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

Mike Meyerstein*, Inhyok Cha, and Yogendra Shah

InterDigital Communications Corporation LLC,
King of Prussia, PA, USA
meyersmv@btinternet.com,
{Inhyok.Cha,Yogendra.Shah}@InterDigital.com

Abstract. The Third Generation Partnership Project (3GPP) standardisation group currently discusses advanced applications of mobile networks such as Machine-to-Machine (M2M) communication. Several security issues arise in these contexts which warrant a fresh look at mobile networks' security foundations, resting on smart cards. This paper contributes a security/efficiency analysis to this discussion and highlights the role of trusted platform technology to approach these issues.

Keywords: Smart card, UICC, machine-to-machine communication, embedded security, trusted environment.

1 Introduction

The idea of M2M is that un-manned terminals, e.g. traffic cameras, meters, cargo containers, can communicate with host servers using wireless global communications networks. This requires the usual secure authentication for network access.

The networks will not be specially M2M-enabled, so the authentication has to follow the standardised schemes currently in place for mobile (e.g. 3GPP) and fixed (e.g. WLAN) networks.

M2M security requirements [1] may make the conventional UICC (Universal Integrated Circuit Card) a less advantageous solution for secure authentication. It is necessary to look at the options for a non-personalised security module to which a network operator's MCIMs (Machine Communications Identity Modules) can be downloaded [1]. This may be accomplished using an embedded Trusted Environment (TRE) in a terminal. The TRE acts as a hardware root of trust for the storage and execution of secure applications and may also have protected software functions. The TRE may host downloaded software MCIMs that emulate the behavior of the USIM (Universal Subscriber Identity Module) [2] or ISIM (Internet Multimedia Services Identity Module) [3] applications.

* Mike Meyerstein is the proprietor of Meyerstein Consulting Ltd, currently providing consultancy services to InterDigital Communications Corporation.

A.U. Schmidt and S. Lian (Eds.): MobiSec 2009, LNICST 17, pp. 214 – 225, 2009.

2 M2M Requirements

The M2M market has some definitive characteristics [1]:

- Terminals may be in hard-to-reach locations (e.g. traffic cameras)
- Terminals may become geographically dispersed over time (e.g. cargo containers)
- Owners of large populations of terminals may want to change the network operator without visiting the terminals (e.g. to change the UICC).
- Terminals need to be protected against unauthorised removal of UICC
- Terminals may require over-network provisioning after sale or installation.

3 The Options for a TRE to Host Secure, Downloadable MCIMs

Client-side technologies for TREs could include

- UICC with download capability.
- An embedded TRE in the terminal, to provide a secure execution and storage environment. MCIMs would be downloaded to the TRE over public IP networks.
- Smart token such as the new multimedia card with on-card UICC (or "SMC" – Secure Multimedia memory Card)

A framework of standardised specifications is needed for the above solutions.

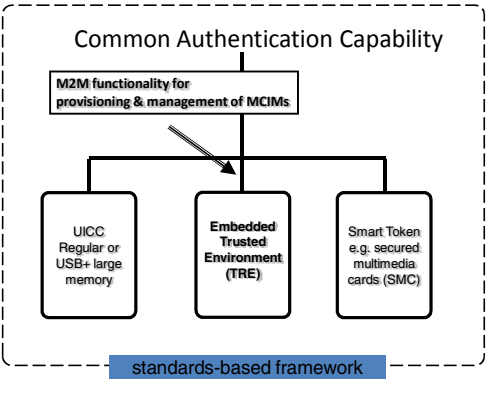

Fig. 1. Options for TRE to Host Downloaded MCIMs

The discussion within standardisation about the (dis-)advantages of the various candidate solutions is lively and far from concluded.

In Table 1 on the next page we collect the main arguments that have been advanced thus far in various forums and standardization committees (there is no reference document in which this information can be found).