EUROSMART
The Voice of the Smart Security Industry

White Paper

M2M Challenges for further development

November 2011

Contributors*: Jean-Pierre Delesse, Daniel Borleteau, Helmut Scherzer.*

Disclaimer

Eurosmart has taken reasonable measures to ensure the quality of the information contained in this document. However, Eurosmart will not assume any legal liability or responsibility for the accuracy, reliability or completeness of any information contained herein or for any consequences of any use.

Index

Introduction

The exciting development of digital technologies will enable more features, more convenience and will make life easier, simpler and safer. On top of changing our lives, there is also an expectation from consumers and citizens that they will facilitate their interaction with this digital world by providing:

- A good balance between convenience and security;
- More information and guarantees of privacy;
- Interoperable devices and services.

There is now an acceptance that M2M eco-systems will be widely deployed; industry analysts forecast more than 100 million industrial cellular M2M devices to be shipped in 2015. If we include other connected devices communicating using technologies like RFID, this figure can reach the billions.

This perspective is however raising questions about some key challenges that M2M systems will be facing for further development:

- Network capability (in terms of deployment and speed)
- Cost (due to technical complexity and market fragmentation)
- Security to protect identity and asset
- Standardisation as a key enabler to ensure interoperable services

Security and **standardisation** remain major challenges for the further deployment of M2M systems. The purpose of this paper is to provide an overview of M2M applications, to stress potential risks in term of security and standardisation for the rapid development of M2M systems, and to provide some proposals to overcome these challenges.

1. Definition

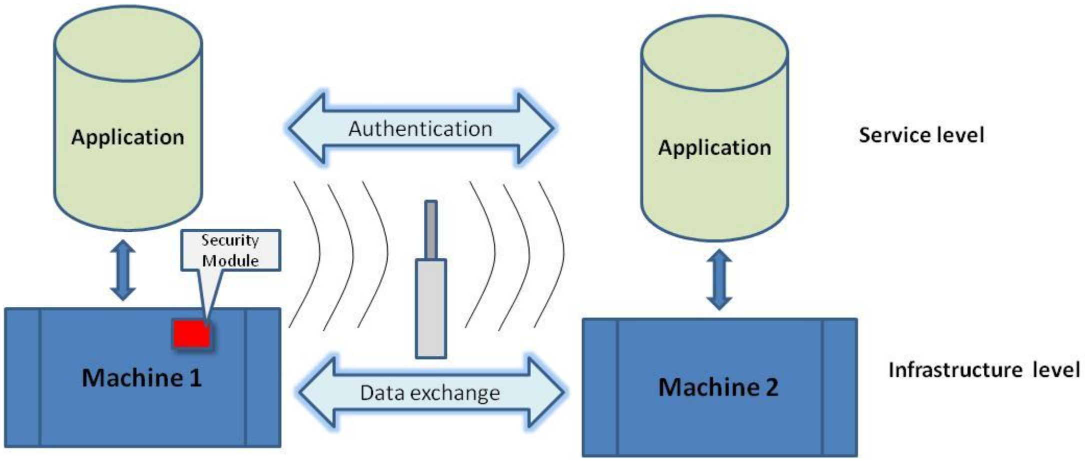
M2M stands for Machine-to-Machine communication. It can be defined as an eco-system that allows communication between two pieces of equipment by exchanging data over a wireless network or by direct (wired) connection without human intervention.

When at least one piece of equipment includes a Smart Secure Device as defined by Eurosmart, it can be designated as a Smart M2M eco-system enabling identification, control and transactions with a high security level.

A smart secure device contains a secure and certified microcontroller and embedded software. The smart secure device is personalized through secure issuance and securely updated through a rigorous, certified lifecycle management process. It offers security services to the Human to Machine and Machine to Machine application domains.

Most emerging M2M applications use a cellular wireless network where the UICC is the Secure Device in the system. In this case, we call the secure element **MIM,** for M2M Identification Module. This MIM is a product with specific requirements in terms of quality and durability and that this has to be taken into account along the value chain, in the best interest of all the actors and the end user.

There are other types of M2M eco-systems which are not UICC centric; one example is described in this document.



2. Market Segmentation

2.1 Overview

The M2M market is extremely fragmented, covering a wide range of applications in the areas of Automotive, Metering, Vending Machines, Health, etc.

Among these applications, some require "mobility", like the e-Call system or fleet tracking, and therefore are UICC centric applications.

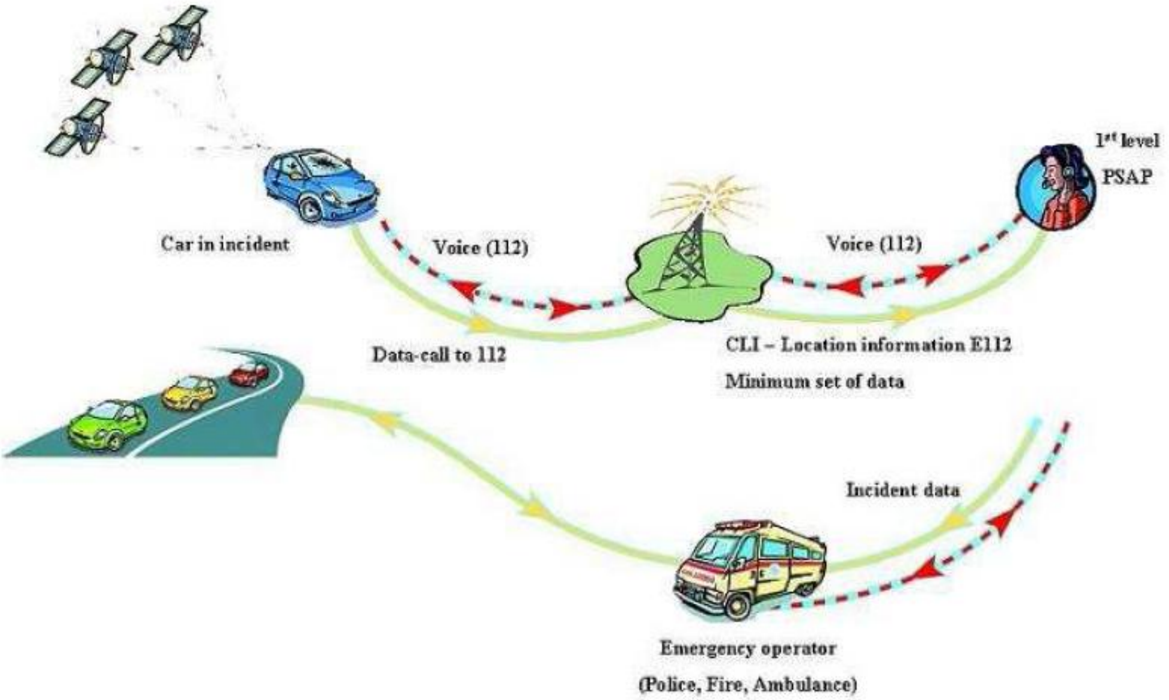
Other applications like anti-cloning or usage control do not require a network to exchange data, or use of a network other than cellular radio. They are, therefore, not UICC-centric applications.

Given that M2M is a fragmented market, with applications in several industries, we propose to give 3 examples of applications in this document: telematics, smart grids and medical equipment anti-cloning. Other promising applications are also rapidly emerging, including e-health.

2.2 Telematics

Telematics cover a wide range of applications & services linked to the automotive fields, including fleet tracking, travel assistance, toll collection, vehicle -to -vehicle systems, etc. Among telematics applications, e-Call is already a market reality which is expected to boom in the next years.

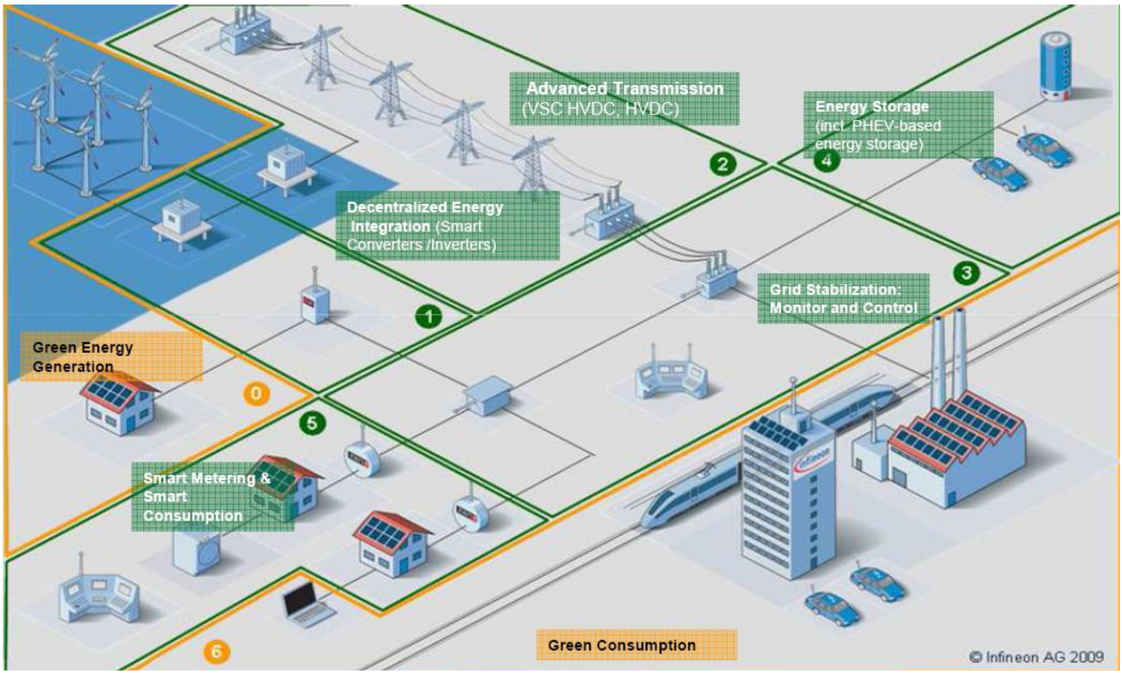
Europe is leading the deployment with the eCall initiative. The project aims to avoid at least 2500 fatalities per year and to dramatically reduce the severity of injuries. eCall is certainly a great opportunity to drive telematics value-based services.



2.3 Smart grids

A smart grid is a type of electrical grid which attempts to predict and intelligently respond to the behaviour and actions of all electrical power users connected to it - suppliers, consumers and those who are both – in order to efficiently deliver reliable, cheap, and sustainable electricity services.

Concept of a Smart Grid:


Advanced Transmission (VSC HVDC, HVDC)
Energy Storage (incl. PHEV-based energy storage)
2
4
Decentralized Energy Integration (Smart Converters /Inverters)
3
Grid Stabilization: Monitor and Control
1
Green Energy Generation
0
5
Smart Metering & Smart Consumption
6
Green Consumption
© Infineon AG 2009

The main drivers for Smart Grid development are the risks linked to climate changes due to the greenhouse effect and dwindling fossil energy resources. Smart Grid will bring several benefits, including:

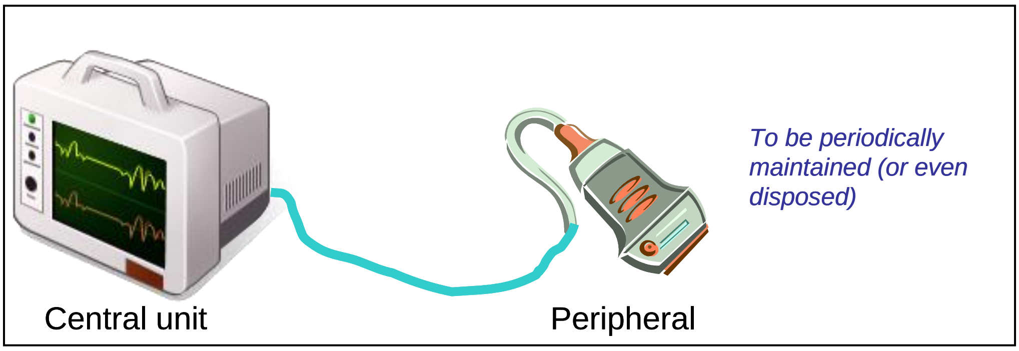
- Energy reduction via increased efficiency and better end customer awareness;
- Efficient use of de-centrally generated green energy.

A key element of a Smart Grid is the Smart Meter. A Smart Meter measures consumption (water, heat, electricity). It communicates bi-directionally with a remote party (master and slave role) and can optionally communicate with household appliances and other devices at home. Smart Meters will be connected through standardized network infrastructures and will likely become the targets of attacks and misuses. Physical access to smart meters is easy and they are basically unprotected.

Therefore, security is also a prerequisite for a successful smart grid operation.

2.4 Medical equipment anti-cloning

Let's consider medical equipment consisting of one central unit connected to a peripheral.



The peripheral must be periodically maintained after a number of hours of use (or even replaced if fully disposable).

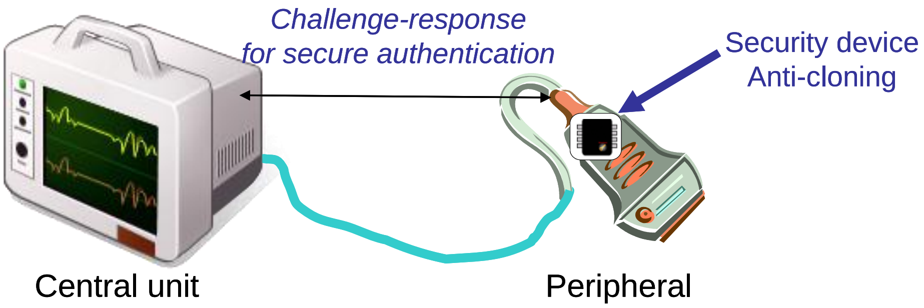
A similar peripheral made by another supplier (a clone!) might not work like the original equipment. This could have a disastrous impact on medical treatment quality and patient health. Consequently, the original equipment maker wants to ensure that the central unit will only work with genuine peripherals that meet target specifications.

Anti-cloning solution

By implementing a secure device (made of secure silicon and software) in the peripheral, the central unit will be able to authenticate the peripheral, typically by using a challenge-response mechanism based on cryptographic functions. If authentication succeeds, the central unit will continue to use the peripheral.

If authentication fails, the central unit will decide between several options like sending a warning message or even rejecting the use of the peripheral.

The authentication device (typically a secure microcontroller running a secure application including an encryption key) is tamper resistant, therefore, it is impossible, or at least tremendously costly, to hack such a device and clone the peripheral equipment.



Additional features can be implemented beyond simple authentication. One example is usage control. In the above medical equipment, it is relatively simple to implement counters in the secure device, for example, in order to monitor the number of hours the peripheral has been in use.

At the end of each session, the central unit updates the number of hours spent in operation and at the beginning of each session, the central unit checks if this counter is still within the specified period of use time. If it isn’t, the central unit will request that the peripheral be replaced (or maintained, if appropriate). Again, since this type of counter is securely stored in the tamper resistant platform, it is not possible to change it. As a result, it provides an extremely high confidence level for data integrity and safe operation.

3. Security challenges in M2M

3.1 About security

Digital applications are spreading out and fraudsters and criminals are actively seeking ways to attacking systems. Attacks can have huge effects both for end-users and for system operators when they impact objects used in our daily lives.

Like quality, security is a feature that is hard to appreciate until you no longer have it.

The upfront savings made from buying low security products when a high security solution was needed, can be very illusory. Equally, why pay too much for something you don't need? The motivation of attackers often depends on the level of assets at risk, and the probability of an attack is not the same as the probability of a successful attack.

With M2M applications, sensitive information is often exchanged and stored while system users and owners have assets to protect, be it their personal identity, money, privacy, intellectual property, state security or others.

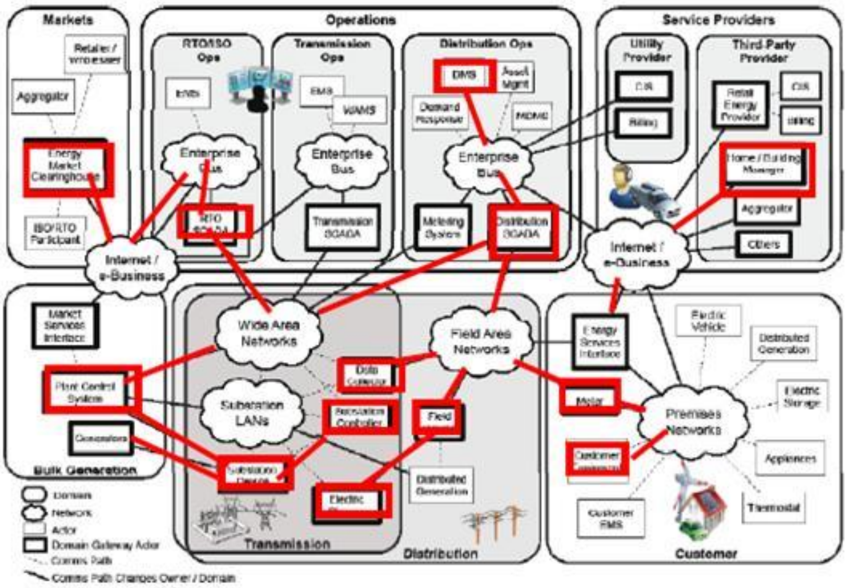
For M2M players who have less experience in smart security, it may be a challenge to define the level of security which fits with their expectations. One of Eurosmart's missions is to provide information and support in order to identify risks and to select the appropriate level of security depending on the asset to be protected.

3.2 Security in M2M eco-systems

It is likely that there will be more security challenges with M2M eco-systems compared to other eco-systems like Human to Machine. We see at least three main reasons for those security issues:

<u>1° Complexity and openness</u>

M2M eco-systems are complex, open with a multitude of players and components, and therefore more vulnerable.



If we consider a Smart Grid environment and existing techniques, attackers could theoretically exploit the openness of the network to enter into the system of a nuclear plant.

2° Human secret

By definition, there is no human intervention in a M2M system. In a system based on smart security, protection is based on two factors: what you have (a credit card for instance) and what you know (a pin code).

In a M2M system, there is no more “human secret”-such as pin code, and this can make the system riskier.

3° Deviations of the system

In many systems controlled by human intervention, it is still possible to solve deviations to established rules on the spot. This ultimate control no longer exists in a M2M system.

3.3 Security recommendations for M2M systems

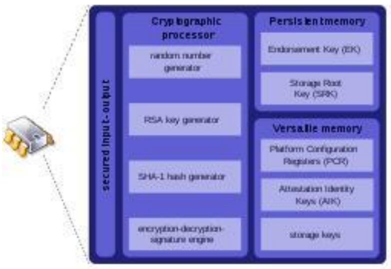
The digital security industry has acquired expertise in smart security, based on secure elements running secure software.

A secure element is generally based on a tamper resistant microcontroller coupled in some cases with a crypto-processor. One important characteristic is that the secure element is personalised by the issuer, and not by the user. This reinforces the protection against hardware and software security attacks.

Some recommendations are:

- To build blocks with an integrated secure element; a MIM is a product with specific requirements in terms of quality and durability, different from SIMs used in mobile phones;
- To develop data storage solutions that include an integrated secure element;
- To install routers & gateways with an integrated secure element;
- To enhance the communication channel’s protection with attack resistant protocols;
- To ensure that value added services use strong authentication techniques;

Trusted Platform module



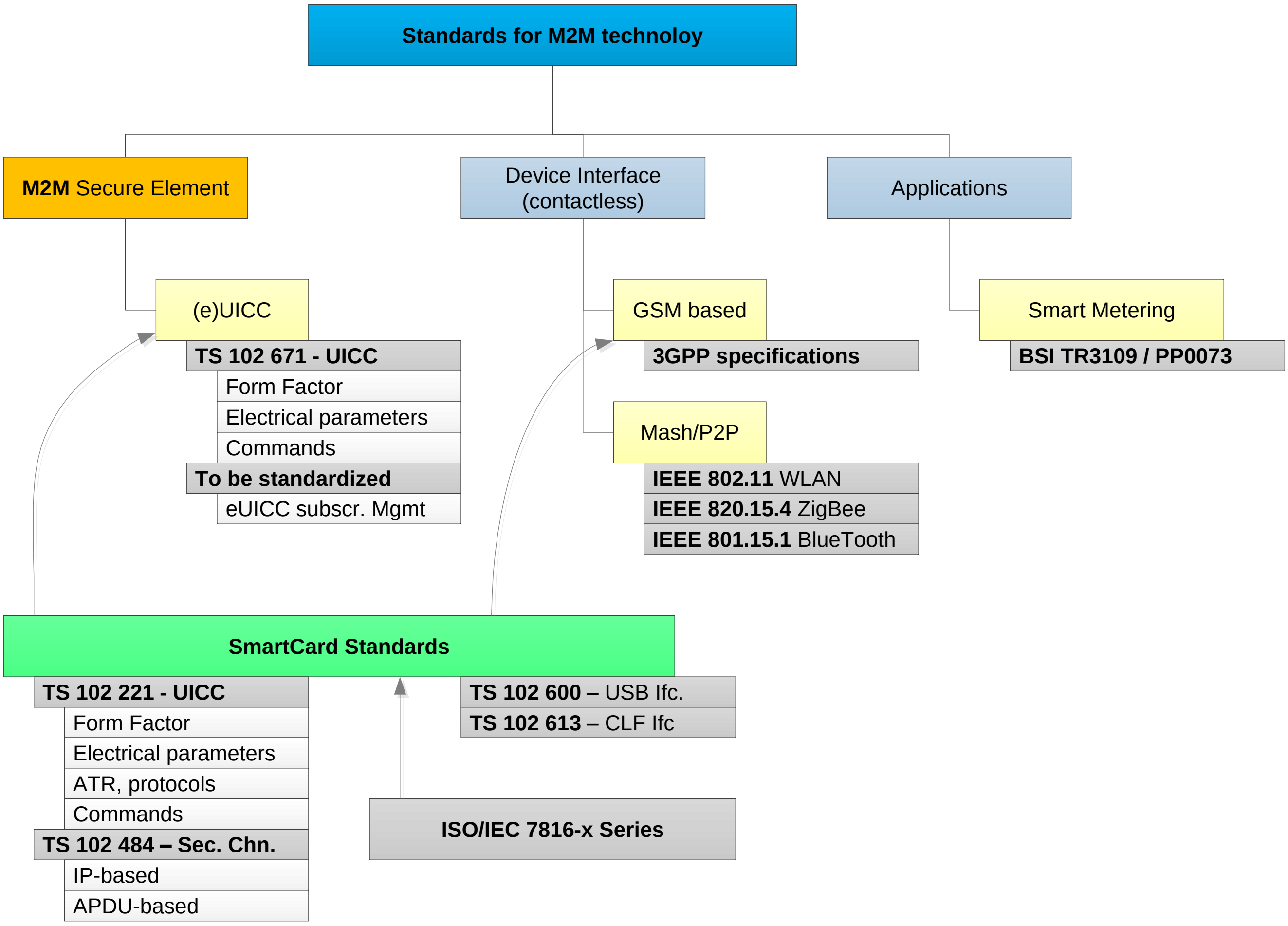
M2M identification module

4. M2M standardization challenges

M2M technology comprises a large set of applications as described in the chapters above. Each of these application fields requires its own specific standards with a focus on the application level. The basic M2M functionality common to these applications can be covered by the two most essential interfaces.

- 4.1 Standardizing the eUICC/Secure Element interface

- Standardizing Device Interfaces
- 4.3 Standardizing Applications



4.1 Standardizing the eUICC/Secure Element interface

Most of the available specifications with a dedicated focus on M2M technology were created by the European Communication Standards Institute (ETSI), hence the "standards" are available as Technical Specifications, which ETSI is officially allowed to deliver. However, an

ETSI Technical Specification may be taken by CEN to become an official European Standard.

4.1.1 The basic standards

The entry point to M2M standardization is TS 102 671 which considers the particular interpretation of existing Smart Card (UICC = Universal Integrated Circuits Card) standards for the purpose of M2M. Two new form factors are specified as MFF1 (plugged) and MFF2 (soldered).

The TS 102 671 MM specification relies on underlying Smart Card specifications for the UICC in the classic Smart Card environment. Since M2M secure elements are technically very similar to secure elements used in mobile phones, this heritage from Smart Card standards is possible.

Smart Card standards essentially inherit their content from the ISO/IEC 7816-x (Part 1 - 8) series. As these standards offer many options, the ETSI standards select a particular set of features from 7816-x for the purpose of telecommunications and M2M.

ETSI Technical Specifications separately provide information about the specified topics, in contrast to having a single standard that comprises all of the features in one paper. The most relevant UICC-related ETSI TS (Technical Specifications) are:

- **ETSI TS 102 221 V9.2.0 (2010-10)**
    - Smart Cards; UICC-Terminal interface; *Physical and logical characteristics* (Release 9)
- **ETSI TS 102 484 V10.0.0 (2011-01)**
    - Smart Cards; *Secure channel between a UICC and an end-point terminal* (Release 10)
- **ETSI TS 102 600 V10.0.0 (2010-10)**
    - UICC-Terminal interface; *Characteristics of the USB interface* (Release 10)
- **ETSI TS 102 613 V9.2.0 (2011-03)**
    - UICC - Contactless Front-end (CLF) Interface; Part 1: *Physical and data link layer characteristics* (Release 9)

and the specification dedicated to M2M technology:

- **ETSI TS 102 671 V9.1.0 (2011-09)**
    - Smart Cards; Machine to Machine UICC; *Physical and logical characteristics* (Release 9)

The UICC specifications describe the particular selection for:

- Form Factors (Dimensions and Contacts)
- Physical Characteristics (Electrical parameters, Environmental conditions)
- Communication protocols / ATR
- Secure channel establishment
- APDU Command Interface

M2M devices may work in very harsh environments, exposed to much higher temperature ranges than secure elements in mobile phones. Therefore ETSI TS 102671 supersedes some parameters inherited from UICC-originated mobile phone specifications:

- Environmental classes
- Additional form factors MFF1/MFF2 for the embedded UICC
- Paring mechanisms (with reference to existing specifications)

4.1.2 The embedded UICC

An embedded UICC is becoming more and more popular for the requirements of an M2M environment. The advantages are smaller size (Form Factor) and production optimization through "pick and place" in contrast to a mechanical contact station. The specified definition for "embedded" is "not easily accessible or replaceable".

The consequence is that, in some cases, the personalization of such an embedded UICC needs to be done as a secure software download which implies subscription management on the back end.

Subscription based secure elements like the eUICC also allow for the software based change of a subscription to a different provider. The possible change of existing business models is associated with the technical discussion of eUICCs.

Specification of the subscription management is currently ongoing in the ETSI SCP (Smart Card Platform) group. A final announcement date for the first TS was not available by Nov. 2011.

The GSMA has initiated a dedicated “Embedded SIM” project and contributed the requirements associated with subscription management.

The SIMalliance group participates in the project work streams on the Architecture, Subscription Manager, Protection Profile, and Certification. This work is ongoing, but a final specification was not released by Nov 2011.

4.2 Standardizing the communication interface

Other aspects currently need to be solved beyond standardization of the secure element, . The most vital discussion focuses on the best communication interface. A final decision on one or two major schemes has not been made yet. Again the standardization discussion is being carried out in a separate ETSI "TC M2M" working group.

In general, the communication of M2M modules may be divided into:

- Wired communication
- GSM based communication
- Point to (n-) Point communication
- IP-based communication

Wired communication is related to use in the connected home landscape. Here, there are already well established standards available. The most popular are the KNX specifications, followed by PowerNet and M-BUS. Current activities tend towards a common application interface for these transport layers, as manifested in EEBUS activities.

Traditional GSM standards apply for GSM-based communication. The advantage of using the GSM network is its good coverage throughout many countries in Europe, and the internet connectivity which is inherent through 2G/3G/4G and LTE technology. Its disadvantage relates to the subscriber fee which competes with DSL internet connections. Technically, GSM products do have a long history of optimizing power management in cases where M2M products need to be run on batteries.

The power problem for battery driven M2M devices is also an important argument for alternative communication Point to (n-) point protocols.

Bluetooth specified in IEEE 801.15.1 is a classic candidate allowing connection in a 1 to 7 network. The coming Bluetooth low-power specification might buy Bluetooth a position in the ranking for the most suitable M2M protocol.

WLAN (Wi-Fi) at 2.4 GHz is very popular today. The disadvantages are rather high power consumption and a small number of channels available for transmission. Its advantages come from its well-distributed IP-interface technology and the availability of associated host devices (WLAN router) in many environments. WLAN is an attractive solution for non-battery driven M2M devices, in particular as there is no additional subscriber fee necessary.

ZigBee (IEEE 820.15.4) works at 2.4 GHz and provides an attractive interface for M2M devices. Many M2M devices with ZigBee are already available today. ZigBee does not comply with WLAN and would require a separate router to connect to the Internet. It also requires a Class-A power amplifier which can work at a maximum efficiency of 25%. Thus ZigBee is not power optimized.

ANT+ (http://www.thisisant.com) is a proprietary protocol of a smaller nature, but well established in the sports industry, e.g. for bike computers that need to transmit sensor information to a host unit (e.g. bike tachometer). Since there is a lot of experience with low power profiles, the protocol is suitable for battery-driven M2M technology.

4.3 Standardizing Applications

While there are lots of application fields around, the Smart Metering (Smart Grid) discussion is best associated with M2M technology. Hence, we only cover the progress made in Smart Metering in the following chapter.

Smart Metering

Smart Metering allows more precise measurement of the power consumption of a household and, when implemented in a Smart Grid, devices can be managed to stand-by or operate with respect to available power production. Stimulated by pricing models, the Smart Grid allows optimized power distribution - the social impact on a non-running dishwasher that "waits" for the best rate has been little investigated.

Smart Metering is, however, an evolving topic. In Germany, in particular, where nuclear plants have been mostly abandoned after the Fukushima catastrophe, energy alternatives stimulate the market, especially through solar panels which have the highest density in Germany today.

Hence the German BSI (National Security Agency of Germany) has created several valuable papers on Smart Metering.

BSR3109 Draft Version 0.20 (10th Oct. 2011) describes the “Security requirements for the interoperability of an intelligent measurement system for material and energy amounts”. This implies M2M Smart Metering devices.

Two appendices describe the crypto-logical requirements for Smart Meter gateways and the PKI Infrastructure required for Smart Meters using a public network. Unfortunately, BSR3109 is currently only available in German.

However, the BSI also provides a protection profile in English which may be used to certify Smart Metering products. Since there is mutual recognition between most European Certification Authorities up to EAL4, this protection profile may well be used in other European countries.

Conclusion

We are just at the beginning of M2M deployment, with several market segments emerging:

- Telematics, including fleet management and e-call applications;
- Smart Grids
- e-Health

Technologies – including devices, networks, IT and services – exist and are suitable for a rapid M2M deployment.

However, there are still some challenges that we have to overcome to ensure wider deployment and acceptance of M2M systems:

- Highly fragmented and usually dedicated to a single application, leading to cost issues;
- Lack of real standardisation and some resistance to going faster;
- Security since M2M will face more challenges than any other system.

M2M and the Internet of things thus represent important opportunities for the smart security industry to secure access, transmission and data storage

Eurosmart recommendations to build smart M2M solution:

- Building blocks, routers & gateways and data storage with embedded smart secure elements having specific requirements in terms of quality and durability
- Communication channels with attack resistant protocols
- Value added services with strong authentication

M2M will certainly change our lives and bring benefits for citizen and enterprises:

- M2M for a better, safer and more convenient life for people;
- M2M for more efficient business management for companies;
- M2M for easier interaction with the digital world;
- M2M for huge opportunities for the electronics industry;
- M2M is paving the way of the Internet of Things.

EUROSMART
The Voice of the Smart Security Industry

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work into dedicated working groups (communication, marketing, security, electronic identity, new form factors, and prospect emerging markets).

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry" and is largely involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit www.eurosmart.com

EUROSMART
Eurosmart General Secretariat
Rue du Luxembourg 19-21
B-1000 Brussels
Tel: + 32 2 506 88 38
Fax: + 32 2 506 88 25
eurosmart@eurosmart.com