gemalto
security to be free

Common Security Schemes for UICC

PSCR 2010 Winter Conference

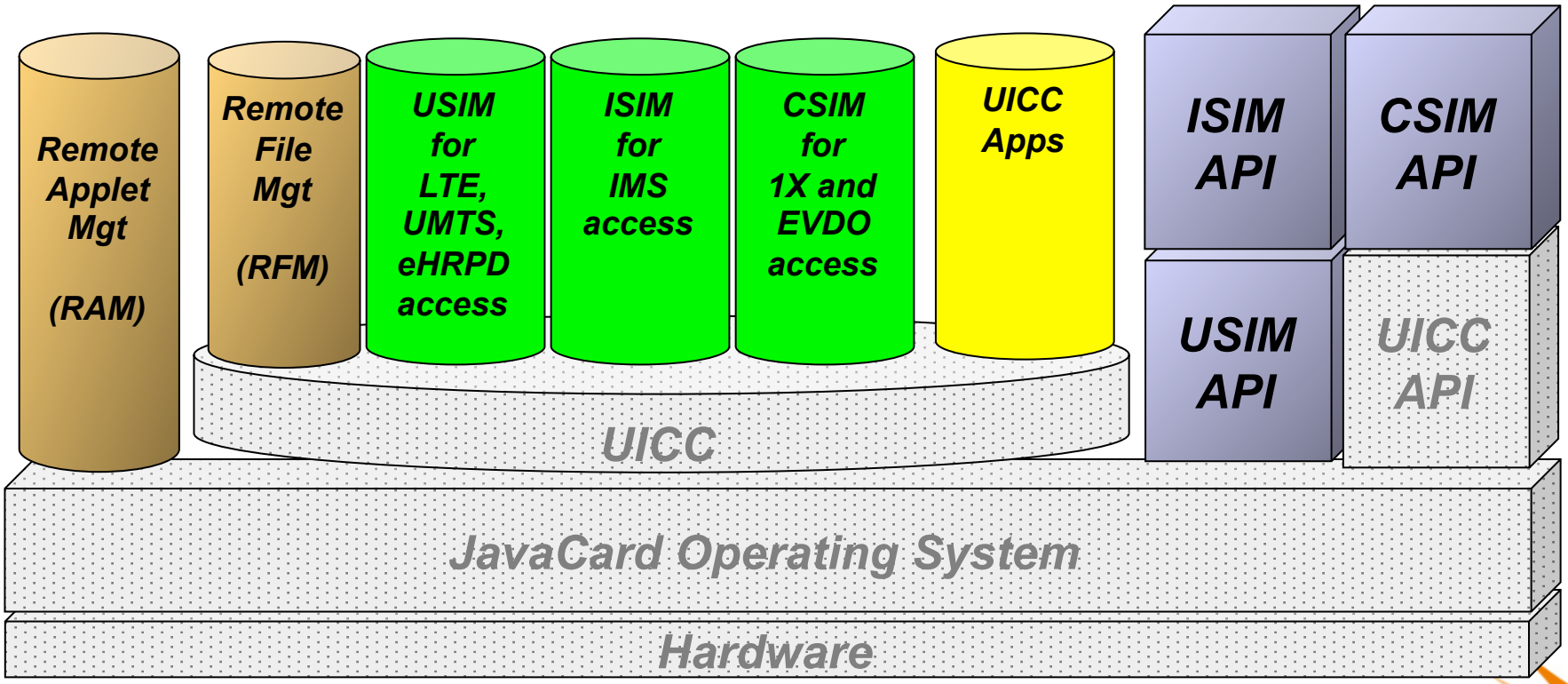
Leader in Digital Security

- Making our transition to digital lives more convenient and secure
  - Public corporation, 10,000 employees worldwide
  - B2B provider of smart cards, secure software and services to over 400 wireless operators, 2,000 banks, corporations, and governments
- Leading provider of SIM/UICC and associated OTA
  - Only GSMA SAS-certified manufacturing and personalization center in the USA
  - Customers include Verizon, AT&T, TMO, Sprint Nextel, MetroPCS, Tracfone
  - The most experienced smart card company in LTE with solutions designed for all-IP environments

UICCs are implemented according to wireless service provider specifications

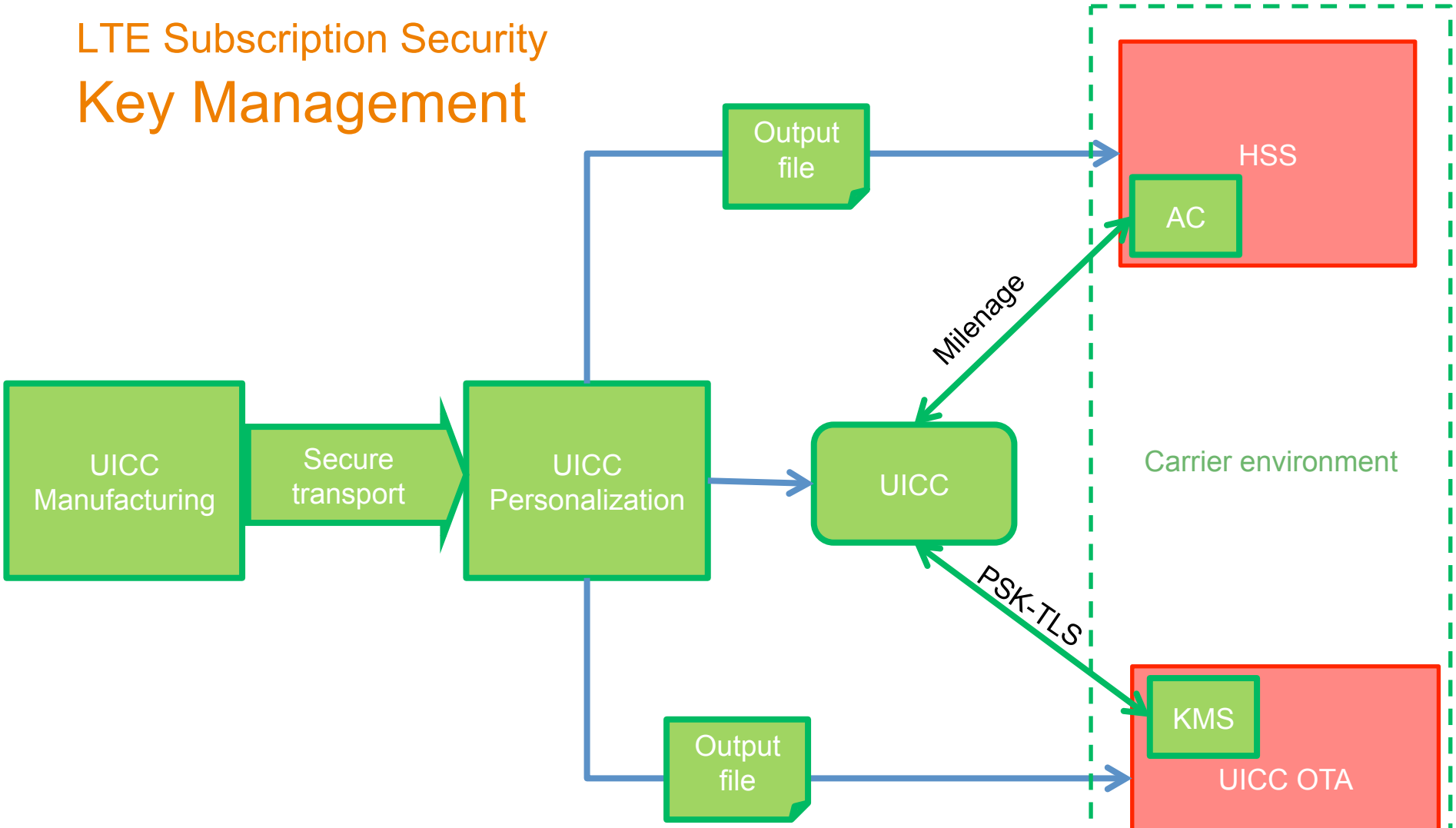
- **Subscriber Identity**
- **Location Information**
- **Roaming Preferences**
- **Network Authentication**
- **Security Mechanism**
- **OTA Remote Management**
- **Personal Data**
- **Applications & Services**

UICC Platform



LTE Subscription Security

Key Management

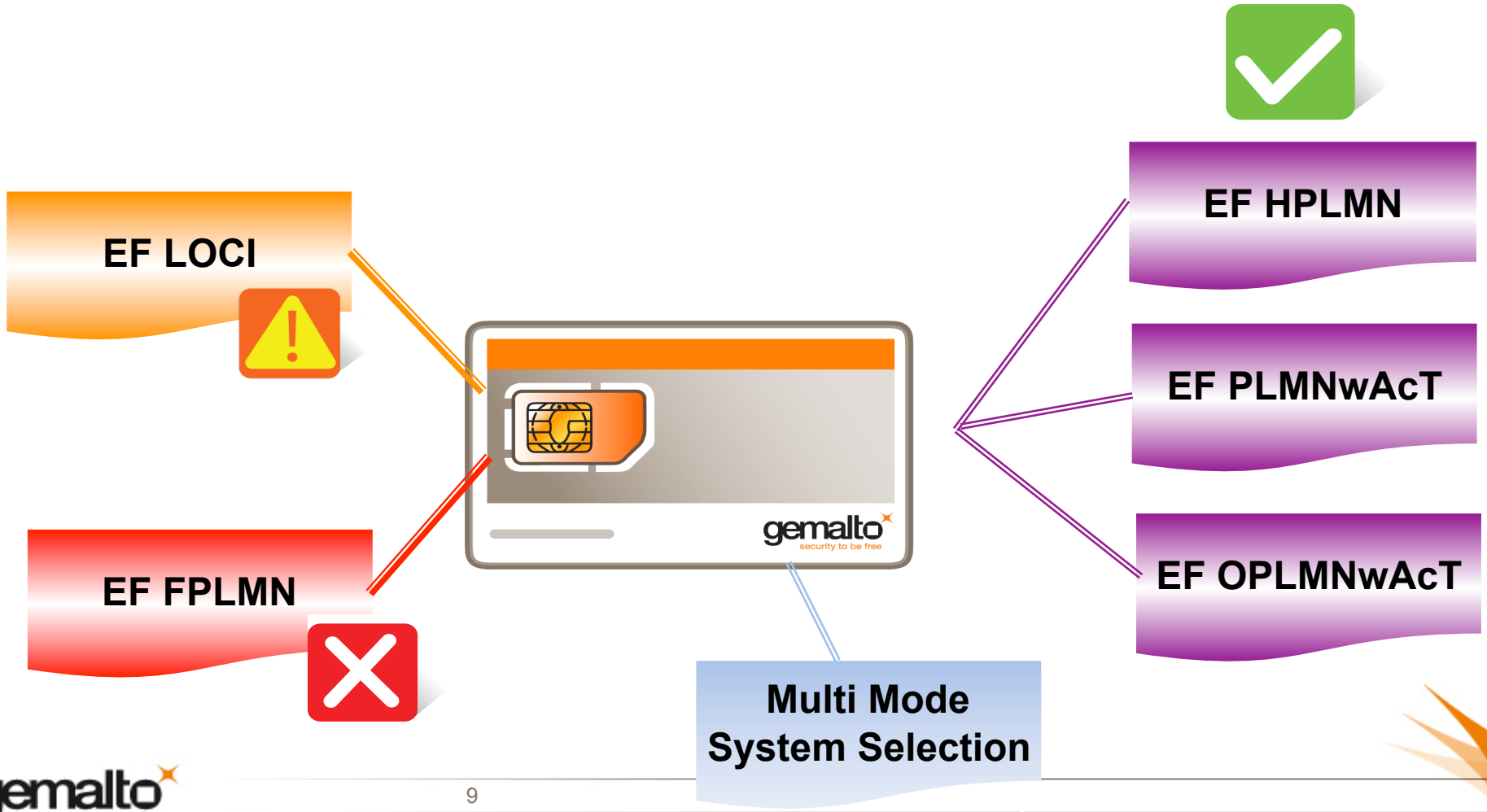


ETSI/3GPP: Secrets and Security Mechanisms

- Device authentication
  - Mutual authentication between UICC and Home network (Milenage)
  - Generate a session key Ks used by device for voice and data encryption to the base-station
- OTA security
  - Mutual authentication between UICC and OTA platform (PSK-TLS)
  - Local access policy enforced by UICC
- Local user authentication
  - 4-digits PIN, usually deactivated in the US
    - 3 attempts before locked
  - 8-digits PUK to unlock the PIN
    - 10 attempts before locked
    - No unlock

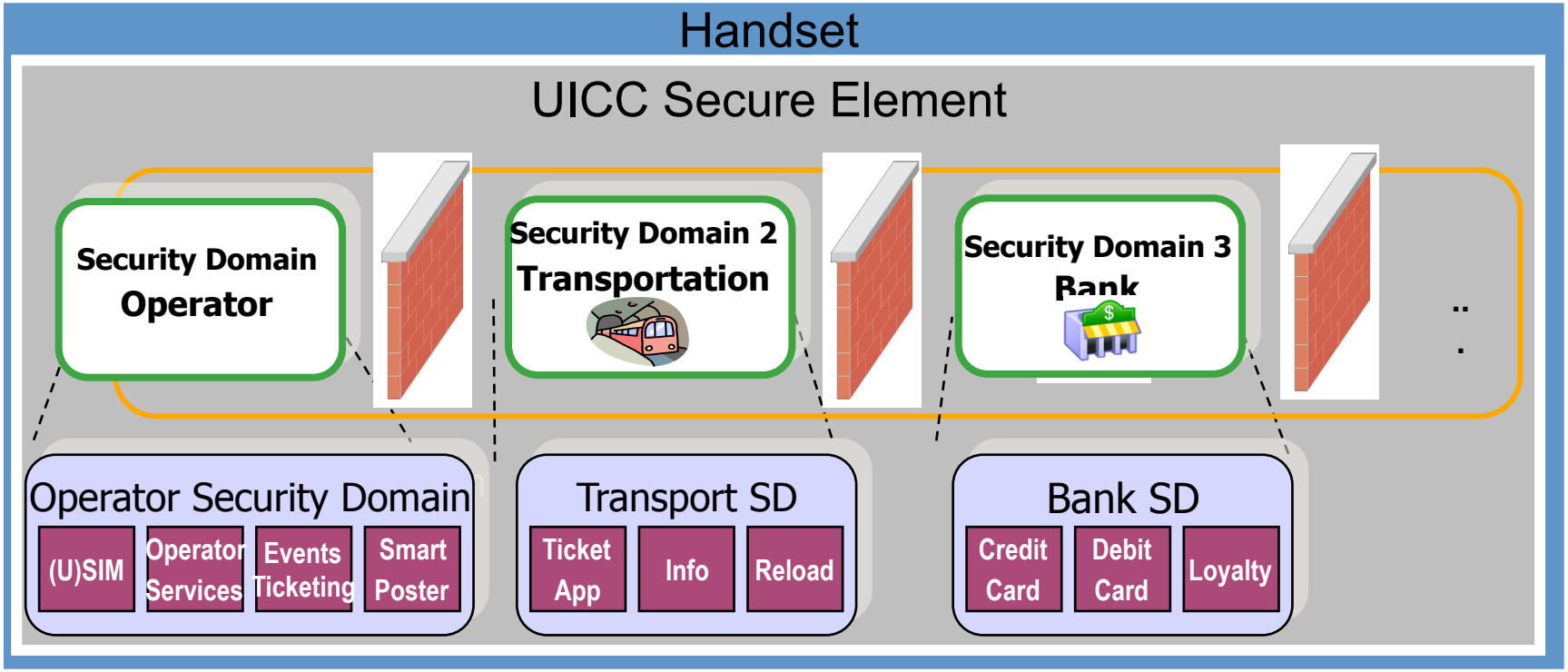
Role of the USIM in Roaming

- Devices retrieve network selection parameters from the USIM



LTE Subscription Security

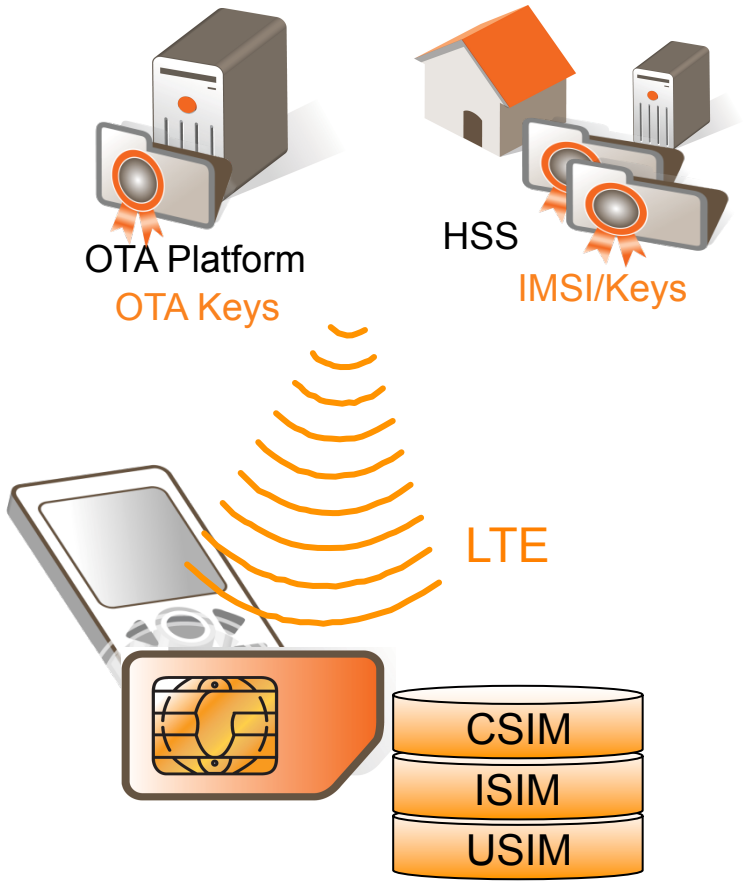
Global Platform: Multi-application environment



- Clear independence between applications running on the secure element
- A standard created by the payment community

OTA

- UICC credentials and keys are pre-provisioned during card manufacturing
- IMSI/Keys are uploaded to HSS
- LTE use cases
  - ISIM IMPU has to be provisioned
  - CSIM parameters
  - Profile parameter updates (incl. roaming files)



Application Execution Environment

- JavaCard development environment
- Card Application Toolkit, a set of standard services on the device that allow UICC applications to:
  - Send & receive SMS, send data, display text & menu, play tone, place a call, detect & intercept a call, set timer, …
- Smart Card Web Server, an HTML server in the card to:
  - Provide a graphical interface for user to access information
  - Provide offline information through the device browser
- Examples of UICC applications:
  - Device tracking, Enhanced roaming, Digital signature, Call monitoring, Lock-to-device, Dual-IMSI, Secure SMS, Call routing
  - UICC applications can be downloaded only using the wireless service provider OTA keys

Commercial devices are not secure

- Attack vectors
  - P2P connectivity: Bluetooth and infrared
  - Synchronization with PC
  - Data services: MMS, SMS, WAP
  - Wifi
  - Physical media
- Types of attack
  - Battery drain
  - Denial of service
  - Stealing of information and location
  - Hijacking
- Attack Examples
  - Cabir (2004 / Symbian / Bluetooth)
  - CommWarrior (2006 / Symbian / SD / Bluetooth)
  - WINCE_INFOJACK (2008)
  - BlueSnarfing
  - Rootkit

15 out of 30 popular free Android Market applications sent users' private information to remote advertising servers, without the users being aware of what was being sent or to whom.
(appanalysis.org)

Considerations for Public Safety

- Basic “generic” LTE UICC profiles
  - USIM, ISIM, Milenage-based,, standard roaming based on USIM files
  - OTA/HTTP for ISIM provisioning and profile updates
  - PIN enablement
  - For dual mode LTE/CDMA
    - CSIM and Multi Mode System Selection
    - CSIM OTA provisioning
- Possible future enhancements
  - Enhanced user authentication preventing PIN capture on host devices
  - Generic Bootstrap Architecture, WiFi authentication
  - Roaming director to modify roaming files based on location
  - Secure communications
  - Secure applications

gemalto
security to be free

Questions?

Contact us at
lionel.merrien@gemalto.com
jean-louis.carrara@gemalto.com