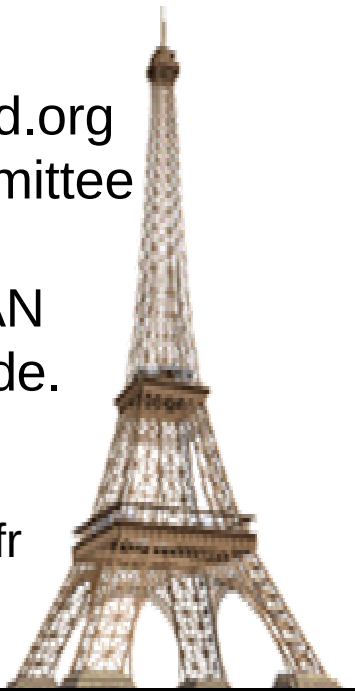
WLANSmartCard.org

WlanSmartcard.org Technical Committee

Wireless LAN A primer guide.

Paris, February 5th

Pascal.Urien@enst.fr



WLANSmartCard.org

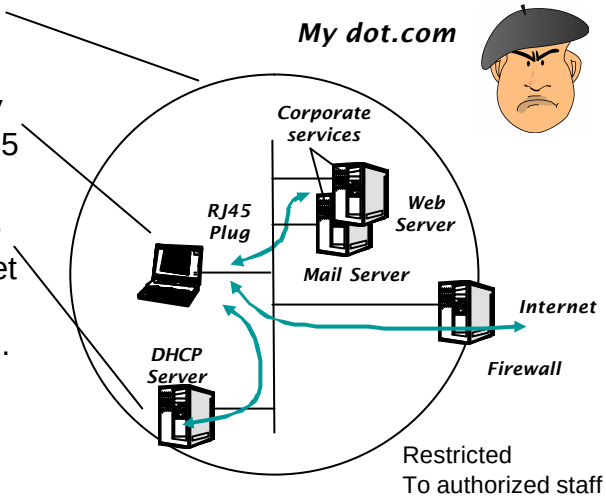
From wired internet to ubiquitous wireless internet

Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

Classical intranet.

- Network access is restricted to authorized staff.
- PCs are physically connected by RJ45 plugs.
- DHCP servers are unsecured, intranet services are freely available (indoors).

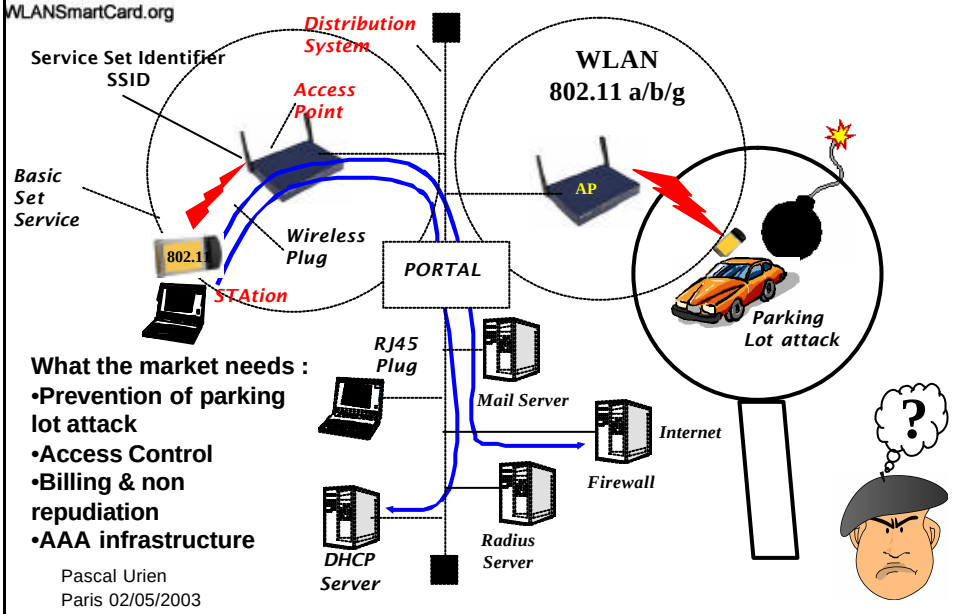


Restricted
To authorized staff

Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

Wireless LAN



What the market needs :
- **Prevention of parking lot attack**
- **Access Control**
- **Billing & non repudiation**
- **AAA infrastructure**

Pascal Urien
Paris 02/05/2003

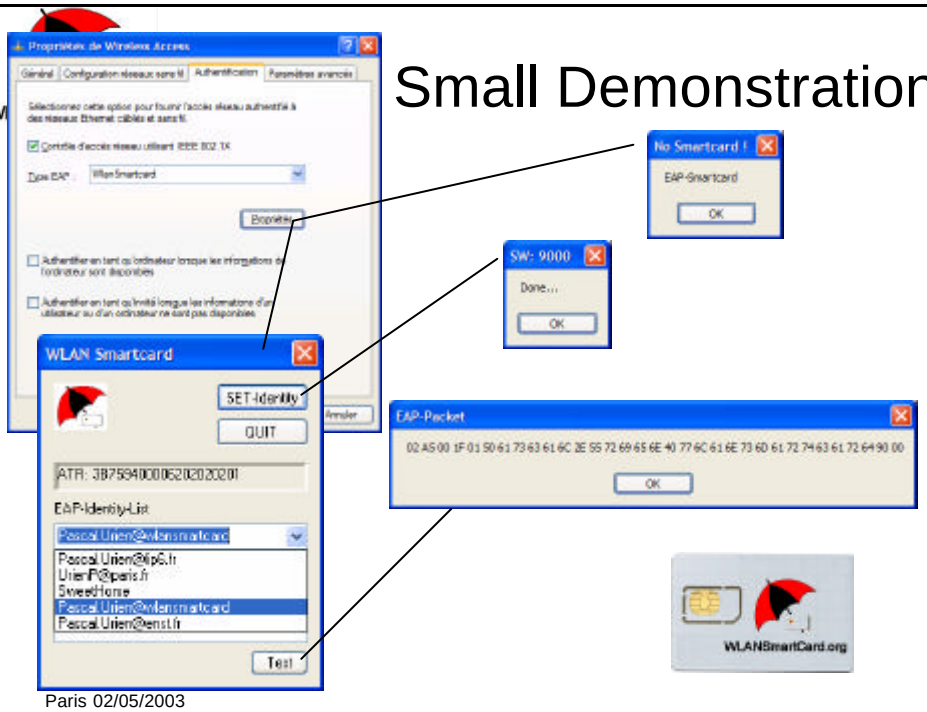
WLANSmartCard.org

New Services

- Wireless access to corporate networks (intranet) or to the internet.
- ***Access control*** is mandatory in many environments (who is using my network ?).
- ***Non repudiation*** (frame signature) is a pre-requisite for service ***billing***.
- ***Wireless user*** privacy is a plus. But it may be performed at application level.

Pascal Urien
Paris 02/05/2003

Small Demonstration



Paris 02/05/2003

802.11 Radio Link Security

Pascal Urien
Paris 02/05/2003

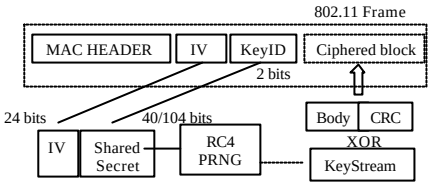
802.11 Radio Security

- 1st generation Wireless Equivalent Privacy (WEP), defined in 802.11 standard
- 2nd generation, 802.1x architecture (with WEP).
- 3nd generation, 802.1i, TKIP, hardware compatible with WEP
- 4nd generation, 802.1i + AES, hardware incompatible with WEP.

Pascal Urien
Paris 02/05/2003

WEP

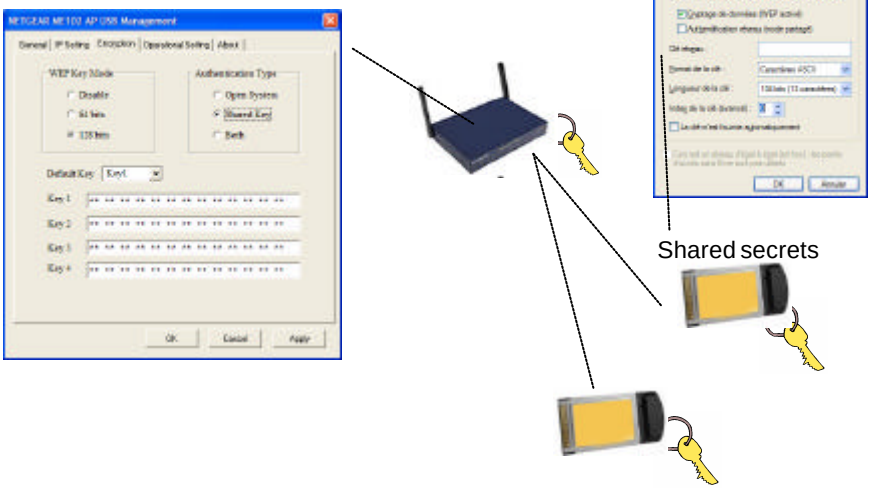
- Works with for four static shared secrets and RC4 keys (64/128 bits), not scalable
- **1G Many security threats**,
  - –Authentication, Data Integrity, Data Privacy.
- 2G - Periodic Authentication,
  - –Uses re-keying mechanisms (10,000 frames recommended, security limit at about one million frames….)



A WEP frame

Pascal Urien
Paris 02/05/2003

WEP 1G, Key Management, not scalable



Pascal Urien
Paris 02/05/2003

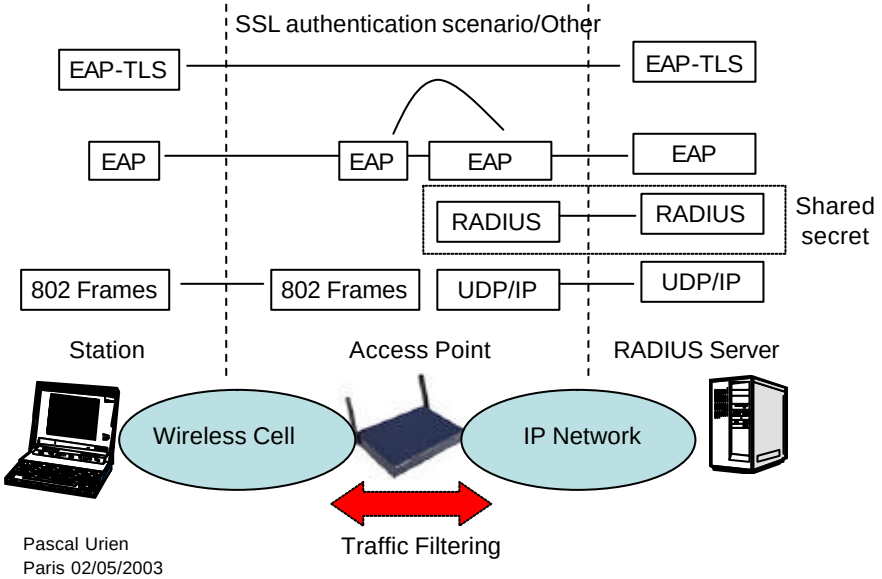
WLANSmartCard.org

IEEE 802.1x

Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

802.1x Stack



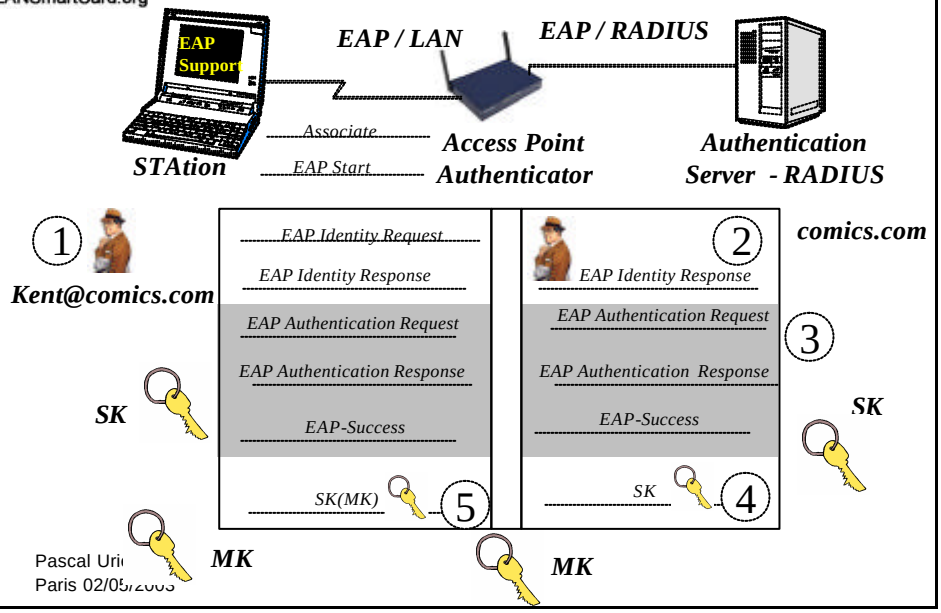
Pascal Urien
Paris 02/05/2003

802.1x Typical Use.

- *Port Based Network Access Protocol*
- Deals with EAP (RFC 2284) protocol and RADIUS (RFC 2058). It is a key distribution architecture.
- Station (STA) sends an 802.11 association request to the access point (AP).
- Station sends a 802.1x EAP-EOL start message to AP.
- (1) Access Point AP sends an identity request to the station
- (2) Station produces an identity response. AP forwards this message to the RADIUS Server (RS), of which address is deduced from the identity parameter.
- (3) A set of request and response messages are exchanged between RS and STA and forwarded by AP.
- At the end of the authentication scenario, RS delivers a success notification to STA. RS and STA share a session key SK.
- (4) RS sends SK to AP. AP chooses a master key MK, other WEP key or TKIP master key.
- (5) AP sends MK to STA, encrypted by the session key SK.

Pascal Urien
Paris 02/05/2003

802.1x architecture.



IEEE 802.1i - TKIP

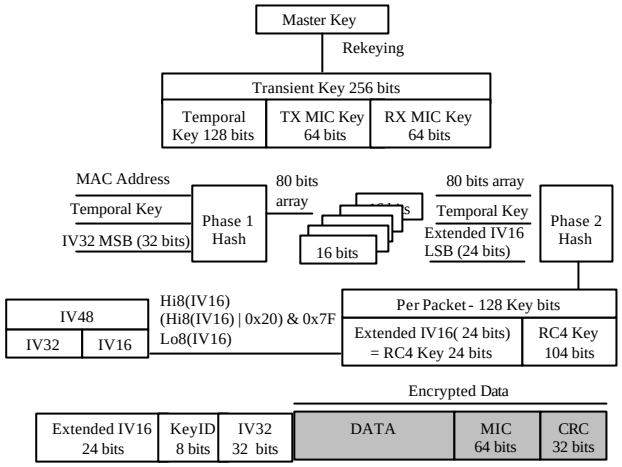
Pascal Urien
Paris 02/05/2003

802.1i TKIP

- New version of WEP, called TKIP, Temporal Key Integrity Protocol.
- Hardware compatible with WEP
  - Per Packet Key (RC4 128 bits).
  - Strong Packet Signature (Message Integrity Code).
  - Master Key Distributed via 802.1x
  - Ephemeris key (*Transient Key*), can be updated via a *re-keying process.*

Pascal Urien
Paris 02/05/2003

TKIP frame (not yet standardized)



Pascal Urien
Paris 02/05/2003

Extensible Authentication Protocol - EAP

Pascal Urien
Paris 02/05/2003

What is EAP ?

- An umbrella of authentication schemes shuttled by EAP packets.
- Defines user **Identity** concept, a Network Access Identifier.
- One authentication scheme (*Type field*) per authentication server,
  - *MD5 Challenge*, a digest is computed from a random value and a shared secret.
  - *PPP EAP TLS* a protocol based on SSL mechanisms.
  - *IAKERB*, adaptation of Kerberos V5 procedures.
  - *EAP SIM* , reuse of SIM smartcards (GSM 11.11).
  - *EAP AKA* , support of USIM smartcards (UMTS security modules).

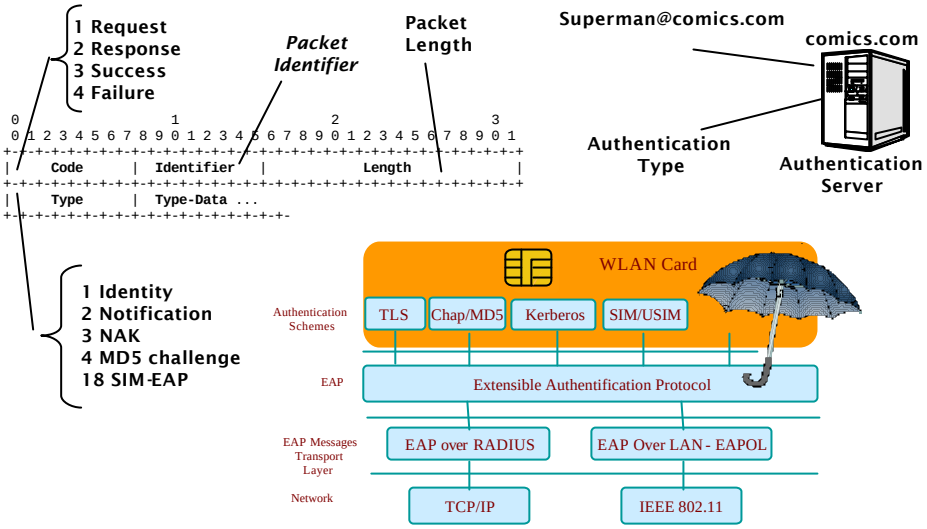
Pascal Urien
Paris 02/05/2003

Who is supporting EAP ?

- Normalization Committees.
  - IETF - RFC 2284.
  - IEEE - 802.1x.
  - Javacard forum
- Network Manufacturers
  - CISCO.
  - NOKIA.
- Operating System Manufacturers
  - Microsoft XP….

Pascal Urien
Paris 02/05/2003

EAP umbrella.



Pascal Urien
Paris 02/05/2003

GSM versus Wi-Fi

Attribute	GSM	WiFi
Network Identifier	Implicit	SSID
User Identifier	IMSI. Operator dependant	NAI. One per WiFi.
Authentication Methods	A3,A8 plus Ki Key	MD5, TLS, Kerberos, Other.

Network Access Identifier - NAI - rfc 2486

superman@comics.com

login

Authentication (radius) server

Authentication Scheme

- *Microsoft*
- *PKI*
- *GSM operators*

Pascal Urien
Paris 02/05/2003

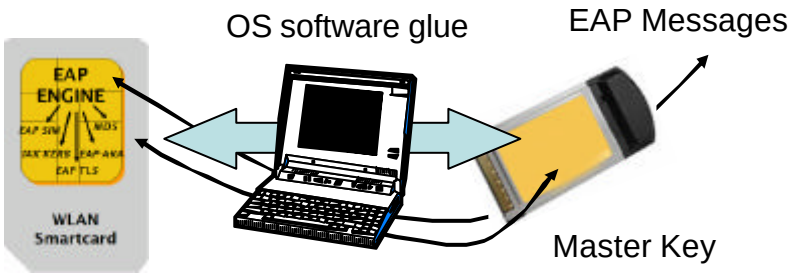
WLANSmartCard.org

OS Glue

Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

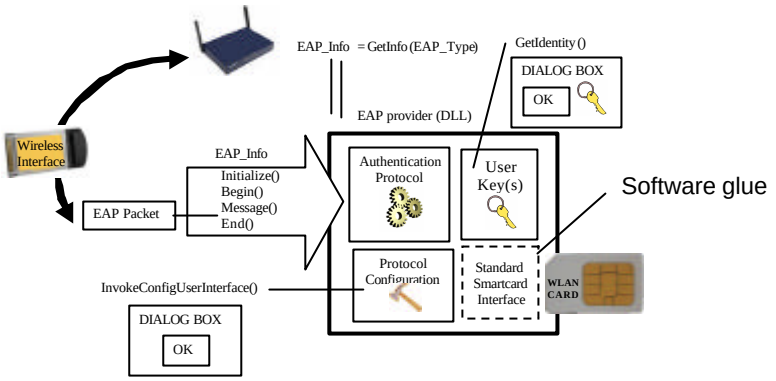
Operating Software Glue.



Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

XP EAP Operations.



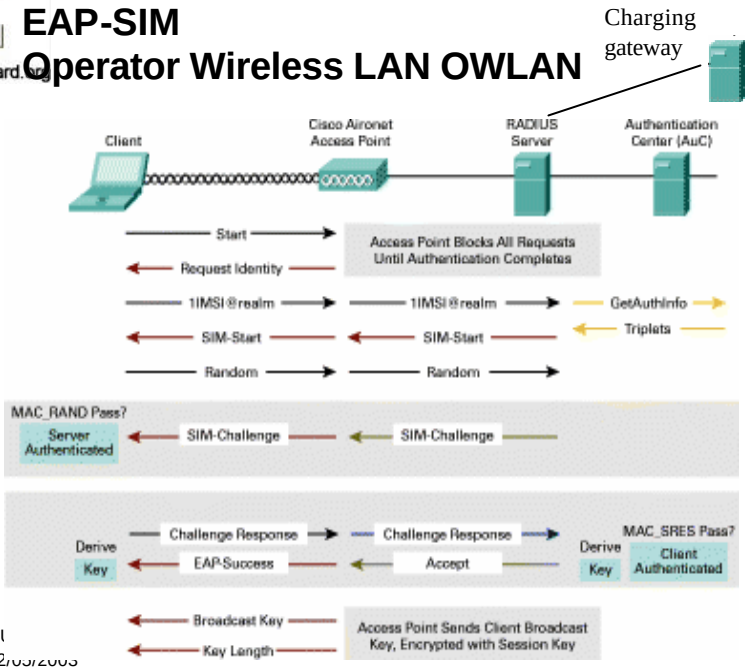
Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

Use cases

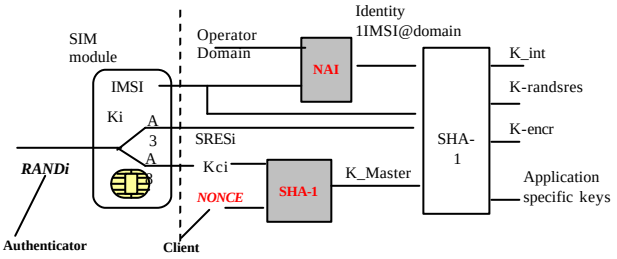
Pascal Urien
Paris 02/05/2003

EAP-SIM
Operator Wireless LAN OWLAN



Pascal U
Paris 02/05/2003

Example1, EAP-SIM, Mobile.



Set-Identity(1IMSI@domain)

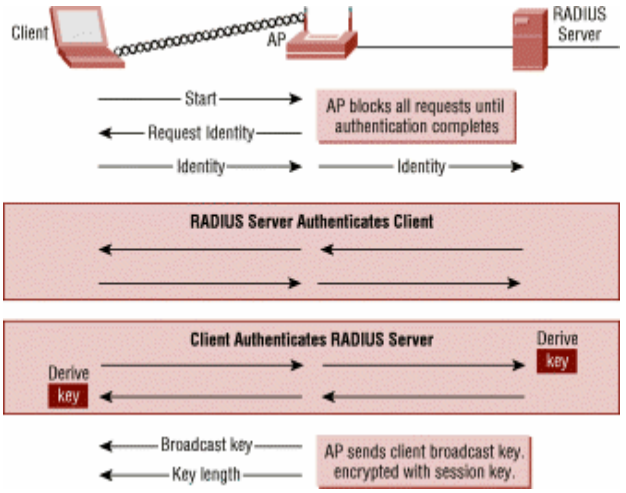
EAP-Packet()

EAP_TYPE = EAP-SIM

Pascal Urien
Paris 02/05/2003

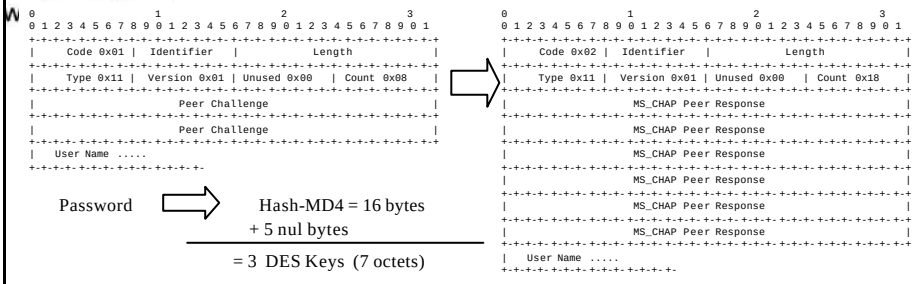
WLANSmartCard.org

LEAP - NT like authentication. Dedicated to MS platforms.



Pascal Urien
Paris 02/05/2003

Example 2, LEAP, MS.



Password ⇨ Hash-MD4 = 16 bytes
+ 5 nul bytes
= 3 DES Keys (7 octets)

Response = 24 bytes $=(Des_1,Des_2,Des_3)(challenge_{8\ octets})$

Set-Identity(MyUserName)

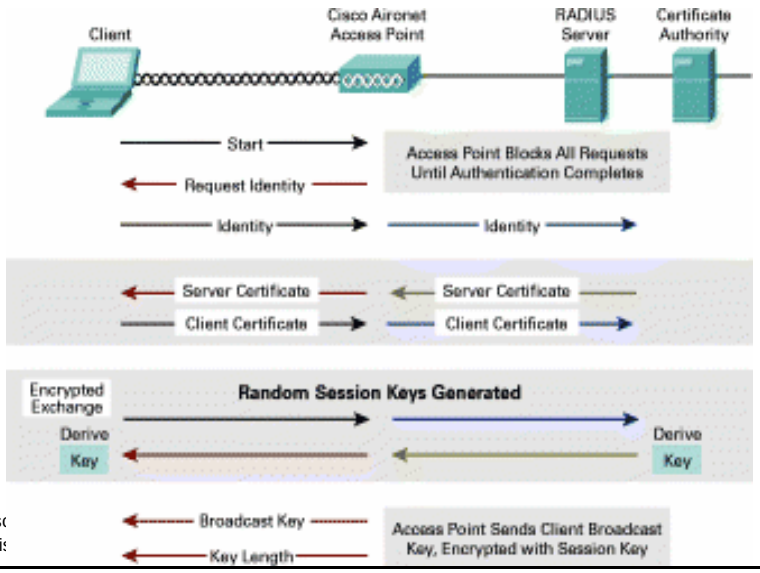
EAP-Packet()

EAP_TYPE = LEAP

Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

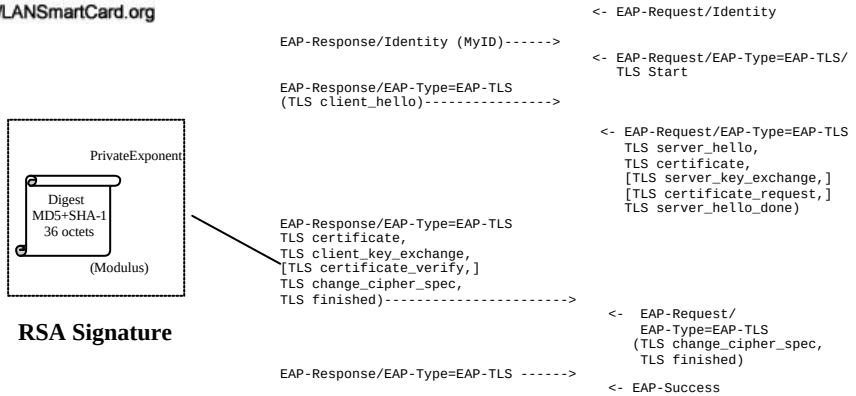
EAP-TLS, PKI Architecture Supported by MS platforms.



Pasc
Paris

WLANSmartCard.org

Example 3, EAP TLS, PKI.



RSA Signature

Set-Identity(MyUserName)

EAP-Packet()

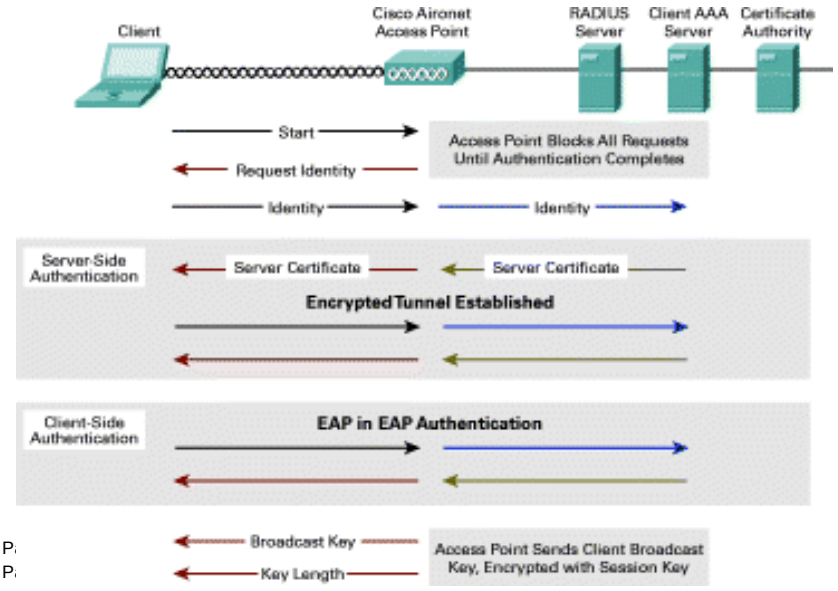
WLAN Card

EAP_TYPE = EAP-TLS

Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

Protected EAP - PEAP



P
P

WLANSmartCard.org

Normalization initiative.

Pascal Urien
Paris 02/05/2003

WLANSmartCard.org

55th IETF
Atlanta, GA, November 17-21, 2002

“EAP support in smartcards”

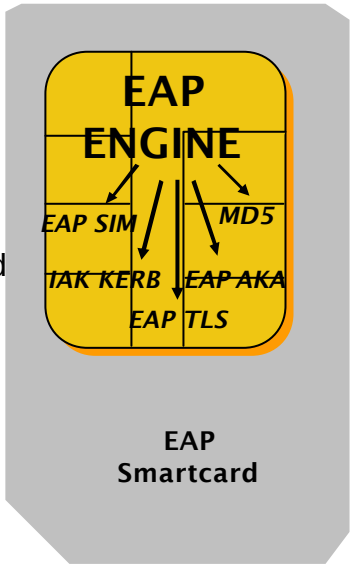
Draft-urien-EAP-smartcard-00.txt

Pascal Urien
Paris 02/05/2003

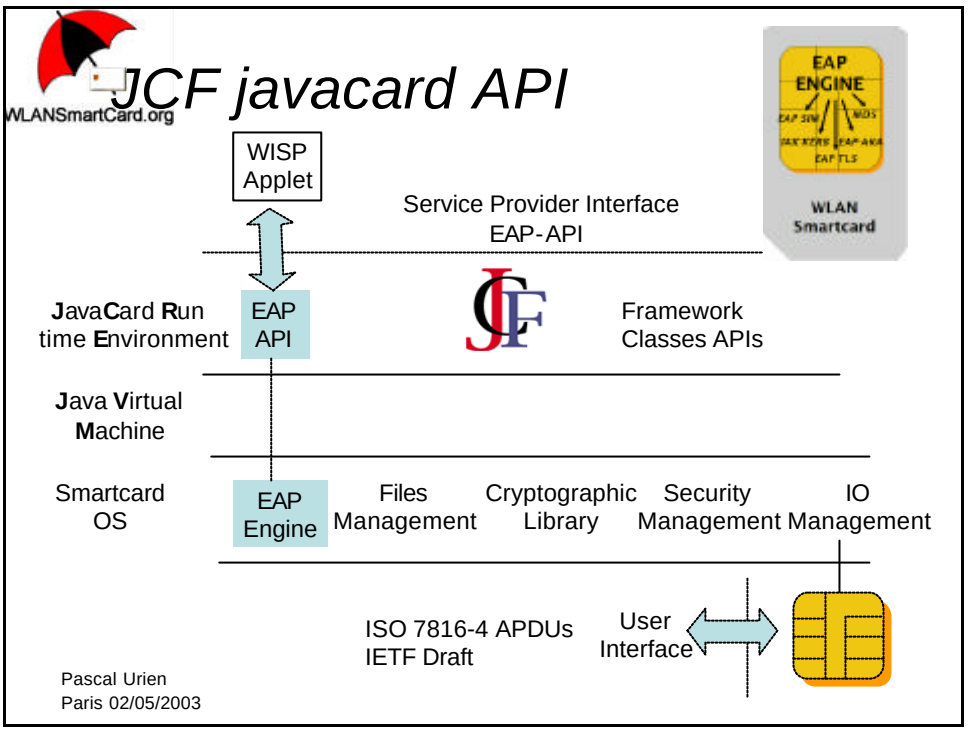
WLANSmartCard.org

Draft Objectives.

- EAP support in smartcards.
  - EAP is computed in smartcard.
  - Profiles definition, for some EAP types (EAP-SIM, EAP-TLS, …)
- Interoperability between ISO 7816 EAP smartcards.
- Agreement between major smartcard manufacturers.
- Four service primitives.
  - Get-Next-identity()
  - Set-Identity()
  - EAP-Packet()
  - Get-RSN-Master-Key()



Pascal Urien
Paris 02/05/2003


WLANSmartCard.org
JCF javacard API
EAP ENGINE
WLAN Smartcard
WISP Applet
Service Provider Interface
EAP-API
JavaCard Run time Environment
EAP API
Framework Classes APIs
Java Virtual Machine
Smartcard OS
EAP Engine
Files Management
Cryptographic Library
Security Management
IO Management
ISO 7816-4 APDUs
IETF Draft
User Interface
Pascal Urien
Paris 02/05/2003