

Security Aspects of Smart Cards vs. Embedded Security in Machine-to-Machine (M2M) Advanced Mobile Network Applications

Mike Meyerstein, meyersmv@btinternet.com

Mobisec 2009 Conference, Torino, Italy, June 4th, 2009



Agenda

- M2M Service Environment
- M2M Security Requirements
- Solutions for M2M Trusted Environment (TRE)
- Security Issues around Integrated TRE
- Security Issues around TRE on a UICC
 - UICC = standardized Smart Card platform for telecomms
- Security Issues around TRE on a Secure Multi-Media Card (SMC)
- TRE on a UICC: New Functions Required
- Summary and Conclusions



M2M Service Environment

- See 3GPP SA1's TR22.868 and SA3's draft TR33.812. ETSI TC M2M is also developing M2M scenarios.
- Terminals can have direct PLMN/Internet attachment
- Hard-to-reach locations (e.g. traffic cameras)
- Wide-area mobility (e.g. cargo containers, in-vehicle applications)
- Assignment of generic (unassigned) terminals to a network operator after sale or even after installation
- Change the service provider and/or network operator without visiting the terminals (e.g. smart metering)
- User motivated to tamper (e.g. smart metering)

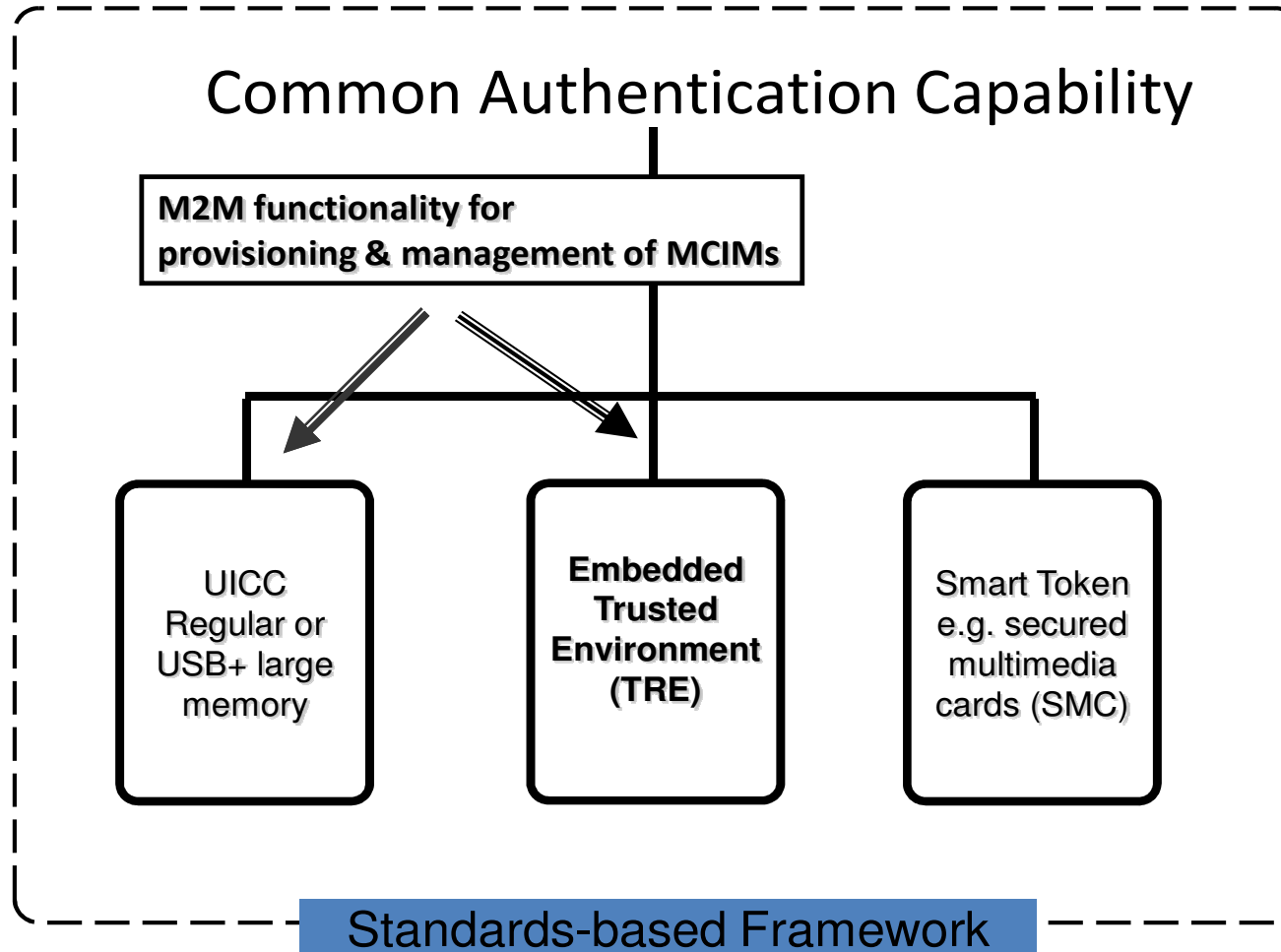


M2M Security Requirements

- M2M Equipment (M2ME) needs a trust anchor (TRE) for
 - Secure storage of credentials
 - Secure execution of crypto including authentication
 - Unique ID for authentication
 - Secure integrity-checking of device and reporting of results
 - Protocol end-point for on-line provisioning of credentials and applications (e.g. MCIM – Machine Communications Identity Module, i.e. M2M version of USIM)
- TRE must be
 - Highly tamper-resistant against local and on-line attacks
 - Strongly bound to the M2ME
 - Such that it can't be cloned
 - Physically robust, last a long life-time



Solutions for M2M Trusted Environment (TRE)





Security Issues Around Integrated TRE

- Pros
 - Non-removable. Bound to M2ME
 - No side-channel leakage
 - Minimum of exposed interfaces
 - Not restricted to limited UICC functions: can download authentication applications & credentials using on-line protocols; can use it to integrity-check the M2ME
- Cons
 - Relatively new and untried
 - Will need a certification scheme (can the vendors do that properly?)
 - Network Operators will need new infrastructure components



Security Issues Around TRE on a UICC

- Pros
 - Long track record of security in 3GPP networks
 - Standardized, available
 - Up to now a certification scheme has not been needed for 3GPP
 - Uses existing infrastructure
- Cons
 - Removable. Logical binding to M2ME is weak
 - History of previous attacks, including side-channel
 - Doubts over secure UICC-terminal interface
 - Limited functionality for M2M provisioning & mgmt
 - Some relevant UICC-related functions have been standardized but not yet widely implemented or utilized.



Security Issues Around TRE on a Secure MMC

- Pros
 - Uses existing UICC-based network infrastructure
- Cons
 - All the disadvantages of UICC, and also
 - No track record (very early in the technology life-cycle)
 - No protection profiles available
 - Questions concerning security of SMC interface
- Other issues:
 - Reliability, cost, size, standardization



TRE on a Smart Card: New Functions Required

- Download of AKA apps & credentials using protocols suitable for IP bearer
- Extraction of k/OTA keys from downloaded AKA app
- Validation of trusted apps on UICC and of functions in M2M Equipment
- New model for security domains, e.g. top domain not necessarily owned by a Network Operator
- Possible common criteria cert'n for UICC/TRE
- Large memory?, USB?, Smart Card Web Server?, costs?



Summary and Conclusions

- A UICC could host a fully-functional M2M TRE if properly enhanced and permanently attached
- UICC/TRE might need to be certified to a M2M protection profile
- An embedded TRE could be the answer for many applications where UICC is impractical
 - Flexible, on-line paradigm but limited track record so far
 - Implementation must resist all threats
 - Will need a certification scheme
- Both solutions can exist in the diverse M2M industry