EUROSMART
The Voice of the Smart Security Industry

White Paper

Smart M2M Module

November 2009

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 - Message from Marc Bertin, Chairman of Eurosmart

M2M has been identified as one of the most promising markets for our industry in years and it is being followed by Eurosmart as such. It's always very exciting when promises become reality!

This is the case today, and I am pleased that Eurosmart is confirming its vision by issuing this new Smart M2M Module white paper.

We believe that our Smart Technologies will have a role to play in most of the smart and communications objects we use in our daily professional and personal life. The M2M market is currently developing through concrete applications based on security and device identification. In the near future, every human being will have to deal with hundreds of smart objects and security and privacy will be essential. Our industry has the technologies to solve those challenges.

Our New Form Factor Working Group has already done a great job, and will obviously keep participating in the development of M2M, by analyzing and promoting market successes.

By the way, Eurosmart will lead the M2M space at Cartes'09! This is another reason why our mission of sharing vision, expertise and educating the market is necessary to this new range of applications.

Enjoy your reading!

Marc BERTIN

Chairman

23 October 2009

1. Market Environment

It was quite difficult to imagine just a few years ago that a vending machine could be able to order coffee on its own by using a wireless network, or that a car could automatically send an emergency call to a rescue center. As of today, millions of machines are already communicating with other machines, and this trend will accelerate to a point that billions of objects and machines will exchange data without human intervention. Machine to machine (M2M) has a relatively low market penetration (1 or 2% of total SIM), however government regulations (safety, energy saving) and the rapid development of wireless data access (3G, LTE) will undoubtedly accelerate the take-up of M2M eco-systems in our everyday life.

The M2M market is extremely fragmented, covering a wide range of applications including automotive, fleet management, energy & utility, etc…

Some applications require a network to connect the machines (Cellular, WiFi, etc.) with a majority being “SIM-centric”. For other applications, data exchange is done through a direct connection between the two pieces of equipment.

While M2M technologies match convenience, there is a real need to look at two other factors: privacy and security.

2. Smart M2M module definitions

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[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 with high security level.

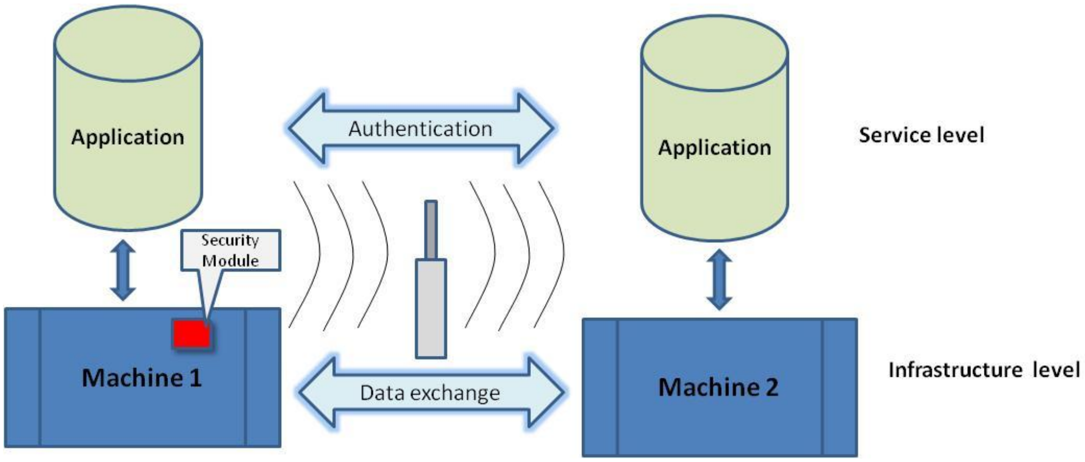
Notion of master and slave: in addition to the traditional reader/card concept, any M2M device may also act as a master. For instance, a secure element in a gas meter could initiate a network session (master role) every month to deliver its data instead of responding to the request of a metering service (slave role).

Most visible M2M applications use cellular wireless network where the SIM is the Secure Device in the eco-system. There are other types of M2M eco-systems which are not SIM-centric. They are described in this document.

[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.



3. Identification and Security

We believe that there will be more security challenges when deploying a M2M eco-system compared to a traditional eco-system like H2M (human to machine)

- Security is not always well understood and this will not improve in a system based on a very complex value chain
- Since M2M will cover a wide range of applications, it is likely that cross-industry security recognition will be a serious challenge. Who will decide or who will be responsible??
- A “human secret” (e.g. a pin code) will no longer be used
- There will be no possibility to solve deviations to established rules on the spot

However, as we already mentioned, it is likely that any M2M eco-system will face the same kinds of threats as other H2M systems: ID theft, hacking, cracking, SPAM, etc.

Security for M2M depends on two main elements:

- The actual reason for implementing M2M
- The risk decision (what level of risk are we ready to accept)

The same SIM card can be used for replenishing a vending machine or for saving human life through e-Call: the objective is different, so is the level of acceptable risk.

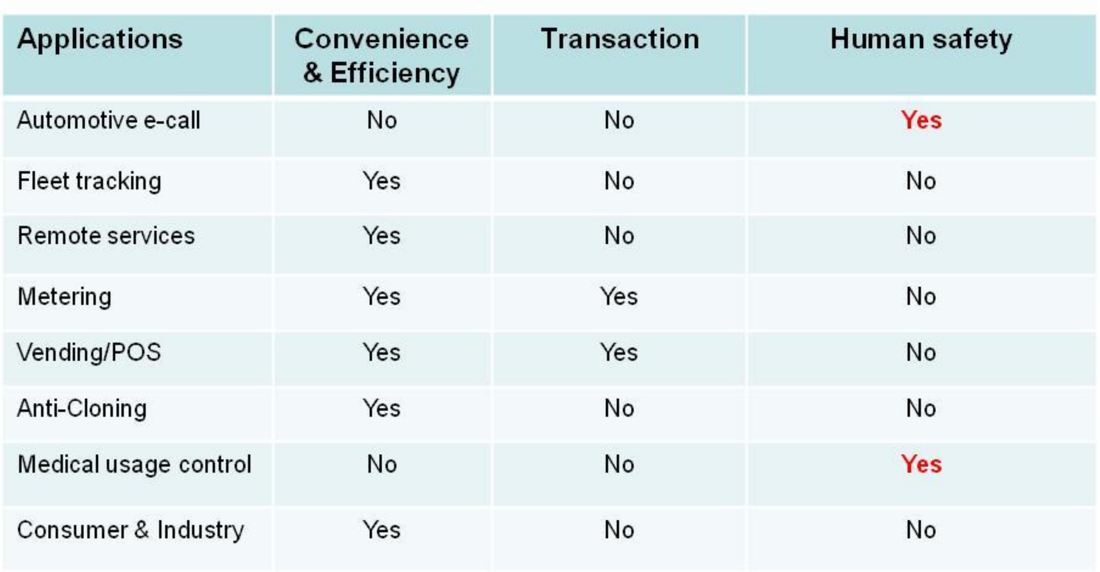
<u>Reason for implemetation</u>

Without being exhaustive, there are three primary reasons for implementing an M2M eco-system:

1. Convenience & business efficiency: M2M can help to protect and optimize business. For instance, a manufacturer of end equipment will use M2M to have close control over accessories produced by qualified suppliers;

2. Transaction: in some applications like Metering, the use of M2M will result in the payment of an invoice.

3. Human Safety: in specific applications like e-call, the objective is clearly to save human lives. For these applications, there should be no compromise in the level of security which has to be implemented.



Applications	Convenience & Efficiency	Transaction	Human safety
Automotive e-call	No	No	Yes
Fleet tracking	Yes	No	No
Remote services	Yes	No	No
Metering	Yes	Yes	No
Vending/POS	Yes	Yes	No
Anti-Cloning	Yes	No	No
Medical usage control	No	No	Yes
Consumer & Industry	Yes	No	No

Risk decision

As we mentioned earlier, we believe that M2M will face the same threats as H2M applications: ID theft, hacking, SPAM, phishing, etc.

It will, therefore, be up to companies, system integrators, and governments to decide what level of risk is acceptable

- What level of risk is acceptable when properly identifying a car emitting an emergency call?
- What % of fraud is an electricity provider ready to accept when implementing a remote payment system based on M2M?
- What level of risk can we take to have a hacker taking the control of an energy network in a city?
- What will the risk level be if a coffee machine is not refilled on time?

A suitable security scheme can be selected depending on the final objective and the risk decision.

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

4. Applications and use cases

4.1 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 they are therefore SIM-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 SIM-Centric applications.

4.2 Automotive applications

4.2.1. Market environment, benefits of Smart M2M

Connecting an automotive application to a cellular wireless mobile network opens the door to numerous applications that can be split in four main categories:

- Wireless connection for security: real time access to vehicle position offers the possibility to track and trace a vehicle, especially in case of theft.
- Wireless connection for safety: indeed security is not limited to the vehicle itself: programs such as 'e-Call' in Europe aim at making people safer. An emergency call system embedded in the card reduces rescue time by identifying the emergency level and the accident location
- Wireless connection for efficiency: real time track and trace systems create environmental as well as economic efficiency:
    - Environmental: traffic optimization implies a reduction in traffic congestion and therefore a reduction in carbon dioxide.
    - Economic: “pay as you drive” applications, for example, allow insurance bill optimization
- Wireless connection for entertainment: the wireless module is a gateway that provides digital services inside the vehicle, from basic voice services to multimedia services to access audio and/or video content

The level of integration of the SIM in the vehicle differs between applications: for example the SIM part of an emergency system requires a high level of integration in the card while a SIM used for entertainment access can even be accessed from the vehicle dashboard. Full integration in an automotive system implies that the SIM device be as reliable as any other component of the automotive system, even in harsh environments. This major difference with consumer SIM requires a new manufacturing process as well as new SIM device characteristics.

4.2.2 Automotive use cases: e-Call

The E.U. set up directive in 2003 with the target of halving the number of road deaths by **2010** in Europe and dramatically reducing the severity of injuries. As a reference, there were 39,000 deaths and 1.7 million injuries on European roads in 2008.

The original target for roll out was the end of 2009, however, the project has been severely delayed.

The objective of e-Call is to reduce the response time to accidents.

It is a combination of an In-Vehicle System (IVS)--a device with a Wireless module and GPS location capability--and a corresponding infrastructure of Public Safety Answering Points (PSAPs). When the device detects an accident, it calls the nearest PSAP, transmits the vehicle location and other vital data, and opens a voice connection to the cars involved in the accident.

It has been estimated that "an e-Call" system that relays the accurate location of the accident to the PSAP and emergency services will allow a reduction of response time to the accident of about 50% in rural areas and up to 40% in urban areas."

In order to be efficient, the M2M eco-system for e-Call will have to ensure strong authentication of the call emitter (the car) in order to ensure that rescue is sent to the right place. Smart M2M will provide the right answer in terms of strong authentication.

4.3 Industrial applications

4.3.1 Telemetry

To fight climate change, the European Union has set ambitious targets to be met by the year 2020: greenhouse gases are to be reduced by 20%, energy efficiency and renewable energy to be increased by 20%. A prerequisite to achieving these goals are smart metering systems installed across Europe.

Smart meters not only offer the benefit of efficient monitoring of the consumption of electricity, gas and water, but also establish two-way communication, thus allowing the possibility to actively control consumption remotely. They provide customers with more control and strengthen their consumption awareness. For utility companies, they help to balance peak loads and manage the network more efficiently.

Several European countries have therefore started using smart meters. Most noticeable is Italy, with over 27 million customers, but also the Nordic countries have mass-deployed the technology.

Security is a key factor for success. Meters must be protected against tampering, privacy must be protected and, last but not least, the smart meter network must be secured. The threats are real. Smart meters have already been successfully attacked.

Strong authentication implemented in Smart M2M devices is the solution. It resembles a set of security technologies which have proven in other applications that they can meet the toughest security requirements.

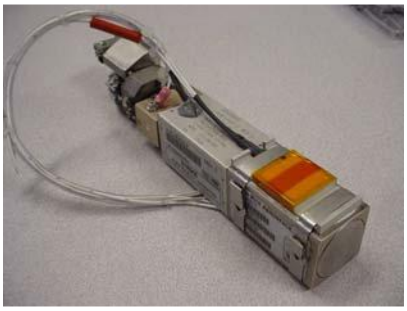
4.4 Cross Segment applications

4.4.1. Aircraft maintenance

The uniqueness and origin of aviation parts are the most sensitive aspects of the reliability of aircrafts and, in fact, to the safety of passengers and crew. Spare parts are typically delivered to airplanes at any location - however, the source of these spare parts is not always known and may potentially harm the reliability of the entire aircraft system.

The "*P*" case

Several airlines including Austrian Airlines, Lufthansa (Germany) and Air France purchased spare parts from the dubious company "*P"* and used them in their fleets. The customer records of "*P"* recorded 50 airlines and hundreds of international service units. In January 2002, the Air Supervision Office, ENAC, raised an alarm publicly. By then "*P*" had already delivered spare parts with fake papers of origin worldwide.



ENAC warned that "… every delivered part might be subject to *"P's*"alteration and had to be considered as a severe threat to the safety of affected aircrafts" – with a recommendation to immediately remove such parts from aircrafts. After several house searches of *"P*" employees, public prosecutors already had evidence – in a hangar, the police found more than 40,000 parts – many of them stored in complete violation of international regulations.

One of the most promising technical answers to the above problem is tagging technology where tags permanently are attached to a part. Currently the following flavors are prominent

- Optical tagging (bar code) (cheap, little flexibility, vulnerable to faking)
- Passive electronic tagging (RFID technology, cheap, little flexibility, fake safe)
- Active electronic tagging (RFID+ technology, expensive, high flexibility, highest security)

All of the above techniques provide unique identification of a part which is as reliable as the tag sticks to the part and as how resistant the tag is against fraudulent copying.

Rationale for M2M in aviation

The sole purpose of M2M technology is the instant identification of aircraft parts in different places and under different conditions. Aircraft companies have four different solution options known as "Mark-it", "Track-it", "Share-it" and "Trace-it". Each is an evolutionary step over its predecessor. "Trace-it" includes lifetime logging of a part whereas "Track-it" only provides proper identification of origin. Lifetime "Trace-it" associates write information on the tag, which implies bi-directional M2M.

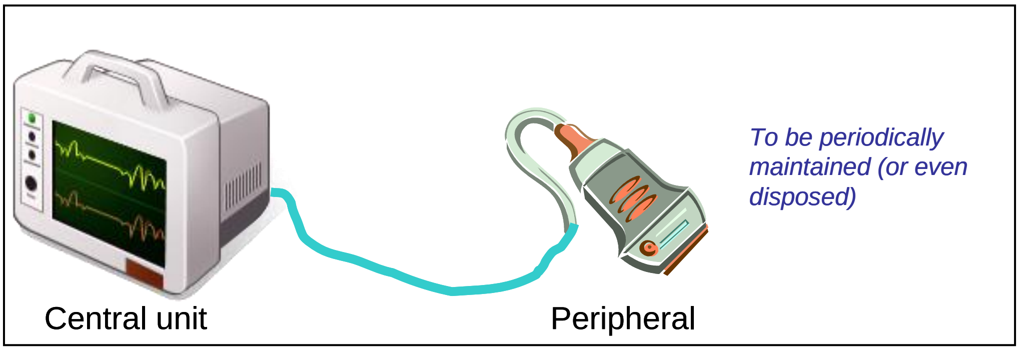
RFID in Aircraft Technology can definitely enable the same performance as M2M, where RFID tags are "passive" unless they are powered by a contactless RF field. To finally achieve the "Trace-it" status, an entire database system is required.

4.4.2 Brand protection

Application example: Medical Equipment.

What is the issue?

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



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

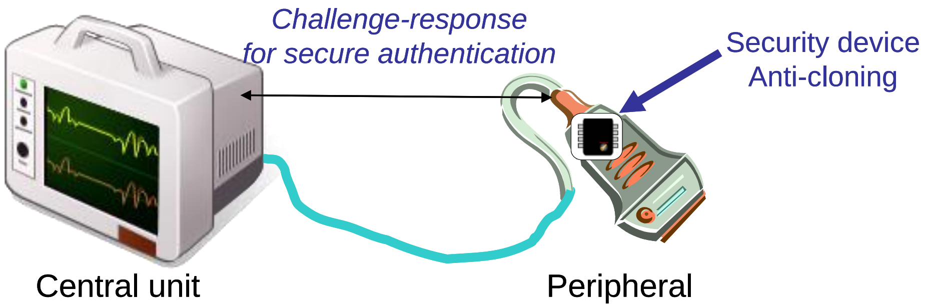
A similar peripheral made by another supplier (a clone!) might not work properly as long as the original equipment. This might have a disastrous impact on medical treatment quality, and patient health. So, the original equipment maker wants to ensure that the central unit will only work with genuine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

Anti-cloning solution

By implementing a secure device (made of secure silicon and software) into 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.



Beyond simple authentication, additional features can be implemented. 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 in use for the peripheral.

So, at 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.

Summary - Benefit

Anti-cloning solutions based on smart devices can provide two main functions:

- ***Secure authentication*** of the peripheral by the main unit providing a high degree of confidence that the peripheral is authentic and specified for the use, hence a high quality level of service. In addition, this can also enable a different business model, for example, in which value can be shifted to the peripheral from the main unit.

- ***Secure storage*** area enabling additional functionality. For example, more sophisticated usage control by monitoring specific parameters such as time of use between two maintenance operations.

Conclusion

The potential of M2M is huge, driven by government regulations and by the deployment of wireless networks; two billion communications devices including 600M in Europe.

The deployment of M2M will offer new services, more convenience, and will help to make the deal with the digital world easier.

Balancing security, risk, and privacy will be a huge challenge for companies and governments when deploying M2M eco-systems.

Another challenge for M2M is to develop enough intelligence to compensate for the absence of human intervention: it is certainly not a big challenge from a technology point of view, but it is a bigger one from a security standpoint.

The Smart Security Industry has more than 30 years experience making compromises between convenience, privacy and security. It can help M2M players decide where the right balance is and how to implement the right technologies including security technologies to protect people and data.

EUROSMART

The Voice of the Smart Security Industry

What is Eurosmart?

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

Contact:
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