



# Challenges of Introducing Trusted Computing to Existing Applications Domains

Gemalto – Gerald Maunier

June 2008



## Smart card & smart token compared to TPM





# Smart cards compared to TPMs

- ✦ Smart Cards are programmable open platforms
  - OS: Javacard 2 and 3, Microsoft .NET
  - ➔ TPMs have a fixed firmware
  
- ✦ Smart cards host multiple applications, linked to users
  - Citizen card, GSM authentication, payment, transportation, physical access control... "TPM"?
  - ➔ TPMs are linked to platforms
  
- ✦ Smart cards are portable devices
  - ➔ TPM MUST be physically attached to platforms



# Smart tokens

- ✦ 2 devices in 1
  - Driverless reader
  - Embedded Smart Card
  
- ✦ 3 ...
  - Encrypted Flash memory to store sensitive information
  - Companion software / portable apps to be executed on the host
  - Mobile secure desktop (virtualization, data leakage protection)
  
- ✦ 4+ ...
  - Equipped with LEDs, buttons and display, e.g. for unconnected OTP generation
  - MoC and even a Biometric sensor...
  
- ➔ Smart tokens are portable security devices, with all required security applications, user sensitive data, user credentials...
- ➔ Booting from a “trusted” device or launching a portable remote terminal application are forms of TC!

# Using Smart cards and TPMs in parallel: VPN access use case

# VPN connection

- ✦ Everyone is concerned about user authentication (password, smart card, OTP,...)
- ✦ But
  - Some secrets can be compromised
  - A valid user can connect from a compromised platform
- ✦ A comprehensive VPN security policy must also include a second level of authentication that ensures that only identified and trusted platforms can access the network

# VPN connection elements

User credentials

- Certificate
- Signature key



Platform credentials

- AIK



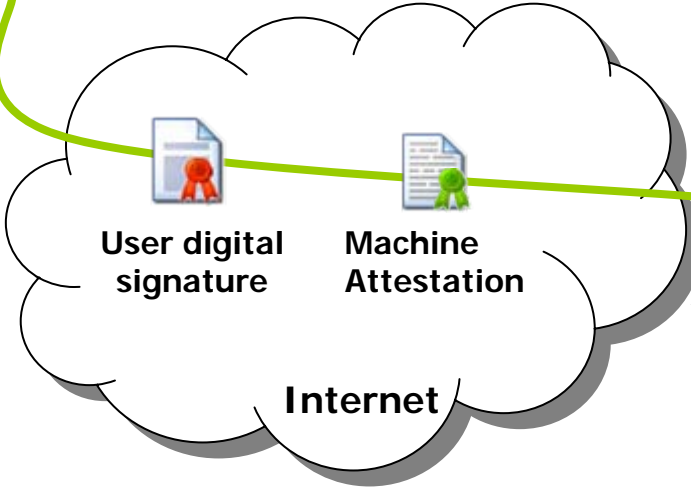
PIN

Passphrase



User credentials

- Smart Card PIN
- TPM AIK passphrase



Authenticator

Privacy CA Attestation Server



AuthN Server

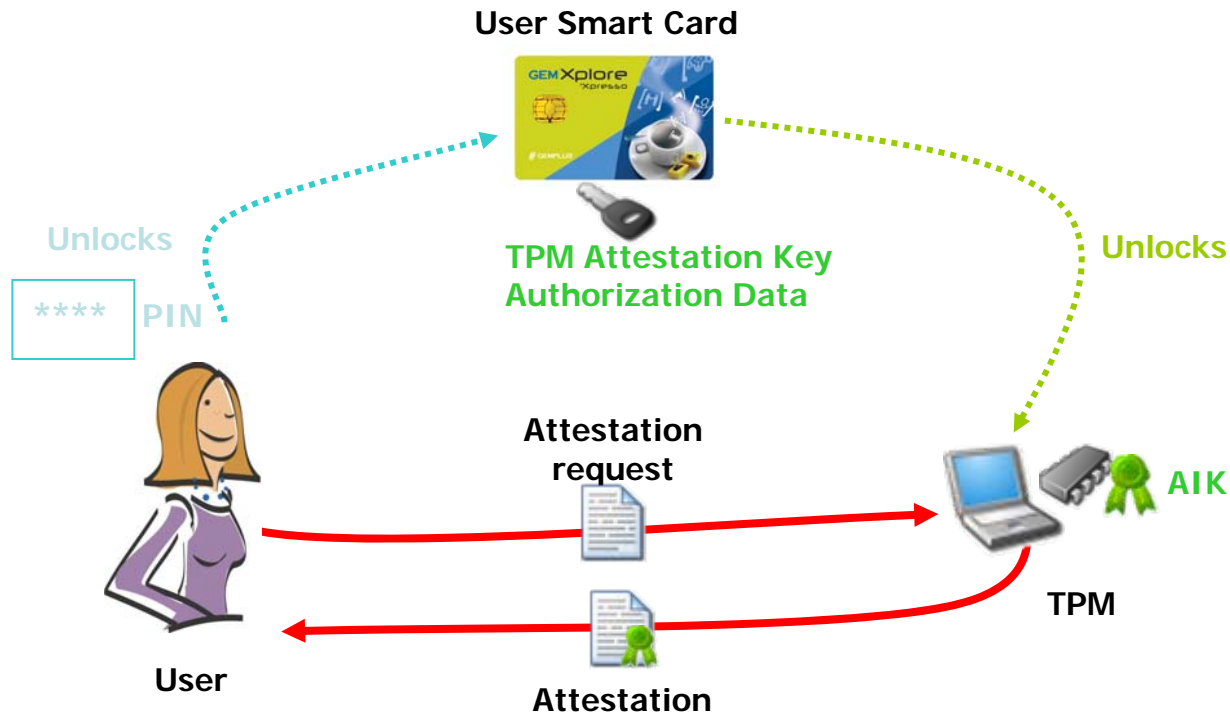
# Mixing Smart cards and TPMs: advance scenarios

# 1-Smart card usage to unlock TPM keys

- ✦ TPM objects are strongly protected by a 20 bytes passphrase
- ✦ But users cannot handle this kind of secrets, so implementations rely on regular passwords, hashed to produce the required 20 bytes
- ✦ This has been understood and addressed by 2 different initiatives:
  - TCG AWG: using existing TPM features to increase TPM protection with SC and biometrics
  - TPM.Next General Authorization: proposal to implement new authentication mechanisms in the TPM itself

# 1-Smart card usage to unlock TPM keys

- ★ Authentication Work Group defines standardized mechanisms to allow Authentication Sources to authorize TPM actions



- AWG Considered Authentication Sources are Smart Cards and Biometric devices
- This could apply to FDE keys stored in the TPM

## 2-Local trust verification



- ★ Main problem: we cannot trust a platform to attest its state/identity to its user
- ➔ A TPM equipped Platform can only attest its state/identity to a remote server via cryptographic operations
  
- ★ TCG TNC defines how a remote server can check if my computer is trusted and grant/forbid access
- ★ BUT many secrets may have already been compromised !
  - BIOS boot passphrase,
  - FDE passphrase,
  - OS login/password,
  - Business Mail password,
  - VPN access passphrase,
  - Personal web sites credentials,
  - And even Smart Card pin code, with possible usage of all PIN protected keys.
  - ...
- ➔ For a corporation, ensuring trust only when a remote connection occurs is certainly not enough!

## 2-Local trust verification using Smart Cards

- ✦ A problem of “trust”: In a cyber café, you know it’s not secure and you can evaluate risks, but if you “think” you’re on a trusted system ... you do not have this evaluation possibility!
- ✦ Smart Cards are capable to check local computer trustworthiness (TNC server role) and protect themselves accordingly
- ✦ Using a smart token
  - Attached applications like password wallet can take benefit from embedded smart card verification: can be unlocked with smart card pin when a trusted host is detected, but require e.g. additional biometric authentication when the host is not trusted
  - User can be informed about host trust level and educated to act as appropriate



## 2-Local trust verification using Smart Cards in a Mobile Telecom environment

- ✦ In the handset ecosystem, trust was not strongly required
  - Few services
  - Model diversity = difficult to implement large scale attacks
  - ➔ few interests for attackers,
- ✦ ME becomes connected and manipulates data
  - Mobile internet, mobile TV, mobile payment
  - ➔ Need for trust anchor increases
- ✦ Existing Security Chipsets (IMSI protection/SIM lock) and TPMs have a role to play, but telecom infrastructure changes are costly
  - ➔ SC can act as a Proxy for telecom operator and check platform integrity before releasing secrets (Network keys, mobile TV decryption keys,...).
  - Existing Other The Air infrastructure can be used to transfer allowed manufacturers certificates and possibly known valid configurations measures into the SIM card
  - SIM card can check unknown configurations out of band and keep last known valid configuration

# 3-Using Smart Cards to ease TPM provisioning

- ★ Challenge of TPM deployment also resides in its deployment phase
  - Taking Ownership
  - Provisioning initial configuration
    - URK,
    - corporate specific keys,
    - AIKs...
  
- ★ Smart Cards can be used to ease this initial phase, but also facilitate operations during all TPM life cycle
  - When stored in the Smart Card, Owner passphrase can be used by the user without disclosure
  - Smart Card can check which operation involves this secret

# 3-Using Smart Cards to ease TPM provisioning

- Smart Cards can be used to delegate owner right for specific operations like AIK generation after platform leaved owner control

