Security Modules for Professional Mobile Radio

Frederic.Rousseau@eads.com

2nd ETSI Security Workshop : Future Security
16-17 January 2007 – Sophia Antipolis, France
Outline

• Professional Mobile Radio

• Security modules for narrowband & wideband flows

• Trade-offs and synergies

• Future security over heterogeneous networks
Professional Mobile Radio:
Secure communications for public safety & security forces
Several families of security services implemented in PMR networks in accordance to operational users’ needs

- Air interface protection: local to each radio cell
- Network infrastructure security
- End-to-end communications security between end-users’ applications
- Management of security features for each subscriber (services such as automatic key distribution over the air; remote disabling & crypto zeroize)

Security services supported by a Key Management Infrastructure (KMI) associated with Subscriber Management, usually performed efficiently for up to several hundreds thousands subscribers
Within the INFOSEC boundary of a communication equipment, a security module is the set of hardware, software, and/or firmware that implements security functions and is contained within an explicitly defined continuous perimeter (ISO/IEC 19790).

Different packages and interfaces can be considered for a security module:

- **Removable Module with specific interface & mechanical embodiment**
- **Board-mounted single-chip module with specific pin-out**
- **PKCS-11 PCI-interface packaged module**
- **Chip module in any ISO-7816 packages or SD card package**
Services from Security Modules

Services expected from a security module

- Secure storage capabilities; Hardware random generator
- On-board cryptographic processor for encryption, authentication and integrity management
- Several security protocol implementations; trusted bootstrap & mutual authentication with baseband modem chip
- Key wrapping/unwrapping; security zeroize

Additional features when the security module is plugged into a mobile communicator

- Small size tamper-proof hardware security module
- Low-power consumption

Other characteristics that may be needed

- Sufficiently high throughput capabilities at interface
- High processing power and high internal clocking rate
- Multiple physical interfaces for flow separation
- Multiple simultaneous cryptographic contexts
- All security related services fully performed within the boundary of the security module
- Mechanical properties of the package for professional use
Professional Mobile Radio:
End-to-End Security over Narrowband communications channels

Performance requirement on security modules:

Handle “approx. 100 to 300 bit” stream
to encrypt in less than “typically 2 to 3 ms”
every “typically 20 to 60 ms” temporal occurrence
+ decrypt parallel duplex stream
+ perform some authentication & integrity operations
+ key wrapping/unwrapping & some security protocols
Lesson learned from the past decade: Security Modules for Narrowband PMR

• More than half a million Security Modules produced in Europe in the past decade for PMR applications, with cryptographic suites usable for end-to-end security

=> Most of them as single-chip ASIC modules or specific small removable module packages providing full security services on-board

• Progressive emergence of Security Modules as standardized for TETRA narrowband end-to-end encryption, based on smart cards with ISO/IEC 7816-3 interface (ETSI EN 300 812)

Smart cards may be suitable for PMR narrowband needs

BUT service & architecture limitations due to ISO 7816-3 low speed

=> Low-speed smart card contribution to confidentiality service is only as a Key Stream Generator

(This has impact on the definition of the INFOSEC boundary during a security evaluation of the terminal platform)
Professional Mobile Radio:
End-to-end Security over Wideband/Broadband channels

Performance requirement on security module:
from 50 kbit/s to several Mbit/s IPSec encryption per user, depending on the technology

ANSI/TIA-902 IOTA
www.tiaonline.org

ETSI EN 300 392
www.tetramou.com

TEDS TETRA Enhanced Data Service

MESA
www.projectmesa.org
Universal Integrated Circuit Card (UICC) – Terminal interface

**Could Wideband/Broadband PMR security services & PMR subscriber identity be applications of a high speed UICC smart card as defined by 3GPP & ETSI Project SCP?**

**Pro:** UICC as the extension of existing PMR smart cards
- UICC USB electrical/protocol interface to terminals defined by ETSI SCP is suitable to host platform performance requirements, overcoming limitations experienced with previous security architecture considering ISO/IEC 7816-3 low speed constraint

**Cons:** UICC issues compared to PMR-specific packaged IC
- Multiple parallel cryptographic contexts (however, this does not depends on interface but on IC)
- Multiple physical interfaces for flow separation (however, this does not depends on UICC specs)
- Mechanical properties of the package for professional use
- Efficient programmability & re-programmability to diverse cryptographic algorithms
- Availability of UICC-USB interface drivers in PMR baseband chips
UICC synergies with PMR security modules (2/2)

Universal Integrated Circuit Card (UICC) – Terminal interface

Could Wideband/broadband PMR security services & PMR subscriber identity be applications of a high speed UICC smart card as defined by 3GPP & ETSI Project SCP?

⇒ UICC USB interface is an interesting basis for a standardized high speed interface for security modules

⇒ ISO 7816 packages and related Integrated Circuits targeting 3GPP public cellular UICCs might not meet the diversity of communication security requirements from public safety and security users communities
Additional requirements for security modules to consider in the near future

- Removable security module with sizeable shape and robust interface mechanics to support 3 insertions/extractions per day (shift work for professional users)

- Typical cryptographic requirement for high-end Public Safety & Governmental communication security, as needed for PMR
  - On-board AES hardware encryption supporting ECB, CBC, CFB, OFB, CTR, GCM standard modes of crypto operations
  + PMR-specific modes of crypto operations (e.g. TETRA E1, E2, E3, E4)
  - On-board memory for programmable cryptography beyond AES, with sufficient cryptographic performance for custom crypto
  - All modes of crypto operations fully internal to the security module with several Mbit/s throughput
  - HMAC, SHA-1 & SHA-2 hardware encryption
  - AES-based key wrapping/unwrapping service
  - ECC cryptography, Elliptic Curve key agreement protocols & signatures
Future Security: Towards a Personal Security Module for end-to-end security interoperability over heterogeneous networks

Personal Security Module

Usable for Portable Identity Management and Security over heterogeneous networks and transparent to end-users

- with a standardized interface to plug diverse baseband modems related to diverse access networks
- with on-board security negotiation protocol to select cryptographic suites & security parameter
- reaching end-to-end security interoperability between end-equipments over heterogeneous networks

Such security module with subscriber data and end-to-end security operations co-localized and fully managed together would be an improvement to some current concepts being standardized.
Model for secure communication interoperability: End-to-end security among security modules over heterogeneous interconnected networks

- Secure automated remote downloading of cryptographic data to security modules
- Accountability and tracking of security modules

Model applicable to the remote management of security modules located in terminals for Public Safety & Governmental secure communications
CONCLUSION for professional users
including public safety and security forces

Need for Future Standardization of
- a high-speed interface for removable security modules suitable for professional users’ secure communications requirements (potentially derived from UICC interface)
- a security negotiation protocol for end-to-end security interoperability among security modules operating over heterogeneous communication networks

To probe further on Removable Security Modules for professional users in the following contexts:

www.etsi.org ETSI project SCP
www.etsi.org ETSI project TETRA WG6
EADS Secure Networks

For the Security of all

www.eads.com/pmr

© EADS 2007 – All rights reserved