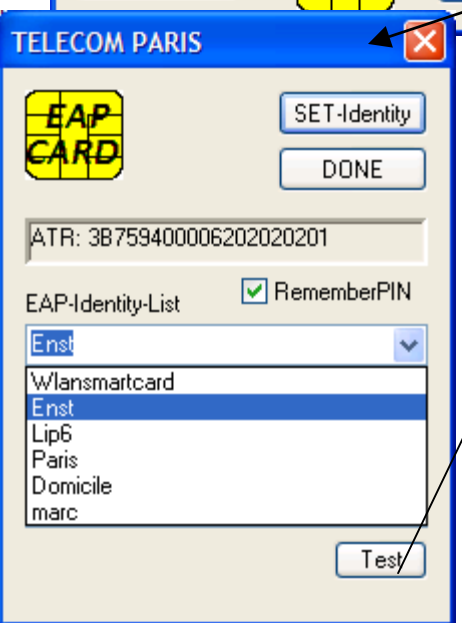
- ***Vendor Specific Services*, ces éléments peuvent être délivrés par une autre librairie.**
  - Ras-Eap-InvokeConfigUI
    - Mise à jour des paramètre utilisateurs (pin code, …)
  - Ras-Eap-InvokeInteractiveUI
    - Paramètres supplémentaires.

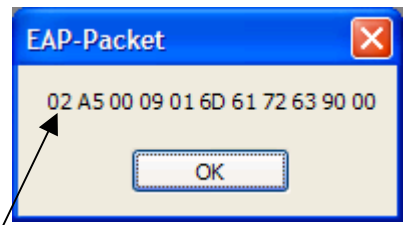
Interaction avec la carte EAP

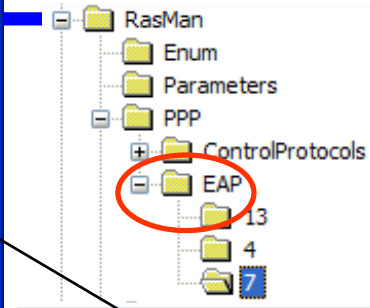


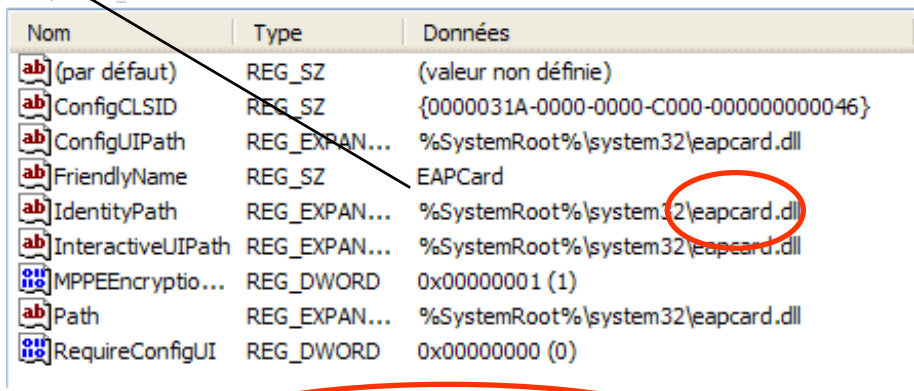
Plateforme XP











Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
ConfigCLSID	REG_SZ	{0000031A-0000-0000-C000-000000000046}
ConfigUIPath	REG_EXPAN...	%SystemRoot%\system32\eapcard.dll
FriendlyName	REG_SZ	EAPCard
IdentityPath	REG_EXPAN...	%SystemRoot%\system32\eapcard.dll
InteractiveUIPath	REG_EXPAN...	%SystemRoot%\system32\eapcard.dll
MPPEEncryptio...	REG_DWORD	0x00000001 (1)
Path	REG_EXPAN...	%SystemRoot%\system32\eapcard.dll
RequireConfigUI	REG_DWORD	0x00000000 (0)

WEP, TKIP, WPA, 802.11i

< 100 €

< 200 €

USB Interface

TELECOM PARIS
école nationale supérieure des télécommunications

Conclusion

- **Nous avons présenté une nouvelle classe de cartes à puce dédiées aux environnements sans fil Wi-Fi.**
- **Ces dernières sont compatibles avec les caractéristiques des puces actuelles (en termes de capacité mémoire ou de puissance de calcul); de surcroît nous avons intégré ces composants aux plateformes Windows.**
- **Tous les éléments techniques sont donc réunis pour le déploiement de telles infrastructures; cependant il n'est pas certain que cette approche, basée sur une technologie typiquement Européenne, résistera au syndrome *NIH* (*Not Invented Here*).**

TELECOM PARIS
école nationale supérieure des télécommunications