EUROSMART

The Voice of the Smart Security Industry

Smart M2M Report

April 2009

Disclaimer

Eurosmart takes 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 therein and any consequences of any use.

INDEX

Message from Marc Bertin, Chairman of Eurosmart

Eurosmart is extending its presence and vision in global Smart Security by issuing this new report on Smart M2M.

We believe that our Smart Card, and beyond Smart Security, technologies will be embedded in most of the smart elements surrounding us in our daily professional and personal life. The M2M market is today developing through concrete applications like e-Call (emergency Call) integrated in cars, or fleet management or remote metering. But if those M2M technologies match convenience and wireless communication, there is a real need for security and for device identification.

Our industry could dream of an electronic identity not only for each human being but also for each Smart object. We are just at the beginning of this new exciting evolution of our Smart Security Industry. This report is about Smart M2M, but is also introducing the concept of Internet of Things, for ubiquitous connectivity and security.

After the report on Smart USB tokens last year, this is another opportunity for our New Form Factor Working Group to demonstrate its ability to analyze and monitor Smart Security evolution.

This new report confirms Eurosmart evolution in addressing all Smart Security fields and eco-systems.

Enjoy your reading!

Marc Bertin
Chairman
30 April 2009

1. Introduction

The key asset of the Security industry is no longer related to a single **specific form factor** like a Smart Card, but rather to its expertise on **strong security** which can be implemented wherever it is needed. It has pushed Eurosmart members to look at a wider scope and to explore the use of different form factors, like **USB token** or **Machine to Machine module.**

The objective of the report is**:**

- To ensure there is a common definition among Eurosmart members;
- To provide relevant information, like technology trends, market figures, etc.;
- To be used as a reference for external communication on behalf of Eurosmart: exhibitions, press conferences, articles, etc.

2. Smart M2M definition

M2M stands for Machine to Machine communication. It can be defined as an eco-system allowing the communication between two pieces of equipment by exchanging data over a wireless network [1] or by direct (wired) connection without human intervention.

When at least one piece of equipment includes a Smart Secure Device as defined by Eurosmart[2], it can be quoted as a **Smart M2M** eco-system enabling identification, control or transaction.

- **Notion of master and slave**: contrary to the classical IFD-ICC (reader/card) view, any of an M2M device may act in the role of the **master**. For instance, a secure element in a gas meter could initiate a network session (master role) every month to deliver its data instead of responding to the request of a metering service (slave role).

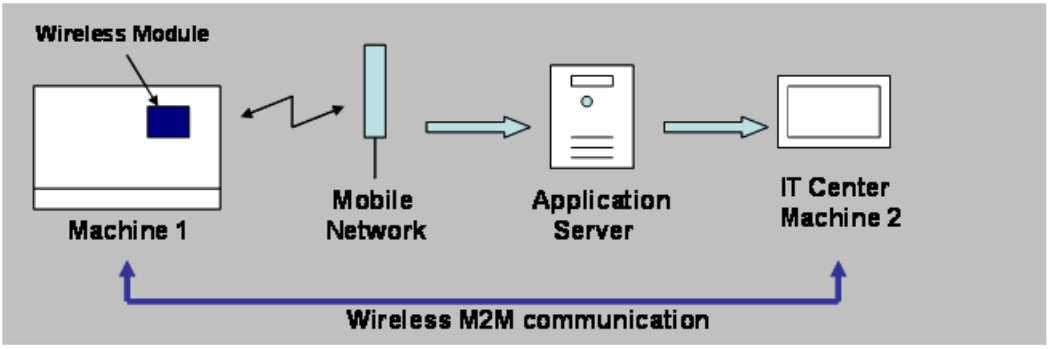
- **SIM Centric**: most visible M2M applications using wireless network are SIM centric, the SIM is the Secure Device into the eco-system.

- **About TPM**: TPM is not included in this report. The working group recognizes that TPM could be some sort of M2M application, however in most of TPM applications, the two pieces of equipment are on the same board and therefore not falling in our definition of M2M application.

[1] 3G, WiFi, Bluetooth, Zigbee, etc.

[2] Smart secure device definition:
- Contains a tamper-resistant micro-controller and software for authentication, integrity, confidentiality and non repudiation;
- Supports personalization by the issuer.

- **M2M drawings** - no human intervention!



3. Market segmentation, risks, examples of applications

3.1 Market Segmentation

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

Among those applications, some require “mobility” like the e-Call system or fleet tracking and therefore are SIM centric applications.
Other applications like anti-cloning or usage control do not require a network to exchange data and therefore are non SIM centric applications.

3.2 Risks

In this open environment, it is likely that M2M will face the same kind of threats as any other applications requiring secure identification (hacking, SPAM, identity theft). For some applications like e-Call or medical control, the consequences of a non-tamper resistant eco-system could be huge as it involves human safety.

What would happen for example if the server of a rescue organisation received corrupted data from a car emitting an emergency call? What would be the benefit of a security network based on M2M technology if a hacker takes full or partial control of the network?

3.3 Examples of applications

- SIM centric applications: automotive telematics, metering, vending machines, fleet tracking:

Remote diagnostics
Emergency assistance
Positioning
Remote Inspection

Automotive

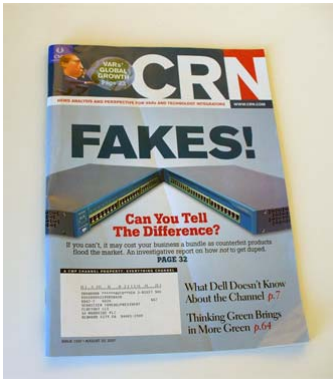
Usage measurement

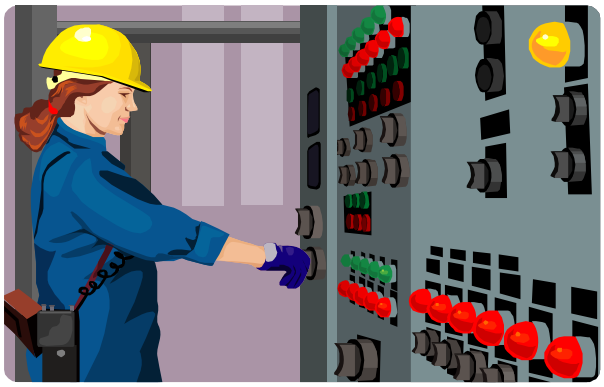
Metering

Remote Inspection
Refill requirement

Vending

- Non SIM centric applications: anti-cloning, usage control





4. Security

As far as security is concerned, we believe it is important to identify first what is the real objective for implementing M2M technology and then to ensure the appropriate level of security is implemented depending of the objectives. For instance, if the objective is to

save human life like e-Call, then a high level of security will be needed. In some cases, there may be a combination of multiple objectives

Without being exhaustive, we see at least 4 different objectives for M2M implementation:

1. **Identification:** in most of the M2M applications, there is a requirement that the machines which are at the end of the chain can identify themselves. For instance, a server for vending machine system will have to identify which machine in the field is sending a request for refilling coffee.
2. **Transaction**: in some application like metering, the use of M2M will lead to a payment of an invoice.
3. **Human Safety:** in specific applications like e-Call, the objective is clearly to save human live. For these applications, there should be no compromise in the level of security which has to be implemented.
4. **Business model**: M2M can help to generate more business; for instance, a manufacturer of main equipment will use M2M to have a close control of accessories produced by qualified suppliers.

Applications	Identification	Transaction	Human Safety	Business Model
Automotive Telematics				
e-call	yes	yes	yes	no
location services	yes	no	no	no
remote services	yes	no	no	no
Tracking, fleet Mgt	yes	no	no	yes
Metering	yes	yes	no	no
Vending/POS	yes	yes	no	no
Anti-Cloning	yes	no	no	yes
Usage Control				
Medical	yes	no	yes	no
Consumer & Indust	yes	no	no	yes

The Smart Security Industry can offer a wide range of security levels and labels, supported by certification bodies, depending on the requirements of the end users and on the main purpose of the application.

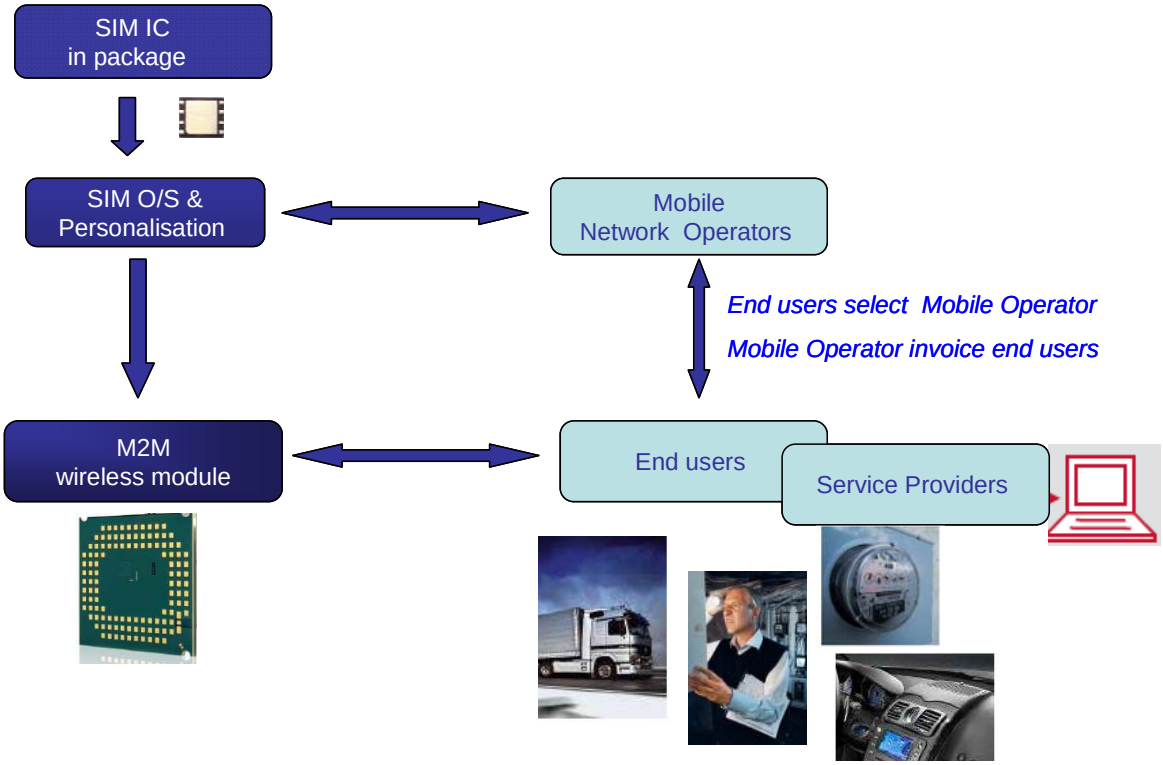
5. Key players for Smart M2M

The value chain of the Smart M2M eco-system remains complex as it involves different players and activities, such as silicon vendors, SIM producers, SIM personalization, Module Makers, Mobile Network Operators, Integrators and Services providers.

For SIM centric, it is not a surprise to see Mobile Network Operators (MNOs) willing to be at the heart of the eco-system. Clearly, M2M will offer opportunities for MNOs to generate new revenues through new applications and new services.

All major MNOs in Europe are defining their strategy to address the M2M market, raising technical and economic expectations to the Smart Security Industry.

- Value chain for SIM Centric applications**:**



6. Technology trend, challenges

6.1 SIM Centric Smart M2M

The different players in the Smart M2M value chain have already identified some common needs especially for the SIM:

- Physical constraints: temperature, vibration, humidity, etc.
- Data retention, life time.

As it is often the case for new applications, standardisation and business model seem to be the remaining challenges that Smart M2M will have to cope with.

For instance, there is an on-going debate at the ETSI level regarding the new form factor which should be used for the M2M SIM: soldered, removable, VQFN, SOP, etc.? So far, the Smart Security Industry has always been able to reach a consensus addressing the needs of the end users and there is no doubt it will be the case for the M2M.

6.2 Non SIM Centric Smart M2M

In that case, the trend is likely to merge the secure element and the main application resources. It has impacts on both the hardware side and the software side: Secure

element will not be SIM like, but rather versatile microcontrollers with enhanced interfacing and computing capabilities with embedded security features.

Similarly, embedded software should cover not only the secure authentication (or transaction), but also the various application needs (timing measurement, data logging, external communications, etc.) without opening security breaches.

6.3 Conclusion

As a conclusion, it can be said that the Smart M2M technical challenges consist in merging fundamental security concepts with embedded application performances and quality requirements.

7. Market figures

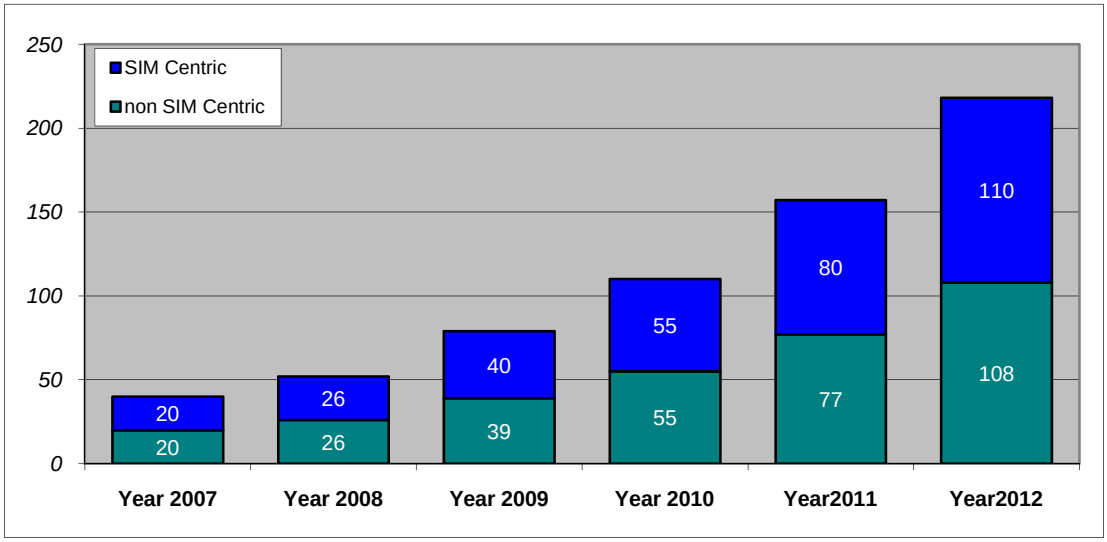
M2M represents a huge market potential. As of today, Smart M2M has a relatively low penetration and it is too early to say how big it will ultimately be. The need for more Security will definitively be a driving factor.

As far as SIM Centric Smart M2M is concerned, the expected growth will be facilitated by the expansion of the GSM network and by the increase of broadband connectivity (like 3G).

Some Smart M2M emerging applications are driven by new regulations for emergency car safety, like the e-Call initiative in Europe, or by programs for energy saving like remote metering.

Berg Insight reports that Europe represents a potential for more than 600 million wireless connections with different levels of security, while IDATE and ABI Research estimate that by 2010, there will be about 2 billion machines which will have the ability to communicate with each other.

M2M modules in Mp per year-estimation Eurosmart as of April 2009



8. Conclusion

Security Industry, and especially Eurosmart members, has already the experience and the know-how to satisfy the requirements of the Smart M2M in term of reliability and security.

M2M is a huge and fragmented market, however we believe that security will be an essential driving factor and we remain confident in the future of the Smart M2M.

Eurosmart is an international non-profit association located in Brussels and representing 25 companies of the Smart Security Industry for multi-sectors applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, developing Smart Security standards and continuously improving quality and security applications.

Manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers gather and work into dedicated working groups on communication and marketing, security, electronic identity and new form factors, and prospect emerging markets. Members are largely involved in political and technical initiatives as well as research and development projects at the European and international levels

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".

More information: www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21 – B-1000 Bruxelles
Tel. (+32) 2 506 88 38/ Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com