Security and Privacy in the Digital World

Solutions from the Smart Security Industry

Smart Embedded Security for the Internet of Things

Content

1. Executive Summary 3

2. Introduction 3

3. Risks and Vulnerabilities 4

4. Use cases 6

5. Recommendations 8

6. Benefits 12

7. Call for actions 13

8. Glossary 14

June 2012

1. Executive Summary

Can we imagine our lives without surfing on the web or using our mobile phone? It is likely that the rapid rollout of Machine to Machine (M2M) technologies will also change our lives in the near future, paving the way for the deployment of the Internet of Things (IoT). As technologies can exceed consumers' expectations, new challenges are rising, and security and privacy issues are growing.

Eurosmart has already spotted several major security vulnerabilities and privacy breaches with M2M and IoT; they are highlighted in this document through different use cases. With more than 20 years of experience, our association is also in a position to provide useful recommendations to overcome those risks.
As in many new technologies, it is always better to have a proactive approach and anticipate risks and vulnerabilities, rather than simply being reactive to deviations of the system. We are calling for action, now!

2. Introduction

A coffee machine that is able to order itself capsules…
A diagnostic of your car that can be done while you are driving on your holidays…
An eco-system, the so-called Smart Grid, helping us to optimise the use of energy…
A car sending an emergency call to a rescue centre without any human intervention…

This is no longer science fiction, this is reality. And behind this reality is technology known as Machine to Machine. Today, millions of machines are already communicating between themselves; but tomorrow, it will be not only machines, but also billions of objects that will directly interface with the digital word through the Internet of Things.

Government regulations and the availability of wireless data access with 3G and 4G have contributed to the take up of M2M eco-systems and are now paving the way for Internet of Things. As there is generally no limit for imagination, M2M is already covering a wide range of applications including automotive, fleet management, energy & utility, health, etc. Tomorrow, the IoT will address an even wider range of applications.

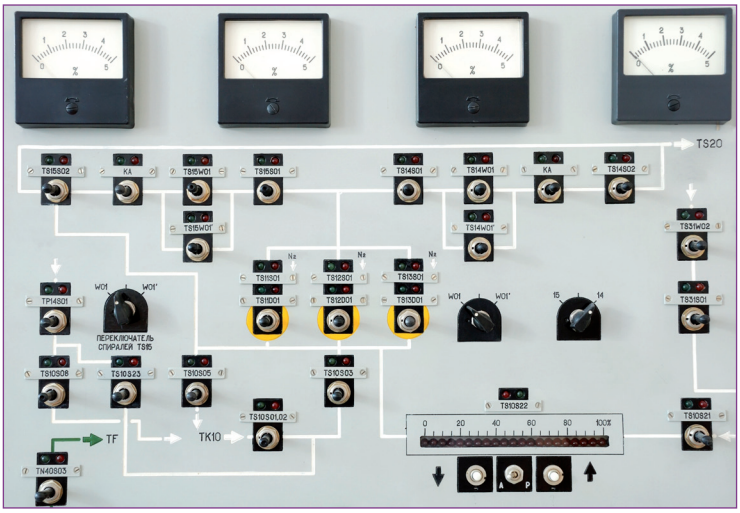
While M2M and IoT technologies mean more convenience, there is also a real need to ensure that this rapid development will not take place at the expense of security and privacy. And as for many other new technologies, standardisation will be a key driver to accelerate the success of M2M and IoT deployments.

3. Risks and Vulnerabilities

3.1 High Level Risks and Vulnerabilities

As more and more digital applications roll out, fraudsters and criminals are actively seeking ways of attacking systems. When this is related to objects used in our daily lives, those attacks can have huge effects, both for end users and for system operators. In 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.[1]

Can we accept that someone takes the control of a nuclear plant through an electricity smart meter network?
What will be the benefit of the e-call initiative if, at the end of the day, we are not absolutely sure about the identification of the car emitting the call?



Above identification issues, government and authorities have the responsibility to protect citizens' privacy. With a sophisticated M2M network, it will be easy for outsiders to obtain information about our private life at home. Will end users accept to have their intimacy disclosed so widely?

Finally, we also learned from the Internet that without considering proper regulations at the early stage of deployment, there will be huge difficulties re-establishing rules that can be applied on a worldwide basis.

3.2. Technical environment

Smart M2M or IoT applications require different quality and security than traditional smart devices due to their demanding physical environment.

For instance, the M2M hostile environment (outdoor, integrated in complex machines, tough atmospheric conditions, etc.) means that the smart device must be able to cope with:

- Temperature;
- Vibration and overall physical stress;
- Electrical environment;
- Accessibility and therefore material lifetime;
- Tamper resistance.

In concrete terms, a SIM card was originally developed and manufactured for integration in a mobile phone, not in a machine. A standardised M2M identification module (MIM) has been specifically developed for this purpose. In addition to constraints issued from physical environment, we need to consider requirements due to form factors (including size of module in some specific vertical) for seamless integration in most of electronic and communicating appliances.

[1] Oberhur Technologies

Initially, M2M market emergence was based on wireless communications when new developments and obviously IoT would use all available and relevant communication technologies and protocols. Our Smart Security Industry is today able to provide proven and industrialised technologies and products for those new applications. In M2M or IoT, the smart device is a secure component of a secure chain. The Machine or Object networks need to be secure as any electronic transaction. Technical requirements are specific but our smart technologies will apply.

3.3 Definitions of M2M and IoT

At Eurosmart, we have been working for 20 years on digital security. We gave a definition of the Smart Secure Device: “A smart secure device is a device that contains a tamper-resistant microcontroller and software for authentication, confidentiality and non-repudiation. It also supports personalisation by the issuer, and not by the user”.

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

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

IoT is based on the same concept as M2M; the main difference is that M2M generally works in a closed environment while IoT is much more open and connected to the web.

4. Uses Cases: Examples of Risks

4.1 Fraud infrastructure

M2M applications are now opening the door to a new hacker community. Consequently, it is vital today to reduce the risk of fraud in such a way as to ensure customer benefits and create a solid business model.
In the smart metering market, for example, the new meters will not be checked physically; therefore the current tamper evidence is no longer a barrier.

Below are a few examples of risks related to fraud infrastructure:

- In Australia, a woman was jailed for using a stolen SIM card in an electricity meter to download $200,000 worth of data from the Internet. New technologies integrated into a device and connected to the Internet need to have a physical and logical security solution to avoid massive fraud.

- In Canada, BC Hydro has launched a programme to reduce electricity theft that currently amounts to approximately $100 million a year in lost revenue[2].

- Researchers at the University of California have found that cars that are built to be compatible with Bluetooth have a potential to be hacked using that connection and some code can even be “snuck in” on a MP3 file.

Physical and logical access need to be secured, and unauthorized access must be identified on time.

4.2 Infrastructure attacks

Protecting M2M solutions against large scale attacks is an absolute necessity for countries. This is why some national authorities such as the BSI[3] are going to propose a dedicated protection profile.

Below are a few examples of risks related to infrastructure attacks:

- The War Texting attacks using SMS and text messaging to attack M2M devices is a good example of the threat that the M2M market is facing today. It has become easy and cheap to hack a network infrastructure even in such a way to stop the car or to modify devices behaviour’s to impact the safety of the vehicle.
- The Stuxnet worm discovered in July 2010 was the first attacks on nuclear software. In other words, it is now becoming possible to endanger - or even kill - people, using internet access.

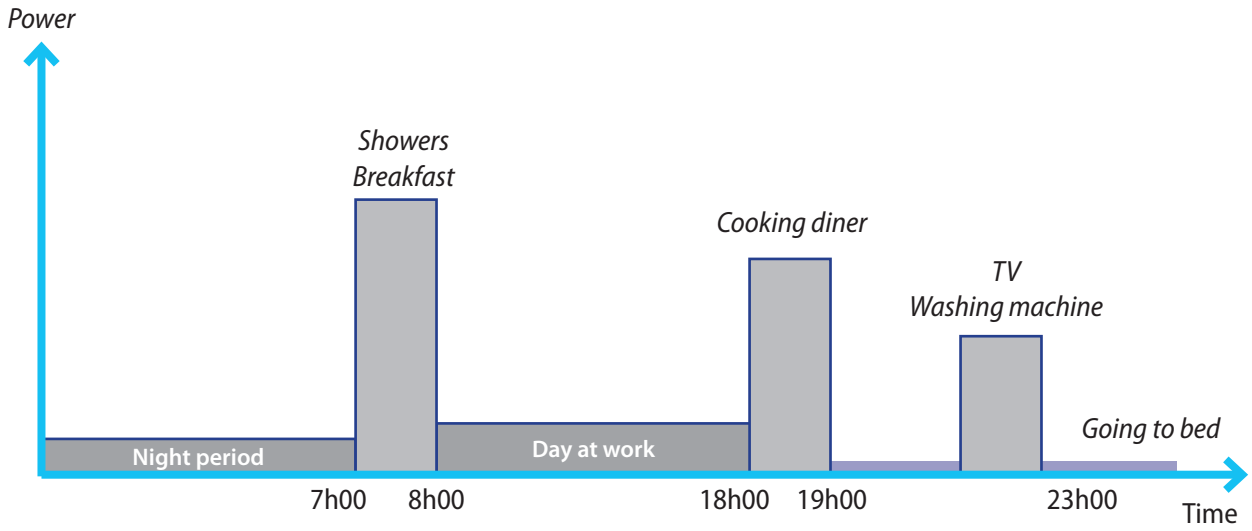
4.3 Privacy breaches

Objects collecting, storing and transmitting information can, in many cases, reveal information about individuals that may be used to derive habits, interests and other information. In IoT this information exchange is not generally noticed by the individual because it is not the human who initiates the communication but the machine. In many cases, people are therefore unaware about this information exchange over a long period of time.

[2] http://www.bchydro.com/etc/medialib/internet/documents/smi/smi_business_case.Par.0001.File.smi_business_case.pdf

[3] Bundesamt For Sicherheit in der Informationtechnnik
The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry.

Various interests can motivate the misuse of private information and danger is imminent that fundamental human rights may occur, or that other serious damage takes place. In smart metering, power consumption will be measured every 15 minutes or even more often. Measurement with such high time accuracy can be misused for profiling. Not only can this reveal whether someone is at home but also what electric devices - coffee machine, washing machine, etc. - she or he is using, and at what moment in time.



Source: Andres Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin. Private Memoirs of a Smart Meter

Privacy and the need for trustworthy Communication

Deployment of IoT will, in some cases, be mandated or encouraged by governments. For example the deployment of smart meter infrastructure is enforced in some countries because it is a crucial technology needed to use energy from regenerative resources at a large scale. As can be seen from the example above there are some serious fears concerning privacy which must be addressed by governments.

Adequate communication with the population is needed to teach people about the benefits of the technology and to finally gain acceptance. Solid privacy protection is a critical requirement. Governments must convey in a trustworthy manner that serious measures are in place to achieve this obligation.

4.4 Lack of regulations, consumer lack of protection

The M2M market is currently fragmented. The global volume is based on several vertical applications in many countries with niche-based or national specifications. The emergence of the IoT market will go through standardisation and then interoperability between the compliant products and solutions.

The vision of communicating smart objects in billions of units will be possible only with standardisation. Beyond professional applications, the consumer market will demand convenience and seamless technology inclusion.

The IoT needs strong security and attached interoperability.

The Smart Security Industry now provides solutions, but this new Internet development requires regulations, possibly at the EU level, to foster innovation, and ensure harmonisation and a level-playing field for all actors of these promising technologies. This will be the foundation for standardisation and innovation which are necessary to a secure and private environment.

5. Recommendations

Eurosmart is calling for 4 main actions to prevent risks on security and privacy and foster the development of M2M and IoT technologies.

5.1 Supporting research in enhanced security technologies

Europe is currently leading in smart device technologies[4]. However, to keep this position, research into ways of handling the increasing complexity of distributed systems from the security perspective is required. This research must examine and aid in the development of the new security functionalities of cost-effective, and tamper-resistant smart devices, and the development of (formal) methods for designing security and privacy into complex and interdependent systems.

The EU, research institutes and the industry should contribute jointly to these research topics, through European R&D funding.

5.2 Deeper analysing security requirements

For the different stages of the IoT, an effective security strategy requires a holistic approach considering the interactions between the different systems and the impacts on systems in case of security breaches in other systems. Due to the need for a comprehensive approach, the European Commission and the ENISA (European Network and Information Security Agency) should be responsible for these activities and encourage Member States in this way: a list of the main use cases of the IoT should be identified and the system interactions and behaviours should be understood. Risk assessments should be conducted for the use cases by identifying assets, vulnerabilities, and threats; specifying the potential impacts.

Numerous actors will capture, transmit, store, edit, and process the information necessary for the use cases.

[4] Top 4 companies are based in Europe: Gemalto, Oberthur, Giesecke & Devrient, Morpho, Oberthur Technologies.

For the interfaces linking actors and transmitting information, the impact of an equipment failure, intrusion, and other security threats can be evaluated for:

Loss of confidentiality — the unauthorised disclosure of information;
Loss of integrity — the unauthorised modification of information; and
Loss of availability — the disruption of access to an information system.

Once this evaluation is made, security requirements such as Access Control, Identification and Authentication, Secure Communication, Audit and Accountability, and Personnel Security can be applied to particular interfaces and corresponding IT products.

5.3 Assuring security with certifications

To ensure an appropriate security level in the IoT from the beginning, regulations need to provide and enforce the corresponding requirements.

Common Criteria Protection Profiles are an established way to define security requirements for IT products. For example, with, the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, protection profiles were defined for IT products used in electronic signature systems.

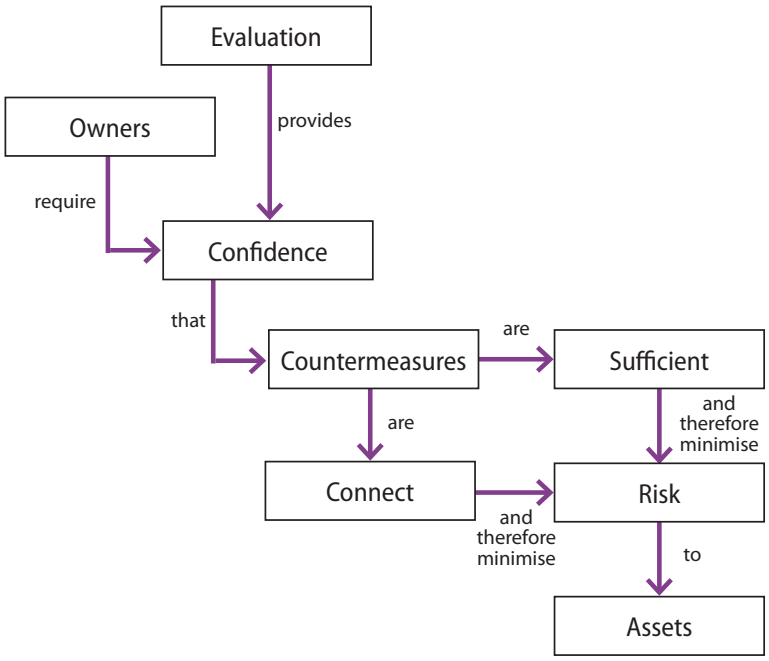
“Protection Profiles” is a description of security needs that can be defined by a regulatory entity. These protection profiles can then be used as part of a regulation, which will only allow specific types of IT products to be used if they meet the corresponding protection profiles. Protection Profiles define the security problem by showing the threats, organisational security policies and assumptions. The protection profile then shows the solution to the security problem by defining security objectives which are translated in requirements for security functionality provided by the IT products and assurance measures applied to these IT products during a security evaluation.

Solid and mandated privacy requirements are also documented in the protection profile, which thereby allows examination of trustworthy third parties. For example the protection profile may mandate anonymity of users, unlink ability of operations, or concentration of specific privacy related data. This method thereby adds a great deal of transparency about the respective measures to protect privacy.

Additionally mandating this procedure demonstrates that the government is not only demanding privacy protection measures, but also actively controlling their proper implementation, thus taking privacy protection seriously.

In Common Criteria security evaluations, the manufacturer must demonstrate that the IT product conforms with the requirements of the protection profile.

An evaluation body verifies, among other things, that the IT product provides the required security functionality, that the development and production site are secure, and that the development process and IT infrastructure are secure. Furthermore, the evaluation body will apply state of the art attacks on the IT product.



The increasing amount of certifications required for the expected amount of different IT products contributing to the security of the IoT means it will be necessary to increase the staff of certification bodies, so as not to hinder a dynamic evolution of the IoT.

Furthermore, it will be necessary to further develop the certification requirements of the Common Criteria to enable the handling of dynamic changing IoT devices, demanding prompt updates due to security incidents, evolving threats and new functional requirements.

5.4 Promoting the integration of smart devices

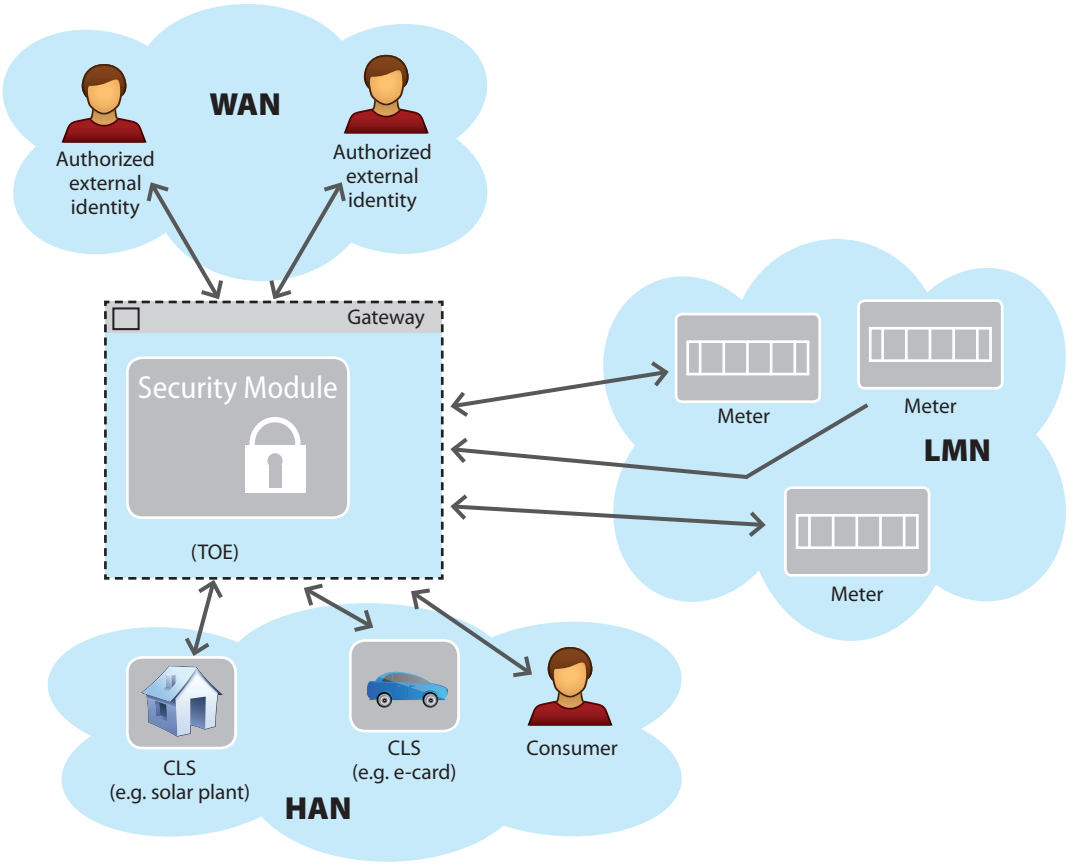
The industry behind EUROSMART has a long experience in offering products (Smart Secure Devices) that provide high security functionality for such things as payment systems, border control, signature creation and mobile communication. Such smart devices store (in a tamper-resistant microcontroller) cryptographic keys, software and other assets such as personal biometric data. The software running on the tamper-resistant microcontroller provides the security functionality for such applications as access control, confidential communication, and data integrity protection.

Smart Devices provide high security at very low cost and are optimally suited to be integrated as secure elements into IoT devices. The established manufacturers offering these smart devices are highly experienced in demonstrating the security of such devices with the international standardised Common Criteria Security Certifications.

On the other hand, for the emerging industry, providing solutions and products for IoT, high security requirements and passing high security certifications will probably be a challenge. By integrating smart devices in the architecture of IoT products and systems, they can gain a high security level, where the security functionality is mainly provided by the smart devices and therefore the security requirements on the remaining system can be more easily fulfilled by the emerging industry for IoT.

5.5 Example of what can be done: the German smart metering gateway

A good example of introducing a comparable system and corresponding devices with smart devices as secure elements is the introduction of smart metering systems in Germany.



In this architecture, the smart device is responsible for the verification of the authenticity of communication partners in the Wide Area Network, Local Metrological Network and the Home Area Network; proving the authenticity of the gateway to these communication partners; securing the communication with them; and securely storing the cryptographic keys and certificates.

Depending on the use case, a decision needs to be made as to which security functionality should be provided by the smart device to an IoT device. The security requirements and the functional requirements were developed by the responsible governmental agencies and the industry contributing to this work.

The security requirements were defined in a protection profile for the smart meter gateway and in a protection profile for the smart device working as the secure element in the gateway. The requirements for the certification of the gateway could be lowered due to the usage of the secure element.

Future secure elements providing even more security functionality to IoT devices would allow for even more reduction of the certification requirements for the IoT devices.

6. Benefits

6.1 Benefits for citizens, consumers and businesses

The exciting development of digital technologies will enable more features and more convenience, making our lives easier, simpler and safer. In addition to changing our lives, there is also an expectation from consumers and citizens to facilitate their interaction with this digital world by providing:

- A good balance between convenience and security;
- More information and guarantees about privacy;
- More standardisation.

M2M and IoT technologies will save human lives, help companies to be more competitive, open new business opportunities and will make our world safer and simpler. These technologies will be fully accepted by consumers, citizens and enterprises if they are giving more assurance that these benefits will not come at the cost of their security and privacy.

6.2 Perspectives, innovation

IoT will challenge our industry ability to innovate and consider a dramatic variety of devices, functionalities, communication environment and electronic resources. We recommend, for instance, the highlighting of the biometry of objects such as PUF[5]. The European Smart Security Industry, including academics together with European authorities and users representations shall build the framework for IoT security and success.

Success necessitates some regulation, and the assessing of security needs and citizen rights in IoT applications or in private and public services.

Without this necessary framework, Europe's smart industry may not lead the way in innovation, leaving the door open to non-European organisations and less secure solutions.

6.3 Cross industries

The Internet of Things covers many and various industries (Smart Security, Consumer Electronics, Smart Grid, Safety, etc.) and a strong political incentive is required to define and implement security transversal standards or requirements.

As already explained in this document, the European Commission and other EU institutions should call for a security element in each electronic device that could interact in any IoT transaction.

[5] Physical Unclonable Function or PUF is a function that is embodied in a physical structure and is easy to evaluate but hard to predict

7. Call for Actions

There will be more security challenges when deploying M2M and IoT technologies compared to human to machine technologies, such as payment with a credit card:

- Security is not always well understood and this will not improve in a system based on a very complex value chain;
- Since M2M and IoT 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.

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 these challenges; but it is equally important that EU and national authorities take initiatives to protect citizens and enterprises against increasing risks on security and privacy:

- Encouraging certifications and standardization;
- Supporting the integration of smart devices;
- Ensuring Europe will keep its leadership in security R&D.

The Smart Security Industry has more than 20 years’ experience in creating an equilibrium between convenience, privacy and security. It can help authorities in finding where the right balance is and how to implement the right technologies including security technologies to protect people and data.

We have to act now!

8. Glossary

- M2M: Machine to Machine
- IoT: Internet of Things
- E-call: emergency call
- MIM: M2M identification module
- PUF: Physical Unknown Function

Authors

Marc Bertin
Jerôme Chancel
Jean-Pierre Delesse
Martin Klimke
Dirk Wacker

About 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, developing Smart Security standards and continuously improving quality of security applications.

Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers who work into dedicated working groups (communication, marketing, security, electronic identity).

Members are largely involved in research and development projects at the European and international levels.

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

Eurosmart members are companies (Austria Card, EM Electronic Marin, FNMT-RCM, Gemalto, Giesecke & Devrient, Infineon Technologies, Inside Secure, LFoundry, Morpho, NedCard, NXP Semiconductors, Oberthur Technologies, Prooftag, Renesas Electronics, Samsung, STMicroelectronics, Toshiba), payment systems (GIE Cartes Bancaires, Mastercard), laboratories (CEA-LETI), research organisations (Fraunhofer AISEC), associations (Smart Payment Association, Mobismart, Danish Biometrics) and independent experts (Michel Koenig, Jonas Andersson).

EUROSMART
The Voice of the Smart Security Industry

Contact us:

EUROSMART
Rue du Luxembourg 19-21
B-1000 Brussels
Tel. (+32) 2 506 88 38
Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com
Visit our website www.eurosmart.com