# Panorama technologique des supports de l'identité

**Pascal Urien, ENST**

# Identités et Organisations

- **L'identité détermine les autorisations et/ou la localisation d'une personne, d'un objet (parfois intelligent), ou des deux, relativement à une organisation (état, privée…).**
- **L'authentification est le processus qui consiste à faire la preuve d'une identité. On peut utiliser divers moyens,**
  - Ce qui je suis, méthodes biométriques,…
    - Eventuellement multi facteurs (passeport électronique…)
  - Ce que je connais
    - mots de passes, ….
  - Ce que je possède
    - Carte à puce, token…
- **Exemples d'organisations gérant des d'identités**
  - Les états (Identité des citoyens et visiteurs)
    - Biométrie, passeports, cartes d'identité, programme US-Visit
  - Le WEB (Applications WEB)
    - Single Sign On, WEBISO, Microsoft Passport, Liberty Alliance
  - L'industrie (localisation, inventaire…)
    - Etiquettes, RFID
  - Services informatiques (ordinateurs personnels)
    - TPM
  - Réseaux bancaires (opération de paiement)
    - Cartes BO', Cartes EMV
  - Réseaux télématiques (échange de données)
    - GSM et carte SIM
    - IP sans fil, EAP-ID, IEEE 802.1x, carte EAP
    - Token, SecureID
- **Que peut on fédérer ?**
  - Les mots de passes
  - Les clés RSA (modules TPM, cartes bancaires EMV, carte d'identités, …)

# Techniques Biométriques

# Techniques Biométriques

- **De multiples modalités**
  - Empreinte digitale, empreinte d'iris, empreinte palmaire, reconnaissance faciale …
- **La biométrie n'est pas exacte, il y a un risque statistique :**
  - Taux de rejet (**FTE** ou *Failure To Enroll*): pourcentage d'échantillons non analysés en raison de défauts.
  - Taux de faux rejets (**FRR** ou *False Rejection Rate*) : pourcentage de non reconnaissance erronées.
    - Pose un problème d'indemnisation d'un éventuel préjudice.
  - Taux de fausses acceptations (**FAR** ou *False Acceptation Rate*) : pourcentage de reconnaissances erronées.

- **Alternative au mot de passe**
  - Remplacement du PIN code d'une carte à puce (par exemple *DeXa Badge* d'Axalto).
  - Remplacement des mots de passe (PC + TPM)
- **Passeport électronique, carte d'identité**
  - Authentification à deux facteurs
    - Techniques d'imprimerie sécurisées
    - Carte à puce (avec ou sans contact)
      - **empreinte digitale**
      - **photographie**
- **Base de données centralisée ou distribuée**
  - BD distribuée: données personnelles
    - Technologie *Match On Card (MOC)*
    - Java Card Biometry API
  - BD centralisée: programme US-Visit
    - Lecture du passeport
    - Enregistrement des empreintes des index.
    - Photographie du visage

© actronix

Caractéristiques :

• Jusqu'à 4000 empreintes mémorisées au sein d'un même boîtier permettant les opération d'enrôlement et de vérification

• Interface utilisateur intuitive avec 3 témoins lumineux et signaux sonores.

• Détection automatique du doigt permettant une identification simple et instinctive.

• Boîtier compact et ergonomique.

• Options multiples d'administration :

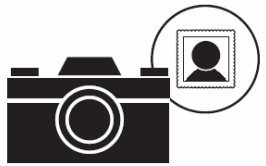
- en autonome (en connectant un PC portable)
- en réseau (option Ethernet)

Temps de vérification : < 1 seconde pour 100 utilisateurs enrôlés

Temps d'enrôlement : < 3 secondes

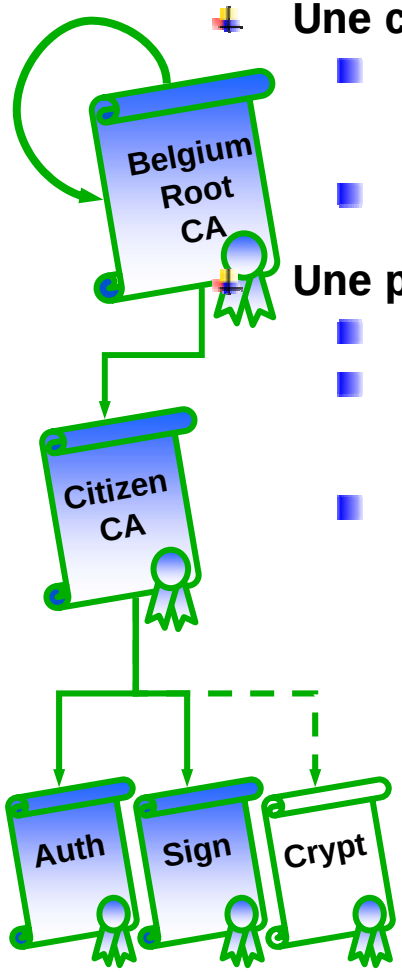
| Taux : | | |
|---|---|---|
| Fausse Acceptation | Rejet | d'Egal Erreur (EER) |
| 0,005 % | 0,01 % | 0.1% |

Prix : environ 1 400 €

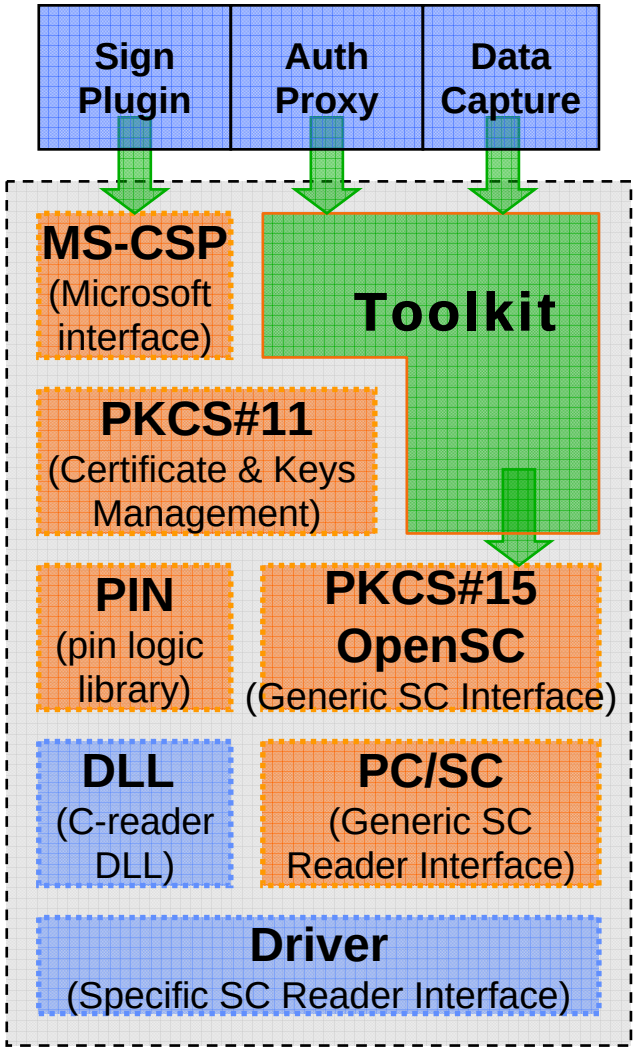
# La carte d'identité électronique Belge

# La carte d'identité Belge: bi facteurs

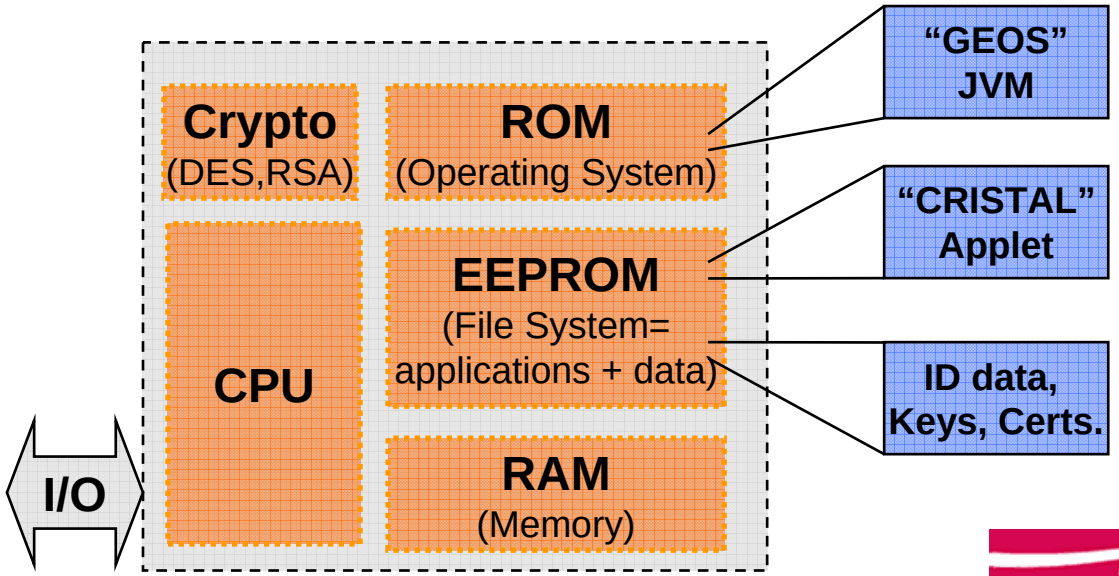



- **Une carte imprimée**
  - Imprimerie sécurisée (*rainbow and guilloche printing, Changeable Laser Image –CLI-, Optical Variable Ink –OVI-, Alphagram, Relief and UV print, Laser engraving*)
  - Nom, Prénom, Genre, Date de naissance, Nationalité, numéro de carte, période de validité, signature, photographie
- **Une puce** *tamper resistant*
  - Une carte java de 32 Ko E$^2$PROM qui loge application spécifique (eID)
  - Un répertoire (Dir-ID) qui stocke des données (nom, prénom, adresse, photographie) identiques à celles qui sont imprimées et signées par le RRN (*Rijksregister – Registre National*).
  - Un répertoire (Dir-BelPIC, protégé par PIN code)), conforme au standard PKCS15, qui stocke des certificats X509 émis par le *Citizen CA*, et les clés RSA privées.
    - Un certificat d'authentification (Auth), authentification WEB, SSO…
    - Un certificat de signature (Sign), document, formulaire WEB, …
    - Un certificat (Crypt) pour les opérations de chiffrement est également prévu

# Les services




- Carte JAVA
- CPU: 16 bit
- Crypto processeur:
  - 1100 bits RSA
  - 112 bits DES
- ROM (OS): 136 Ko (GEOS JVM)
- $E^2$PROM (Application + Données): 32 Ko (Cristal Applet)
- RAM: 5 Ko



# Architectures *Single Sign On*

**WEBISO**

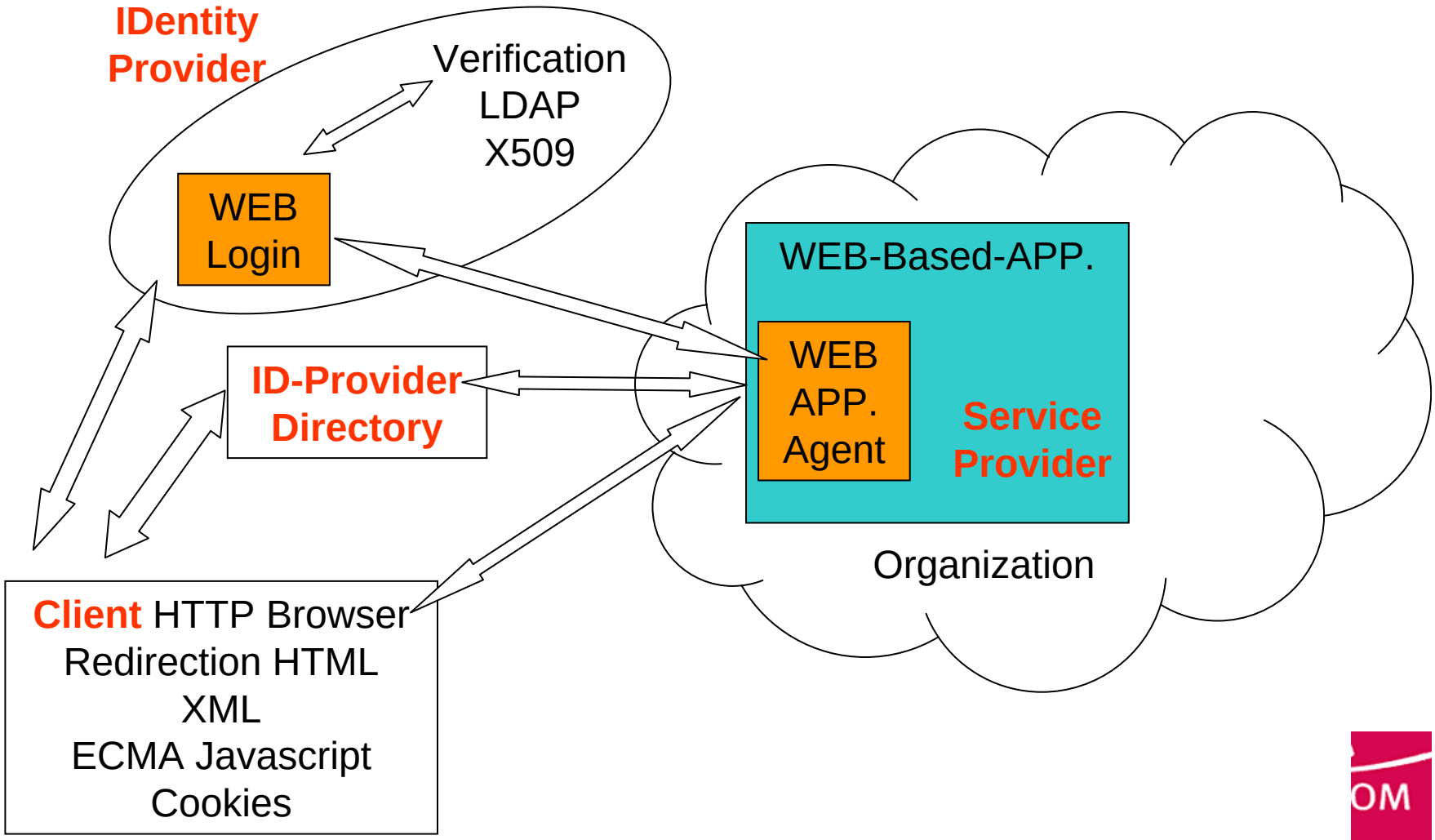
**.netPassport**

**Liberty Alliance**

# Architectures de *Single Sign On*

- **De nombreuses organisations proposent des applications accessibles à travers des interfaces WEB (*WEB based App*)**
  - Les identités des utilisateurs (login, password, certificats) sont stockées sur des bases de données.
  - Le processus d'authentification consiste à vérifier l'identité d'un utilisateur afin d'établir ses droits relativement à un service disponible.
  - On désigne par *"Sign On"* l'opération d'identification / authentification d'un utilisateur du service.
  - Une architecture *"Single Sign On"* permet d'éviter de multiples d'opérations *" Sign On"*.
- **Exemples**
  - *WebISO*: Service model and component capabilities, draft-morgan-webiso-model-01 (2003).
    - Un modèle des applications WEB
  - *.netPassport*, Microsoft
    - Une identité unique pour tous les services
  - *Liberty Alliance*
    - Une fédération d'identités pour de multiples services.

# Le modèle WEBISO



- **Un passeport est une collection de deux classes d'informations *Credential et Profile*, identifiée par un PUID (*Passport User ID*, 64 bits)**
- **Les messages d'authentification sont échangés sous forme de tickets, insérés dans des *cookies*.**

| Information | Data Type | Required to create a Passport? | Shared with other sites? |
|---|---|---|---|
| email address (Sign in name) | Credential and Profile | Yes | If user opts-in |
| Password | Credential | Yes | Never |
| Secret Questions and Answers | Credential | Optional | Never |
| Mobile Phone Number and Mobile PIN | Credential | Context dependant | Never |
| Security Key | Credential | Optional | Never |
| Birth Date, Country/Region, First Name, Gender, Last Name, Occupation, Postal Code, Preferred Language, State, Time Zone | Profile | Optional | If user opts-in |

Service Provider

Accords Contractuels
(SERVICE PROVIDER Key


{Ticket}Service Provider Key

Participant Cookie
{Ticket}ServiceProviderKey


4 Sign In

3 TGT

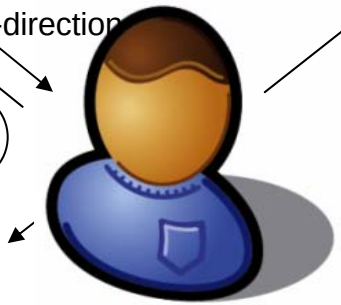
1 Passport login

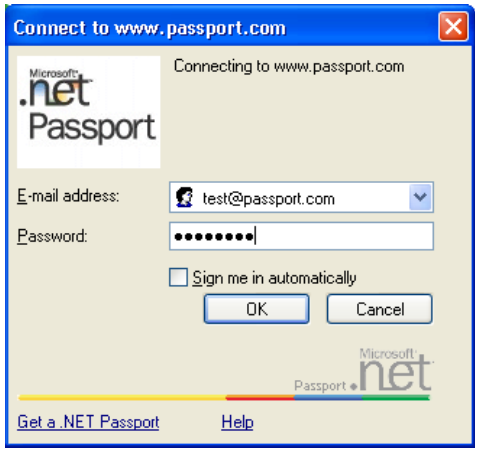
Site de gestion des passeports

HTTP Re-direction

Service Provider Login

2






Cookie du Service Provider
{Ticket}Service Provider Key

Cookie d'Authentification
TGT, Ticket-Granting Cookie
{PUID,Password}SSL

TELECOM PARIS
école nationale supérieure des télécommunications

# Mais … des “bugs” 3/3

- **Usurpation d’identité par vol de cookie (durée de validité d’un cookie de l’ordre de 15 mn)**
- **Failles dans la confidentialité des informations stockées dans le passeport découvertes par** *Marc Slemko* **(en 30 mn!) en Novembre 2001.**
- **Richard Purcell (Microsoft) le 01/10/2001 : « nous ne pouvons pas garantir une sécurité totale sur Passport »).**
  - http://www.men.minefi.gouv.fr/webmen/revuedeweb/passport.html
- **Mai 2003, Muhammad Faisal Rauf Danka, (étudiant pakistanais) accède à tous les comptes** *passport*, **en insérant la chaîne** *emailpwdreset* **dans une URL d’accès**
  - https://register.passport.net/emailpwdreset.srf?lc=1033&m=victim@hotmail.com&id=&cb=&prefem=attacker@attacker.com&rst=1
  - L’attaquant (*attacker@attacker.com*) reçoit un courrier électronique contenant une URL qui lui permet de changer le mot de passe du compte cible.

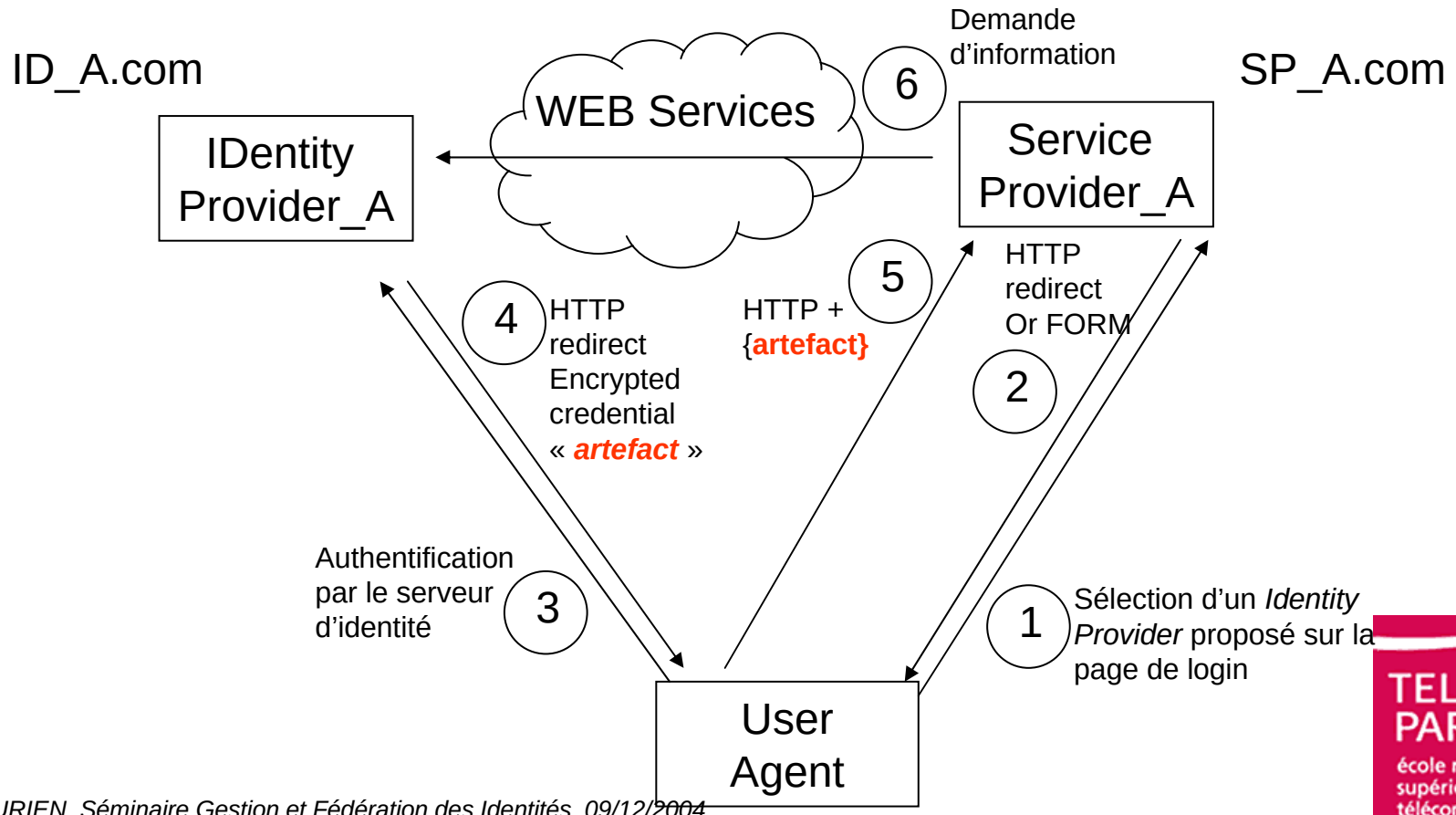
- **Objectifs**
  - Fédération* de multiples identités associées à des fournisseurs de services WEB.
    - L'identité la plus commune est un couple (login, password). Le login peut être un identifiant de compte ou un NAI (*Network Access Identifier*, RFC 2486), similaire à une adresse de courrier électronique (la partie située à gauche de @ représente un identifiant de compte, la partie droite est le nom du domaine (serveur) gérant ce compte).
  - Une seule procédure d'authentification est suffisante pour accéder à un ensemble de services (*Single Sign On*).
  - L'infrastructure assure l'anonymat de l'utilisateur entre services fédérés.
- **Les entités fonctionnelles**
  - L'utilisateur (*User*); il possède un terminal informatique muni d'un navigateur WEB.
  - Les fournisseurs de services WEB (*Service Provider*).
    - Un Service Provider gère une identité pour déterminer/appliquer les droits/privilèges du client (*Authorization*).
    - *"Liberty explicitly accommodates identity provider use of arbitrary authentication mechanisms and technologies"*
  - Les gestionnaires d'identités (*IDentity Provider*).
    - La fédération de deux identités gérées par le *Service Provider* et *Identity Provider* est un acte volontaire du client.
  - Le lien entre *Service Provider* et *Identity Provider* sont réalisé par des *WEB services*.

*Fédération, n. fém. (lat. foedus, foederis «alliance»).
1. Organisation politique et administrative de l'État fédéral.
2. Par ext. Groupement de sociétés, d'associations, de syndicats, etc.

TELECOM PARIS
école nationale supérieure des télécommunications

et_2@ID_A.com
**Alias="abcd"**
- SecurityDomain= "SP_A.com"
- **Name = "1234"**

et_1@SP_A.com
**Alias="1234"**
- SecurityDomain= "IDP_A.com"
- **Name = "abcd"**



# Identité des objets

## Etiquettes

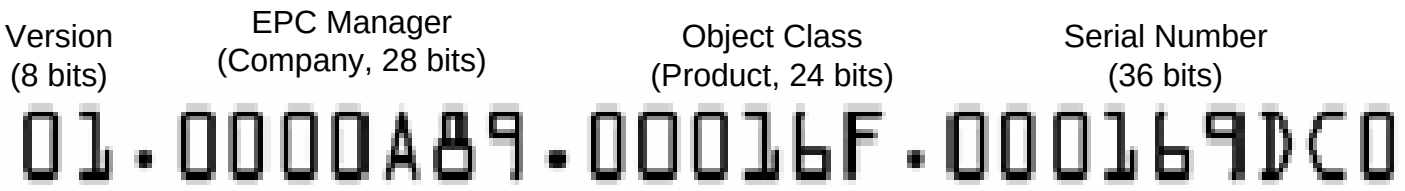
## RFID

# Etiquettes Electroniques 1/3

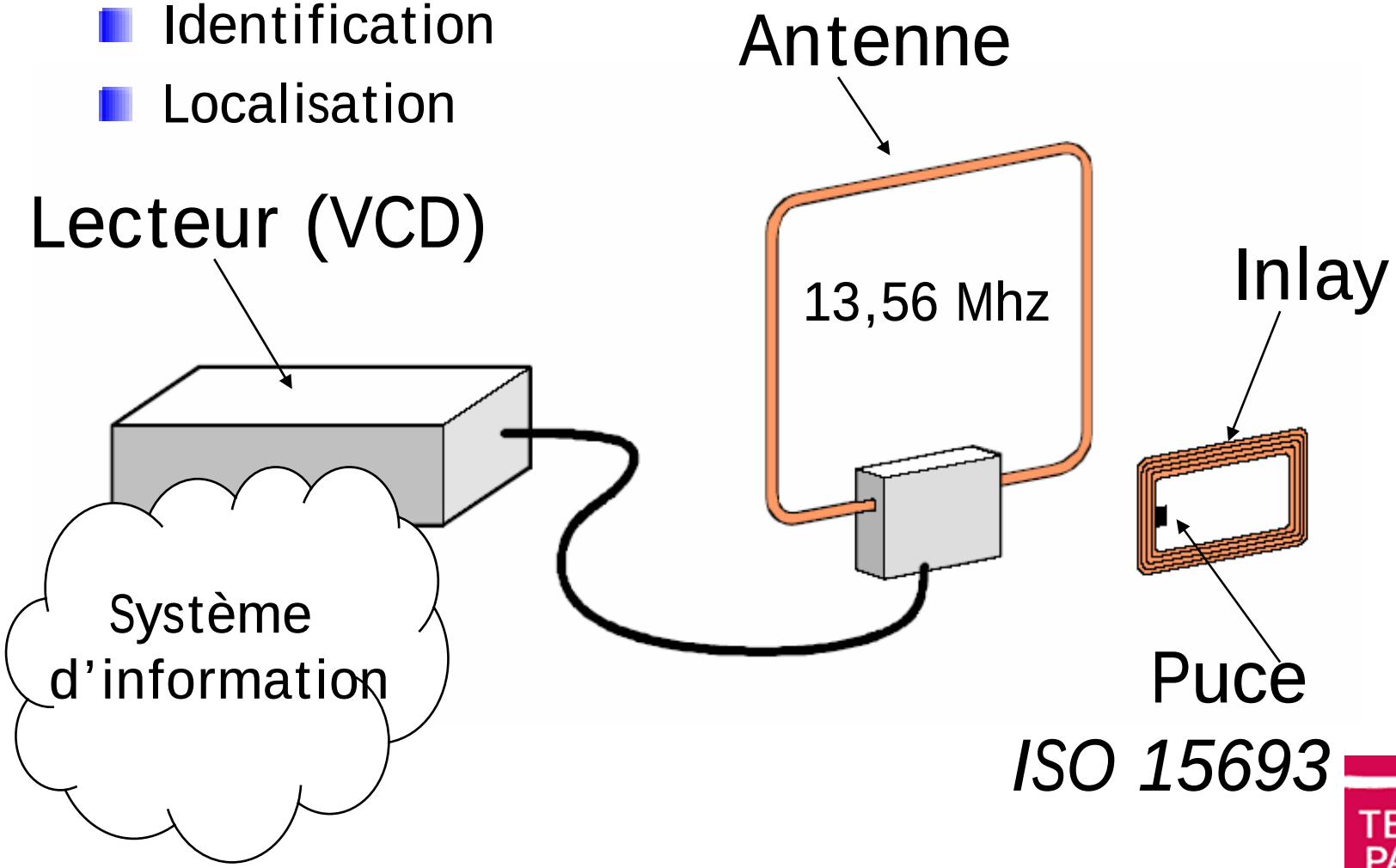
- **Les produits sont actuellement identifiés par des codes barres à lecture optique.**
  - GTIN, *Global Trade Item Number* (code à 8,12,13,14 chiffres)


Exemple: Code GTIN, 13 chiffres

- **Etiquette électronique (TAG)**
  - EPC, *Electronic Product Code* (code à 64, 96 bits)

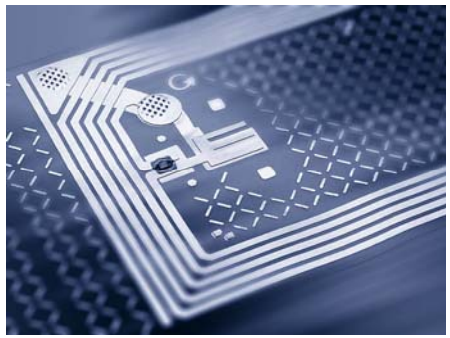


- **Services**
  - Identification
  - Localisation



# RFID ISO-15693 3/3

- **Vicinity coupling device (VCD), Vicinity Integrated Circuit Card (VICC).**
  - Fréquence de travail (fc) 13,56Mhz.
  - Débits (en mode *single carrier*) 6,62 kbits/s (fc/2048) 26,48 kbits/s (fc/512)
  - Distance de fonctionnement compris entre quelques centimètres et un mètre.
  - Champs magnétique d'opération compris entre 0,15 A/m et 5 A/m
- **Organisation de la mémoire**
  - 256 blocs au plus de taille maximale 256 bits
- **Paramètres VICC**
  - Unique identifier (UID) 64 bits.
  - Application family identifier (AFI) 8 bits.
  - Data storage format identifier (DSFID) 8bits.

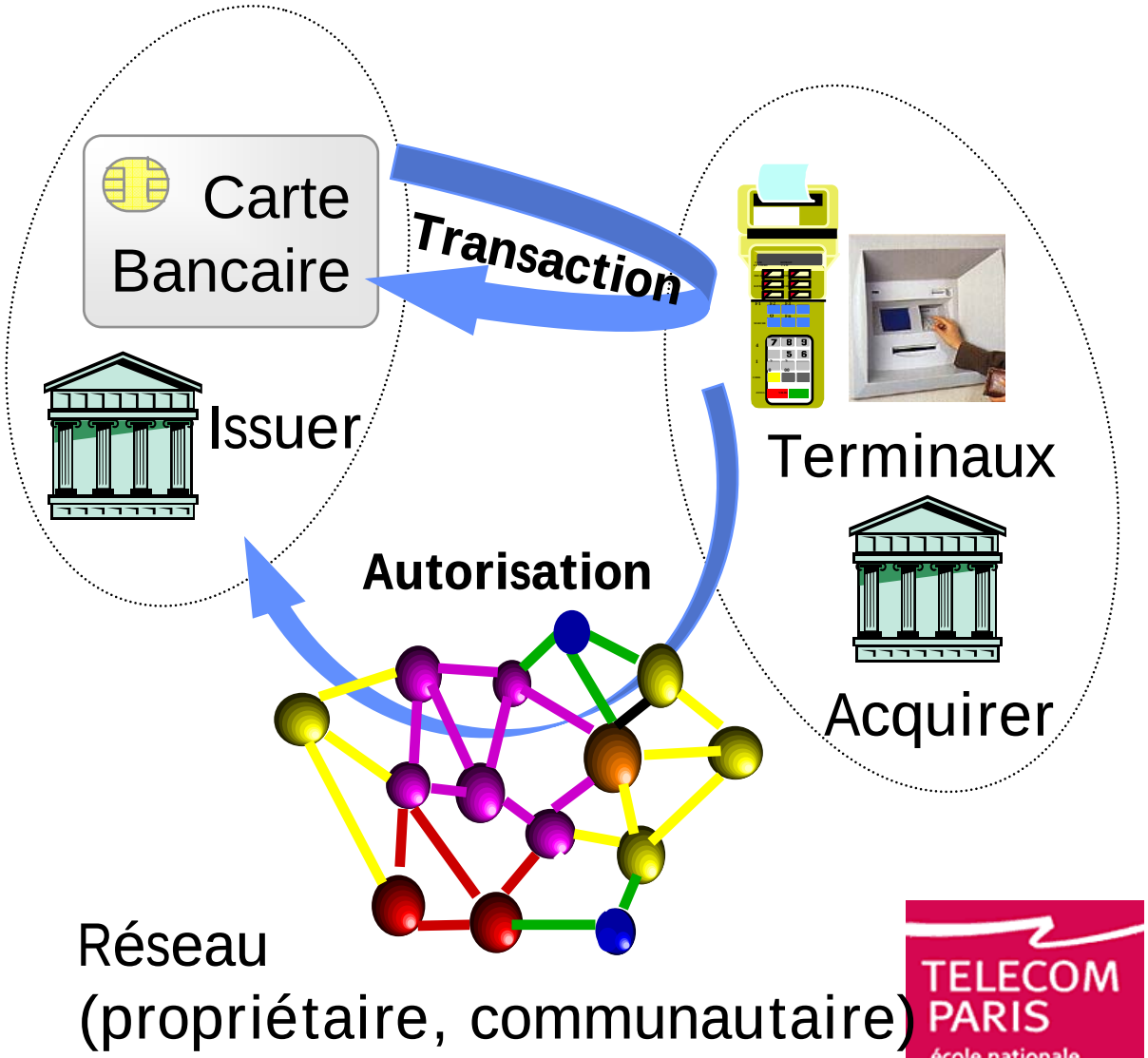


- **15 Commandes VICC sont définies par la norme ISO 15693-3**
  - Inventory, Stay Quiet, Reset to Ready, Select
  - Read Single Block, Read Multiple Blocks, Write Single Block, Write Multiple Blocks, Lock Block, Get Multiple Block Security Status
  - Write AFI, Lock AFI
  - Write DSFID, Lock DSFID
  - Get System Information
  - Custom, Proprietary.

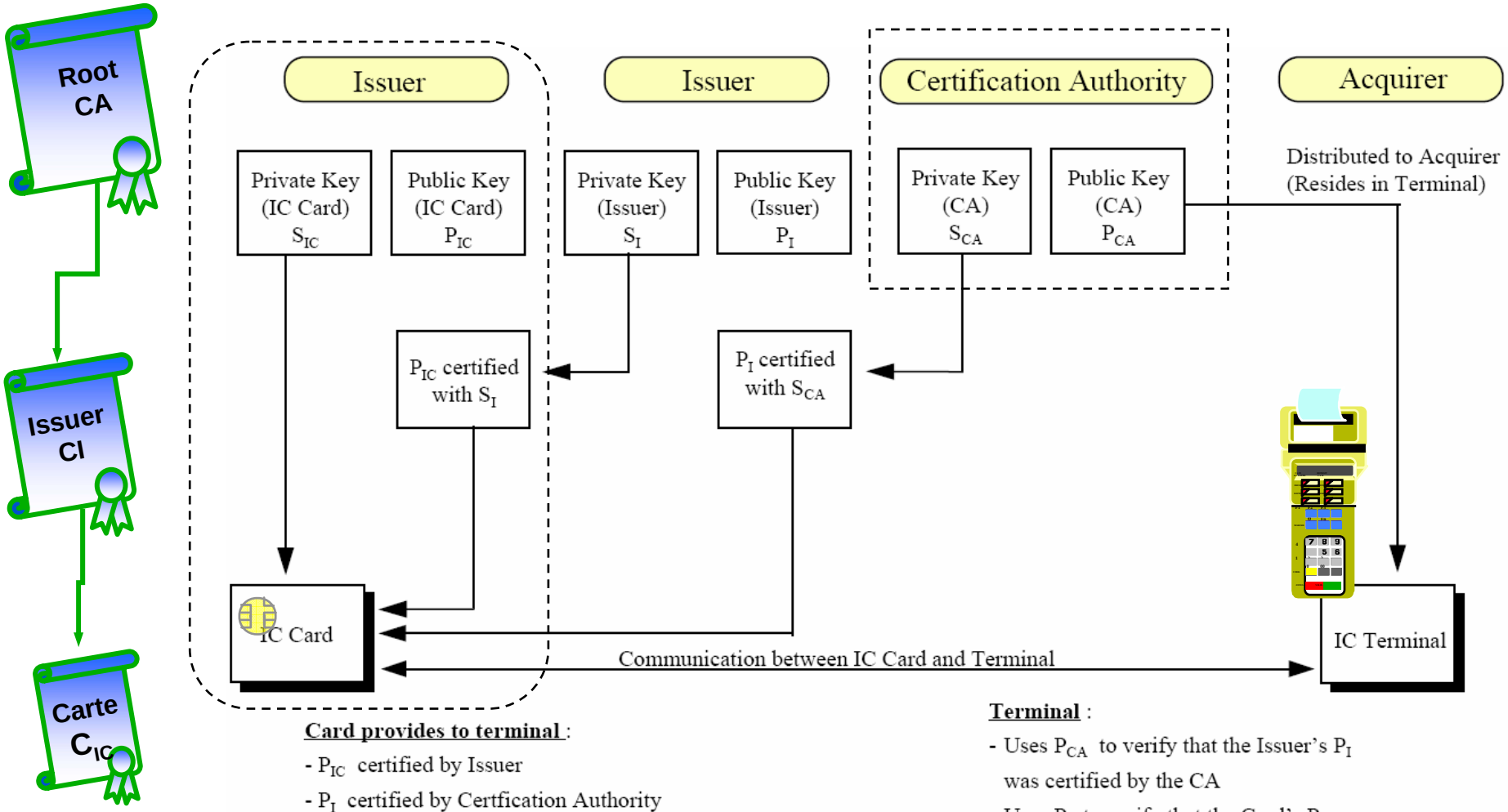
# Réseaux de Paiement

# Infrastructure de paiement & Identité

- **Trois entités fonctionnelles**
  - Emetteur de la carte.
  - Acquéreur.
  - Réseau.
- **Identité**
  - Numéro de carte
- **Deux types d'authentification**
  - Statique, valeur signée stockée dans la carte
    - Valeur de Signature VS pour BO'
    - Certificat pour EMV
  - Dynamique, algorithme cryptographique exécuté par la carte
    - Clé symétrique (BO') + fonction TELEPASS
    - Clé asymétrique (EMV) gérée par la carte + fonction RSA
- **Authentification à deux facteurs**
  - PIN code du porteur
  - Clés cryptographiques gérée par l'émetteur



# EMV: Dynamic Data Authentication




**Card provides to terminal** :

- $P_{IC}$ certified by Issuer
- $P_I$ certified by Certfication Authority
- Card and terminal dynamic data with digital signature

**Terminal** :

- Uses $P_{CA}$ to verify that the Issuer's $P_I$ was certified by the CA
- Uses $P_I$ to verify that the Card's $P_{IC}$ was certified by the Issuer
- Uses $P_{IC}$ to verify the digital signature of the card data

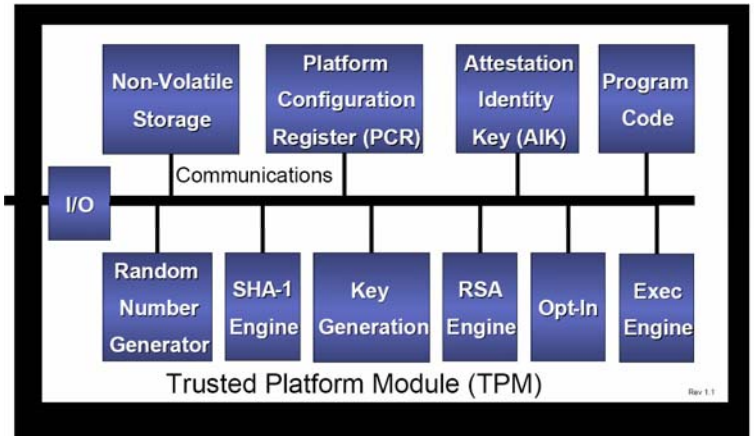
# Identité des Plateformes

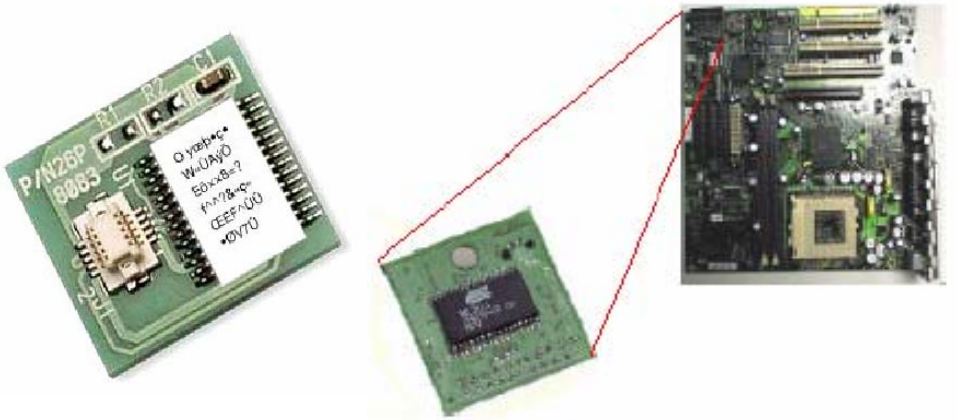
## TCG et TPM

# Identité des plateformes: TPM

- **Un module de sécurité lié à une carte mère (TPM,** *Trusted Platform Module)*
  - Un composant proche d'une carte à puce (mêmes fondeurs)
- **Un modèle de sécurité figé, TCG -** *Trusted Computing Group.*

| Attaque | Solution courantes | Défauts | Apports TPM |
|---|---|---|---|
| Vol de données | Chiffrement, intégrité (VPN, …) | Stockage des clés dans des espaces non sures | Stockage sécurisé des données |
| Accès non autorisés à une plateforme | 1)Login, mot de passe<br>2) Biométrie<br>3)Token externes (cartes à puce…) | 1) Attaques par dictionnaire<br>2) Fiabilité des techniques biométriques<br>3) Crédits d'authentification indépendants de la plateforme | Protection des données d'authentification liée à la plateforme. |
| Accès au réseau non autorisé | Windows network logon, IEEE 802.1X | Données d'authentification stockées dans un espace non sure | Stockage sécurisé des données d'authentification. |

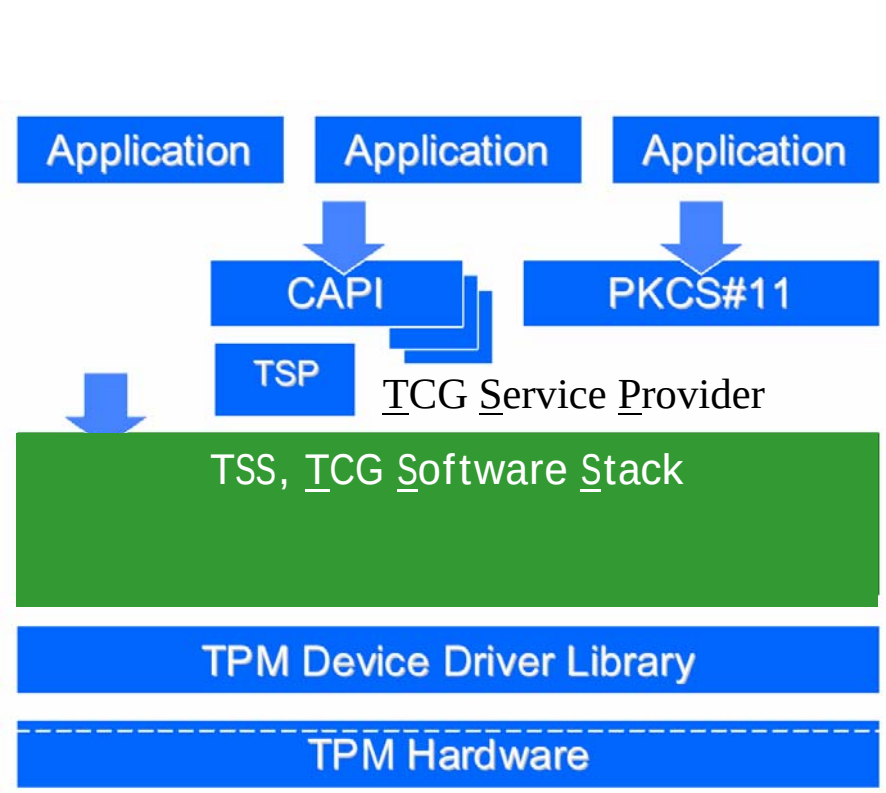


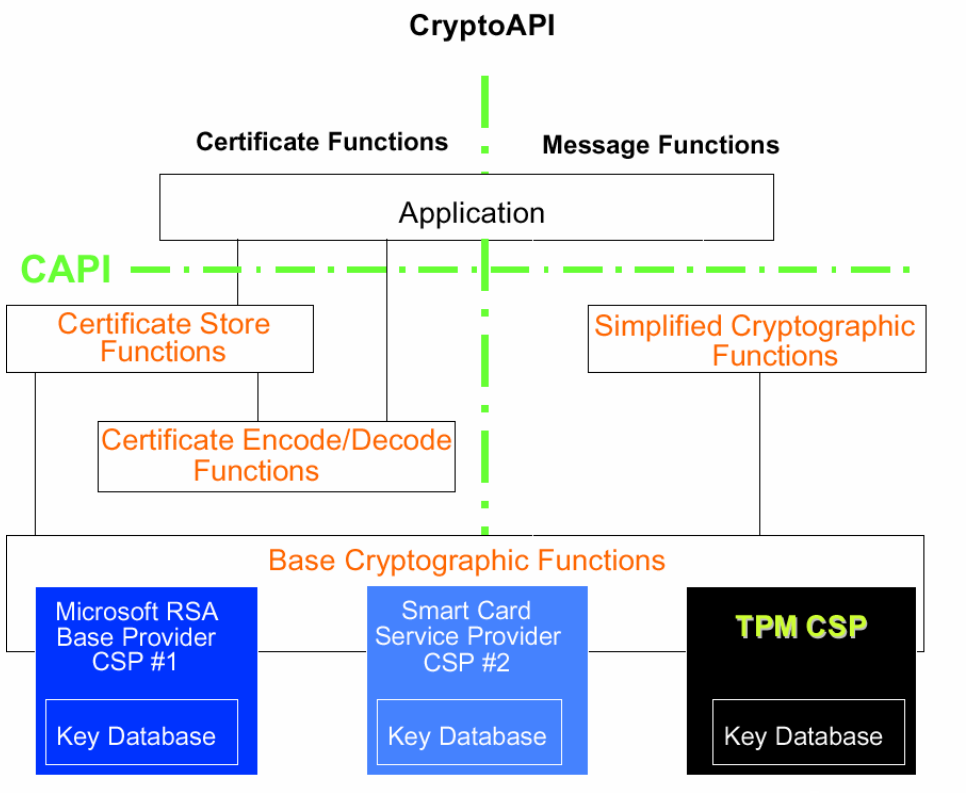



# TCG, Modèle

- **Owner Key, clé maître d'autorisation symétrique, 160 bits**
- **Endorsement Key (EK),clé RSA 2048 bits**
  - Deux modes de génération sont disponibles, création par le TPM, ou stockage sous contrôle de la clé *Owner Key*.
  - Permet d'établir un canal de communication sure ($\{M\}_{EK\_publique}$ avec le TPM (qui stocke la clé privée EK).
- **Storage Root Key (SRK), clé RSA 2048 bits**
  - Le TPM gère un anneau de clés privés RSA de stockage; la clé d'indice 0 est SRK; la clé d'indice k est chiffrée par la clé d'indice k-1. Une goutte de clé (*key blob*) est la valeur chiffrée d'une clé K stockée à l'extérieur du TPM.
  - Une goutte d'information (*data blob*) est un fichier protégé à l'aide d'une clé de stockage k.
  - La hiérarchie des clés de stockage est par exemple *TPM, administrateur, utilisateur*.
  - Les clés de stockage sont activées à l'aide de *Personal Identification Number* (mot de passe, biométrie, carte à puce…)
- **Platform Configuration Register (PCR)**
  - 16 registres de 20 octets sont disponibles pour stocker des empreintes (produite par un fonction SHA1)
  - Une goutte d'information peut être liée au contenu d'un registre PCR, dans ce cas les données sont liées à la plateforme
- **Attestation Identity Keys (AIKs)**
  - Le TPM stocke des clés publiques délivrées par une autorité de certification CA. L'action conjointe de CA et de l'administrateur du TPM ( {{M}AIK_Private)}EK_publique ) permet de produire des données d'authentification pour un service (par exemple une paire de clé RSA).
- **Des clés RSA 2048 bits**
  - Les clés Parents (*Parent Keys*) sont crées sous contrôle de la clé *Owner Key.*
  - Les clés Enfants (*Child Keys*) sont générées sous le contrôle d'une clé parent.

# Pile Logicielle TCG





école nationale supérieure des télécommunications

# Identité des réseaux

**SecureID**

**GSM**

**Wireless LAN**

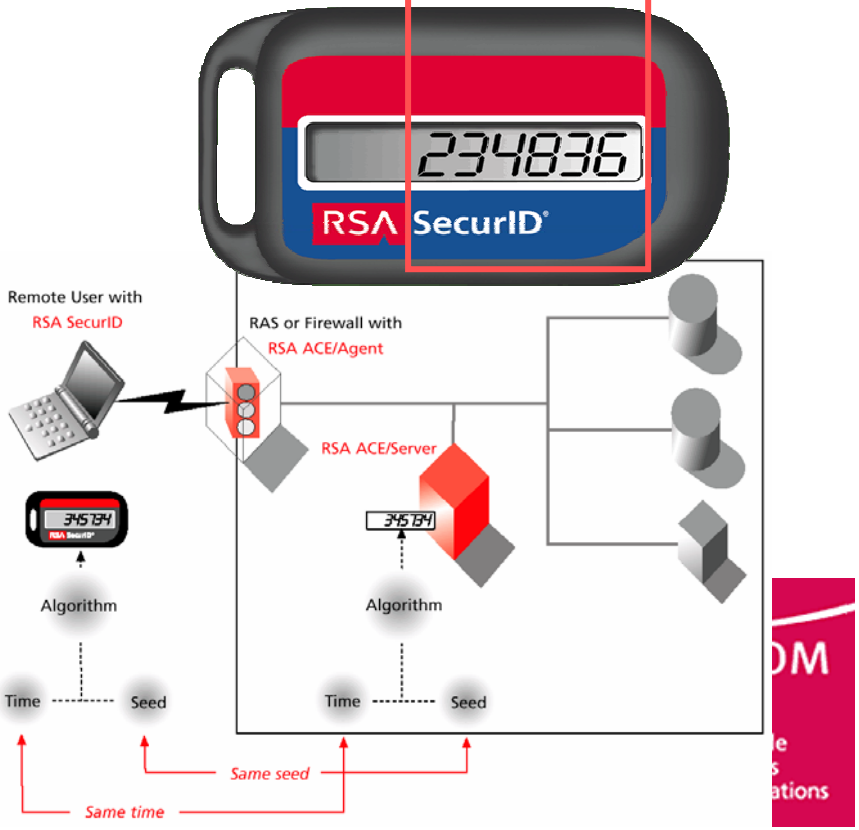
**Carte EAP**

# SecurID 1/1

- **Authentification à deux facteurs: PIN code + TOKEN**
- **Supporté par les plateformes Windows fin 2004**

```
Login:      FMARTIN
Passcode: 2468234836
```

**Mot de passe = PIN + Token Code**

# L'identité sur le GSM – GSM1/1

- **Une authentification à deux facteurs (PIN code + clé secrète Ki)**
- **Une carte SIM supporte 21 commandes réparties en quatre groupes**
- **Gestion des fichiers ISO 7816 (10)**
  - Un répertoire Télécom contient des informations telles que les annuaires utilisateur.
  - Un répertoire GSM contient des fichiers tels que l'identité de l'abonné (**IMSI**)
- **Contrôle des accès (5) aux fichiers (PIN codes, PUK, ..)**
  - L'usage des fichiers et de l'algorithme d'authentification sont contrôlés par le PIN code (blocage après trois faux codes).
- **Un algorithme d'authentification symétrique A3/A8, associé à une clé Ki de 128 bits (commande *RUN_GSM_ALGORITHM).***
- **A partir d'une valeur d'entrée de 16 octets, il produit 12 octets, les 4 premiers constituent la signature SRES, et les 8 suivants la clé Kc (mais 10 bits sont forcés à zéro) utilisée pour le chiffrement des paquets voix (avec l'algorithme A5)**
  - L'algorithme COMP128-1 a été craqué en 1998, en $2^{19}$ vecteurs
  - L'algorithme A5/1, version forte, a été craqué en 99
  - L'algorithme A5/2, version faible, a été craqué en 99
- **Transfert de données (5) avec le mobile (messages SMS,...)**

# Historique des normes de sécurité – WLAN 1/4

**1999 — 802.11**

- Wireless Equivalent Privacy WEP
- Chiffrement RC4 à l'aide de secrets partagés (statiques)
- Pas d'infrastructure de distribution de clés

**2001 — IEEE 802.1x avec WEP**

- Extensible Authentication Protocol EAP
- Calcul d'une clé de session
- Distribution dynamique des clés WEP

**WEP est cassé**
Arbaugh & All
Fluhrer & All $2^{22}$

**2003 — WPA**

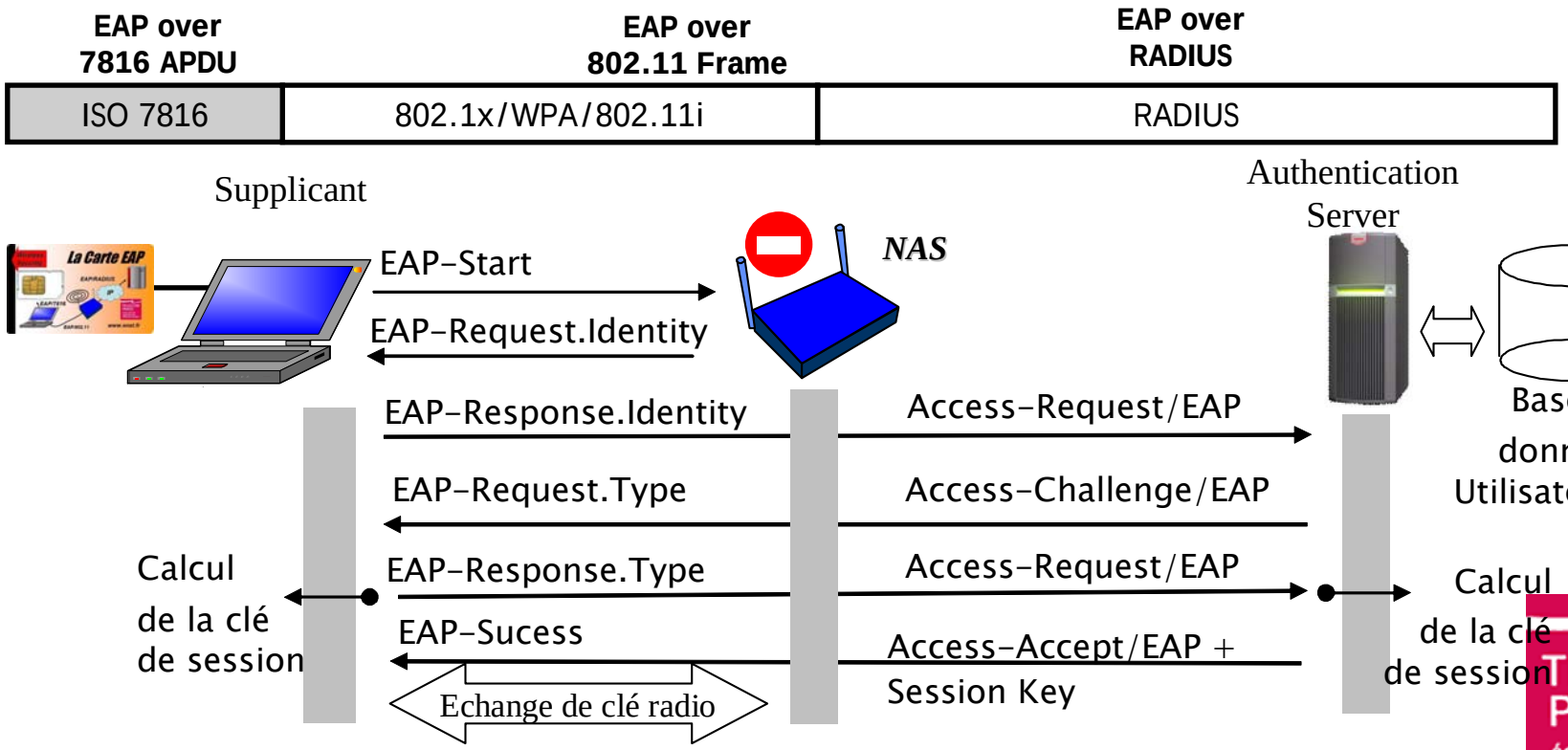
- Version IEEE 802.11i de Mars 2003 – IEEE 8021x + EAP + TKIP
- Distribution des clés avec mutuelle authentification AP/Poste Client
- WEP amélioré (WEP2) TKIP

**2004 — 802.11i (WPA2)**

- Infrastructure d'authentification 802.1x +EAP
- Four way handshake
- Basé sur AES
- Pre Shared Key possible entre AP et client.

# 2001, IEEE 802.1X – WLAN 2/4

- **Trois entités, Supplicant (client), Authenticator (Access Point), Authentication Server (serveur RADIUS).**
- **Authentification Mutuelle entre Supplicant et Authentication Server**
- **Echange de clé pour la sécurité radio**

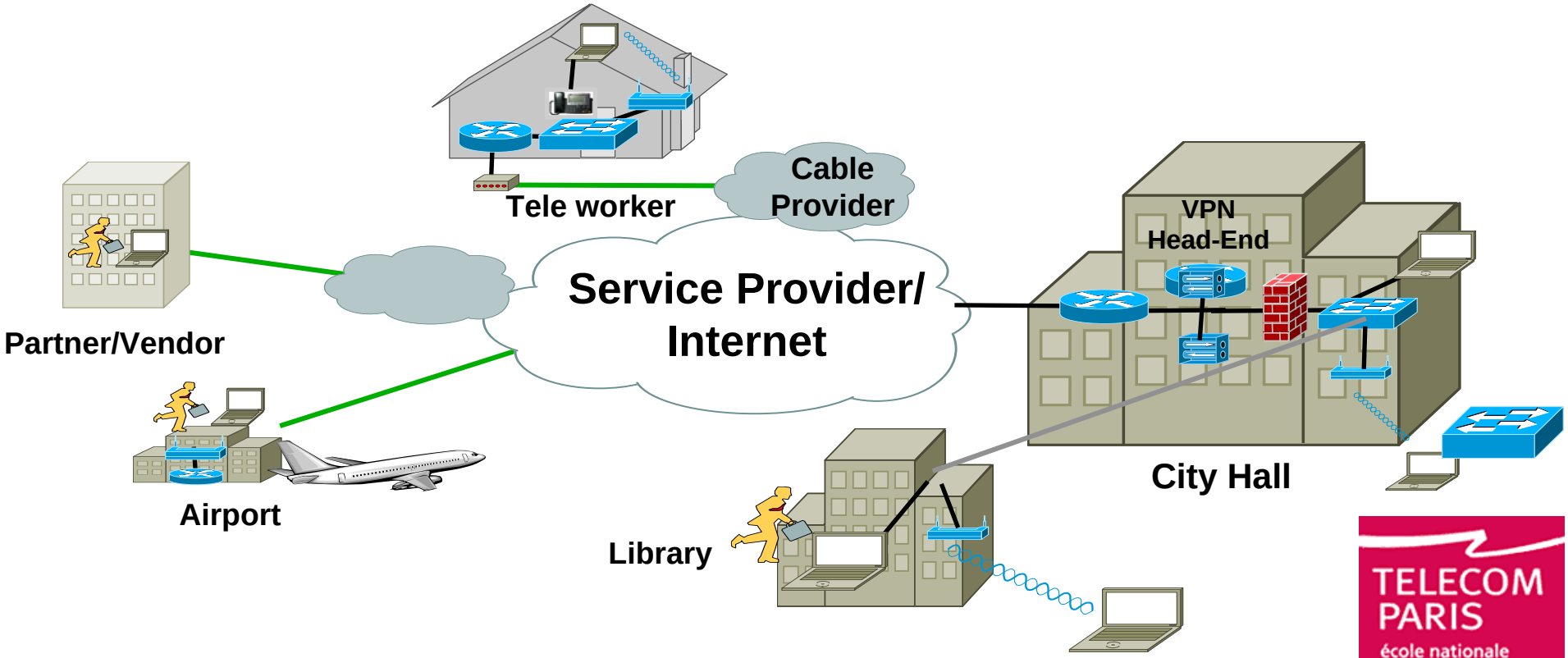


# EAP et carte à puce – WLAN 3/4

- **Extensible Authentication Protocol**
  - Un protocole parapluie qui transporte de multiples méthodes d'authentification
    - EAP-SIM, importation de l'architecture d'authentification du GSM
    - EAP-TLS, infrastructure d'authentification basée sur des clés asymétriques et des certificats
    - EAP-MSCHAPv2, authentification à base de mot de passe pour les plateformes Windows
    - Etc…
  - Triplet d'authentification (EAP-ID, Méthode d'authentification, lettre de crédit)
- **L'authentification est la clé de voûte de la sécurité des réseaux sans fil IP émergents**
  - Wi-Fi (IEEE 802.11), Wi-Max (IEEE 802.16), Wi-Mobile (IEEE 802.20), WirelessUSB (IEEE 802.15).
- **La carte à puce EAP**
  - Une carte qui traite le protocole EAP.
  - http://www.infres.enst.fr/~urien/security

# CISCO: Identity Based Network Services – WLAN 4/4

- **Une même identité (EAP) pour**
  - De multiples terminaux (*Supplicants*)
  - De multiples réseaux d'accès



# Conclusion

# Conclusion

- **De multiples organisations**
  - Des moyens d'authentifications et des réseaux qui présentent beaucoup de similitudes
- **Quelle confiance peut on avoir dans ces infrastructures compte tenu des expériences antérieures (GSM, WEP, .netPassport…)**
- **Que peut on fédérer ?**
  - « la résistance d'une chaîne sécurisée dépend de son maillon le plus faible ».