European Commission
Information Society and Media

SEVENTH FRAMEWORK PROGRAMME

Large Scale Integrating Project

EXALTED

Expanding LTE for Devices

FP7 Contract Number: 258512

WP6 – Device Improvement

D6.4
Demonstrator prototyping the mechanism into an M2M module

Contractual Date of Delivery to the CEC:	31/08/2012
Actual Date of Delivery to the CEC:	12/10/2012
Responsible Beneficiary:	GTO
Contributing Beneficiaries:	GTO, SWIR, UNIS, UPRC
Estimated Person Months:	18
Security:	Public
Nature	Report
Version:	1.0

Document Information

Document ID:	EXALTED_WP6_D6.4
Version Date:	2012
Total Number of Pages:	27
Abstract	This deliverable defines the prototype hardware demonstrator, software user's guide and hi-level architecture for the secure device mechanism implementation
Keywords	M2M, Secure Element, LTE-M, Pairing, Device improvement

Authors

Name	Organisation	Email
Matthieu ANTOINE (editor)	GTO	matthieu.antoine@gemalto.com
Jerome d'ANNOVILLE	GTO	jerome.d-annoville@gemalto.com
Bruno CORLAY	SWIR	bcorlay@sierrawireless.com

Approvals

	Name	Organisation	Date	Visa
Internal Reviewer 1	Petros BITHAS	UPRC	12/10/2012	OK
Technical Manager	Pirabakaran NAVARATNAM	UNIS	12/10/2012	OK
Project Manager	Djelal RAOUF	SWIR	12/10/2012	OK

Executive Summary

This deliverable is built around three main items: an exercise in combining the results of the device improvement work package in a single device, a detailed specification of the Secure Element (SE) and a presentation of the pairing mechanism used in EXALTED.

The first part of the document consists in an exercise that leverages the results of different work items in the device improvement work package with a particular interest in the areas of energy efficiency, device reliability and device security. The system described here takes advantage of several results of the EXALTED project such as the SE providing device security, the local Self Diagnostic Manager (SDM) providing reliability at device and network of devices levels and, finally, an energy consumption equalization algorithm that provides energy efficiency in a group of devices.

The second part of the document appears in the form of a companion specification to the SE designed and prototyped in the EXALTED device improvement work package (WP6). The new SE is intended to fulfil the critical tasks in the critical area of M2M device security as well as the energy efficiency and low cost concerns indentified by the EXALTED project as key requirements in the M2M market. This SE specification is twofold addressing both hardware and software aspects. The hardware part details the overall design of the SE as well as the electrical characteristics needed for hardware integration (for instance in the EXALTED test beds prototyping work package, WP7). The software part covers the communication protocol between the host system and the SE over SPI as well as a description of SE hosted application which is similar to java applets. Overall, the SE is functionally very similar to a SIM card in terms of the secure services it provides, the essential difference besides the new form factors resides in the SE supporting hardened environmental conditions as requested by demanding industrial applications.

The third part of the document deals with the different pairing mechanisms which can be implemented in the three chosen use cases. Each of the three use cases presents really different constraints which can be overcome by selecting the right pairing. Each scenario can be split up into three levels of security which intends to ease the choice of pairing:

- Within an M2M device, between the SE and the host microcontroller
- Within a capillary network, to manage access rights
- Within the whole architecture, to ensure E2E security

Table of Contents

Table of figures

Introduction

Driven by the trends of ubiquitous connectivity to the Internet and an ever growing number of connected equipments, the EXALTED project intends to provide solutions into key areas of M2M communications. Introducing an end-to-end system concept for M2M communications over LTE, EXALTED also looks into device improvement with a particular interest in the energy efficiency of the device, device reliability and device security. While these objectives are shared by the different work packages in EXALTED, the device improvement work package was specifically involved in addressing them.

The previous deliverables in the work package addressed these objectives separately (see [12], [13] and [14]), this document will take a slightly different approach. A first section in the document is dedicated to a collective exercise: combining the work package results in the areas of energy efficiency, device reliability and device security in a single device in order to demonstrate the cumulative benefits for networks of M2M devices.

In a second section, the document will focus on the last main requirement in the device improvement work package: device security. M2M devices show a great diversity in the service capabilities they support leading to different requirements regarding security. Some devices may be capable of mobile network access thus requiring a SIM card to do so but many others never will (devices connecting through ZigBee, Bluetooth, Wi-Fi, etc) and, security wise, may only need access to basic yet robust services. This is what the Machine Identity Module (MIM) designed in EXALTED does: providing a streamlined set of security services that fits shared requirements among M2M devices (key storage, challenge resolution, etc). When compared to a SIM card, the MIM appears more like an elementary yet key component in the device's security scheme or in the M2M application's, and brings a flexibility that fits the wide variety in M2M design. Besides the specifications of the MIM available in the further sections of this document, prototyping the chipset was also an important part of the deliverable. Both the specifications and the chipset and intended to find their ways into the EXALTED test beds of the integration and proof of concepts work package (see [15]).

The document finally presents in section 3 the different pairing mechanisms which can be set up in the three chosen use cases. They are, in a first time, described in a theoretical way to be then correlated with the use cases.

1 M2M device improvement

Besides the M2M device security detailed in this deliverable, the “device improvement” initiative within the EXALTED project produced several results at different levels such as energy efficient M2M device communications, energy-efficient operating systems and M2M device reliability. In this section, we will combine some of these results in a device participating into a M2M network in order to fulfil the device integrity objective and to show how it could be extended to network of devices integrity. This exercise intends to show how these separate results can stack up and benefit a typical M2M device and, more specifically, networks of M2M devices.

Three work items are at stake here:

- The virtual network of M2M device self diagnostic module as depicted in section 1.1 (more details are available in the EXALTED deliverable D6.3 [14]) enables claiming network integrity statements
- Energy equalization algorithm applied to a capillary network of devices as depicted in section 1.2 (more details are available in the EXALTED deliverable D6.2 [13]) provides dynamic communication routes that optimize energy consumption at the network level
- Device security as depicted in this deliverable provides key security services for the device

Implementation-wise, the results of the energy efficiency optimization of a Linux kernel in the EXALTED deliverable D6.1 [12] could also be considered as a valuable addition to this combination of different results of the device improvement work package in EXALTED.

1.1 Diagnostics of networks of M2M devices

In D6.3 [14], the EXALTED project described a mechanism for device self diagnostics. This mechanism was described as a key building block in the definition of a “larger” network diagnostic service involving a virtual network of interconnected self diagnostic modules.

1.1.1 Device self diagnostics

At the core of the mechanism described in the EXALTED deliverable D6.3 [14] is the self diagnostic module (SDM), a software entity that runs in the device and acts as a local diagnostics for a variety of local or remote diagnostic clients. The SDM applies a set of logically and hierarchically connected rules to a set of Managed Objects (MOs) representing a context for the device in order to produce a diagnostic result. Eventually, this result is evaluated against a set of predefined reactions the SDM can trigger (sending notifications to clients, initiating healing procedures, etc).

At the expense of a locally increased workload in order to produce the diagnostics, it reduces the reliance on the communication link (only the initial diagnostic request and the diagnostic answer are transmitted) and enables better communication efficiency when compared to a standard device context exposition associated with a remote diagnostic production such as OMA’s DM DiagMon [17]. It is interesting to note that this offloaded workload submits very well to process scaling mechanisms such as those described in the EXALTED deliverable D6.1 [12] especially when the M2M application is delay tolerant.

The nature of the SDM client to SDM server communication path implies strong security requirements especially in the areas of mutual client and server authentication and authorization to access internal resources that may be submitted to privacy concerns. In the

EXALTED device, the SE provides such security services as well as application hosting service. Such applications are possible SDM clients. Their access to critical or private information could be conditioned to the current status of the device integrity. Integrity-oriented rules used for self-diagnostics could provide this criterion for granted resource access.

1.1.2 Virtual networks of self diagnostic modules

As described in section 1.1.1, the SDM is a diagnostic server for a variety of diagnostic clients. D6.3 [14] went a bit further and developed an extension to this client to SDM server concept considering that a SDM could be a client for another SDM and that the diagnostic resulting from the latter could be combined to a local diagnostic in order to represent a diagnostics that covers both devices.

Chaining client SDMs and server SDMs connected over a network of devices enables to produce a network diagnostic addressing only the entry point of the virtual network of interconnected SDMs. The diagnostics requests will spread from SDM clients to connected SDM servers until the edges of the virtual network of SDMs are reached and diagnostic results are returned to their respective requesters. Each SDM client to SDM server connection only “suffers” a single request/answer transaction which reduces risks of overused paths and energy depletion of overused nodes equalizing the diagnostic traffic when compared to a network diagnostic mechanism that would address each device individually.

The communication link that connects to the entry point of the device network (typically the LTE-M radio link the EXALTED project describes in the corresponding work package) also greatly benefits from this virtual network of connected SDMs as it is also only addressed with a single network diagnostic request/answer transaction and doesn’t have to support the whole diagnostic traffic resulting from individual addressing.

Figure 1-1 and Figure 1-2 illustrate the differences between an individually addressed diagnostic scheme and a virtual network of SDMs. In Figure 1-1, devices A, B, C and D form a capillary network of M2M devices. B, C and D are non LTE-M devices while A is LTE-M capable and acts as an entry node to this network of devices. Each devices is addressed individually which is illustrated by the LTE-M link supporting all of the resulting diagnostic request/diagnostic answer traffic.

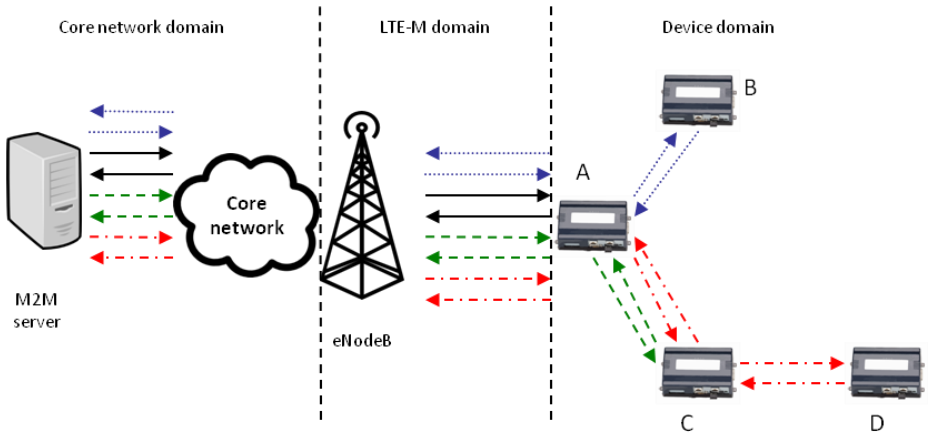

Figure 1-1: individually addressing the status of a capillary network of devices

In Figure 1-2, the balancing benefit of virtual networks of SDMs over individual diagnostic clearly appears in the amount of diagnostic traffic supported by the LTE-M link between the eNodeB and the LTE-M capable device A. The radio path between device A and device C also illustrates diagnostic traffic balance within the capillary network.

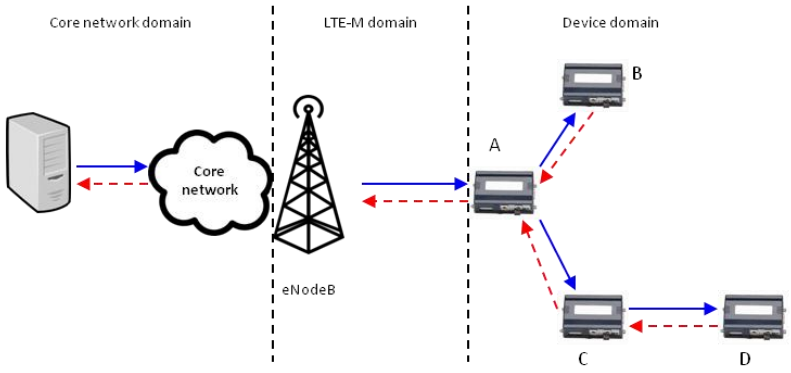

Figure 1-2: Addressing device network status via EXALTED's virtual network of SDMs

As the virtual network of SDMs relies on the routes of the physical network of devices, it is expected to support dynamic reconfiguration so it can apply to self organized networks of devices too. For instance, dynamic SDM reconfiguration is expected to support the network route reconfiguration algorithms motivated by energy efficiency described in section 1.2 and the EXALTED deliverable D6.2 [13].

1.2 Energy equalization at forwarding node level in a multi-hop M2M network

The typical M2M application as described in EXALTED involves collection of data regularly or instantaneously by a large number of measurement devices constrained in cost, power processing or power supply. Such constraints raise limitations on the communication schemes to be applied between data collecting devices and data processing systems, individual direct connectivity could be excluded in favour of a multi-hop communication scheme between the data producing device and the gateway. Such an architecture fits in the larger picture described by the EXALTED system architecture in deliverable D2.3 [7] and in Figure 1-3.

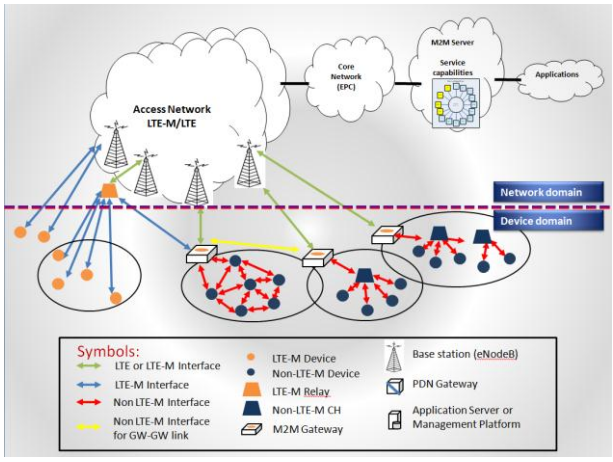

Figure 1-3: The EXALTED system architecture

Yet, a capillary network of M2M devices built upon a large or very large number of devices connected to a gateway via a multi-hop communication scheme raises severe concerns regarding data congestion at data forwarding nodes. Each device may transmit few amounts of data yet a large number of them transmitting simultaneously could result in a high traffic load on the forwarding nodes where the data flows merge. These nodes are described as network hotspots, locations were the heavy burden leads to early depletion of energy resources. Among other means to reach better energy efficiency, the EXALTED deliverables D6.2 [13], D4.3 [9] and D4.4 [10] describe an algorithm that tackles this imbalance in the energy consumption rate at node level in the capillary network of M2M devices. This algorithm favours energy consumption equalization in the device network applying different strategies: MAC level measures, routing level measures such as best forwarding node selection, Cluster Head (CH) selection and scheduling of individual traffics in order to ensure equalized traffic on forwarding nodes.

1.3 Application to network of M2M devices

The device improvement work package brought various solutions in order to fulfil its objectives and, while covering very different aspects of the device, these solutions are not completely disconnected, they can stack up to reach and extend the work package's objectives. Here, we will have an illustration of how some results can be combined and completed very efficiently. For example, using mechanisms such as the SE, the device self diagnostic (see section 1.1) and an energy-efficient multi-hop communication scheme (see section 1.2) it is possible to build a secure, energy efficient and reliable network of M2M devices.

Stating the obvious, the SE appears as a key component for the security aspects granting authentication and authorization to the diagnostics part of the device integrity decision process. Network integrity will rely on the virtual network of SDMs, each SDM bringing its integrity status contribution to build a network integrity status. Additionally, at a very basic level, the SDM client to SDM server connections necessary to setup the virtual network of SDMs are enabled by a mutual authentication service provided by local SEs. More services such as ciphering could also be involved to ensure diagnostic traffic privacy if required.

The virtual network of SDMs produces the network integrity status with the mechanism described in section 1.1.2. Yet, this virtual network remains submitted to the reality of the physical connections between the nodes of the capillary network. The diagnostic traffic remains balanced in a single SDM client to SDM server connection as long as the configuration of the virtual network remains stable but if a client is connected to several servers, the workload of the client will increase with the number of connections and its energy resources will deplete at a quicker rate than the servers' own resources. Energy consumption equalization then becomes necessary in order to reach better overall energy efficiency in the network of devices. As the diagnostic traffic blends in the general data traffic, it will benefit from the application of the algorithm described in section 1.2. This algorithm will drive the network route reconfigurations with an energy efficiency objective in mind which will naturally solve the imbalanced depletion problem generated by the combination of measurement data traffic and diagnostic traffic.

The end result is a network of devices that is secured thanks to the SEs stored into each device in the network. Its reliability is handled by a virtual network of individual SDMs while a network route reconfiguration scheme ensures energy consumption equalization hence a longer operational interval. This example could be enhanced on a per device level at implementation stage looking into local optimizations as suggested in D6.1 [12] for a Linux based system or in D6.2 [13] for a selection of MAC protocols.

2 Secure element

2.1 Presentation and objectives

Three scenarios are chosen to demonstrate the purpose of EXALTED in the most significant and illustrative way. These entire scenarios are defined in D2.1 [6]:

- **Intelligent Transport System** (ITS): communication of vehicles and transport infrastructure with ITS application servers, which controls parameters such as transportation time, traffic collision avoidance, on-board safety, fuel consumption, and many others
- **Smart Metering and Monitoring** (SMM)**:** very applicable use case of industrial, environmental, energy, and other types of monitoring
- **E-healthcare**: a relationship between a healthcare organization and a patient, established through the M2M communication

Security is a mandatory requirement in all scenarios, as explained in the chapter dedicated to technical requirements in D2.1 [6] (functional and service requirements). As stated here [5] in the public project presentation, *"the aim of WP6 is to provide specification for efficient M2M devices"* targetting the following high-level objectives: **energy-efficiency** (O6.1), **reliability** (O6.2) and **security** (O6.3).

The SE is the deliverable proposed by EXALTED intending, within the WP6, to release a prototype of demonstrator for an energy-efficient, reliable and secure mechanism into a M2M device. The mechanism demonstrated here is the way to handle the application layer security in a M2M device.

In general, security is the condition of not being threatened where a threat is defined as any possible event or sequence of actions that might lead to a violation of one or more security goals. These goals are defined as follows:

- **Confidentiality**: information should only be revealed to an authorized audience
- **Data integrity**: any modification of data should be identifiable or detectable
- **Accountability**: it should be possible to identify the entity which triggers an event
- **Availability**: resources should be available and operate properly
- **Controlled access**: only authorized entities should be able to access a resource

The development of a new system often puts the security aside. The main reason is that its implementation is really complex and makes the development harder. Security must have its whole place in the design from the beginning.

The main purpose of the SE is to bring a plug-and-play security toolbox which brings a real added-value in a M2M device without complicating its development. It is made possible by offering a peripheral accessible through a set of APIs.

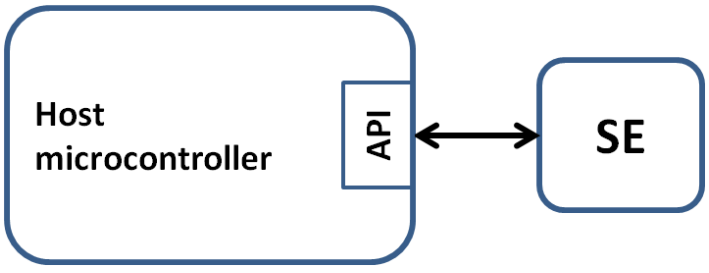

Figure 2-1: Host microcontroller vs. SE

The Figure 2-2, extracted from D7.2 [15], describes where the SE takes place in M2M devices. The terminology equivalence defined in D2.3 [7] tells precisely that “M2M devices” stands for “LTE-M and Non-LTE-M devices”.

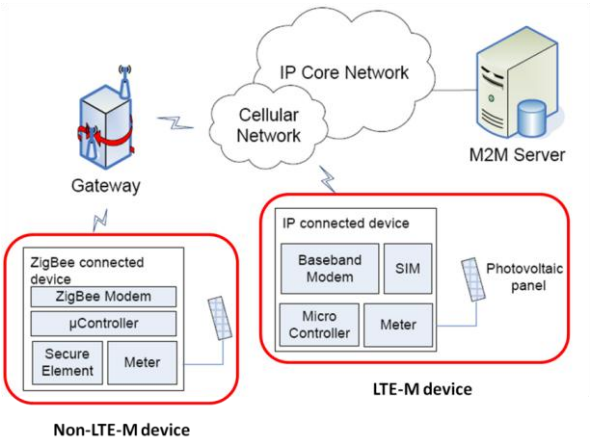

Figure 2-2: Sub test bed 2.4 components

Concerning the application layer security in LTE-M devices, we can have two different approaches. The first one is based on the SIM availability. D5.1 [11] and D2.3 [7] stand up for the idea to embed this application layer security in the current SIM.

The second approach is based on the possibility to meet several issues:

- The MNO does not accept to add this feature in the SIM
- The owner of the device wishes to switch to another MNO (discussed in D5.1 [11])
- Costs related to deploy the feature in the SIM are higher than using the SE

The SE can be here a valuable alternative to physically separate the two functions (network authentication and application layer security).

For Non-LTE-M devices, there is no need to access the cellular network so no SIM is available. The SE is then mandatory to implement the application layer security.

The SE is a peripheral in the EXALTED architecture which brings an optional feature, as explained in D2.3 [7] (“(...) *flexible security layer must enable applications to protect their data according to the security requirements. This feature is optional. Applications may decide to protect against unsolicited data modifications thanks to the integrity mechanism provided by the security layer or to use ciphering to protect the confidentiality of the data (...)*”). This point of view is also discussed in D5.1 [11]: “*(...) unless carefully managed, secure storage of keys drops to the “lowest common denominator” in a capillary network, which may discourage parties who wish to supply devices with SEs from doing so, or it may deter customers from buying capillary devices with SEs (Why bother, if there is no security gain?)*”. Although it is presented as optional, EXALTED brings the proof that security is an integral part of its architecture and system concept success.

Concerning the Key Performance Indicators (KPIs), we can rely on D7.2 [15], “*KPIs were identified in order to capture the wide range of the project's objectives, to serve as the basis for the assessment of the candidate technologies, techniques and system concept and to quantify their impact on the overall performance of the EXALTED system*”. Among all the KPIs defined, the most relevant are **K46** (Computational energy consumption) and **K49** (Flexibility of the security enrolment process for capillary devices).

2.2 Conception

2.2.1 Architecture

The choice of the SE as defined above to ensure E2E security in M2M devices fits with the statement made in D4.3 [9], where the hardware SE is described as more secure than a software-only SE, especially concerning key management.

The architecture of the SE is described in Figure 2-3:

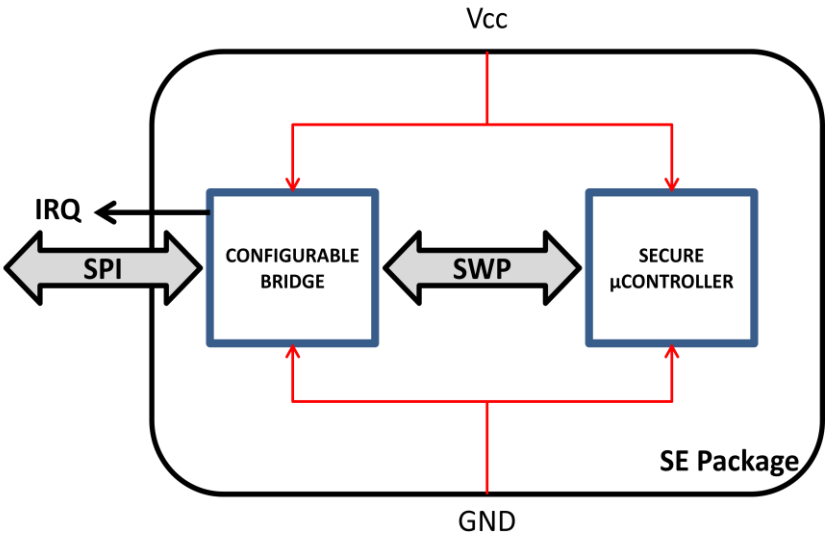

Figure 2-3: SE architecture

The choice of the embedded components in the SE was mainly driven by the key objectives defined above. These components are described in the following paragraph.

2.2.2 Components

2.2.2.1 Secure microcontroller

The secure microcontroller is based on an MIM. A MIM is the equivalent of a SIM, with specific features such that it can be used in machines and enable authentication.

In this application, the secure microcontroller is used in two ways:

- As a cryptographic toolbox to provide needed secure algorithms
- As an electronic vault to safely store keys needed by the application layer security

The communication process is based on a client / server scheme. The host microcontroller has to send a command and wait for the answer given that the secure microcontroller does not take the initiative.

The first advantage of using a secure microcontroller based on a MIM is the reliability offered by such a component. It is indeed M2M-capable and presents an extended operating condition range. That kind of device must come through really harsh conditions without threatening the application security. The reliability can also be assessed by the maturity of this technology. Secure microcontroller, as hardware / software couple, has proved itself for more than twenty years in various domains (telecommunications, banking, identity, etc.), mainly based on its tamper-proof resistance.

This secure microcontroller is also energy-efficient. This advantage comes from the fact that this chip is designed on purpose to have the lowest power consumption in operating mode. When the MIM is not used, it can be switched in a stand-by mode which decreases the power consumption to a really low level. The MIM can also be completely switched off and turned on only when needed. The low booting time makes this feature possible. The embedded software plays also a part in energy-efficiency. The software has to be highly optimized due to very constrained operating conditions (available memory, internal frequency, etc.). It results in fast code execution which is a step in the energy efficiency.

Last but not least, the secure microcontroller provides a secure execution environment. The MIM on which this component is based is a certified platform. Before accessing any embedded application, the host microcontroller needs to run an authentication scheme.

Beyond these key objectives, the secure microcontroller brings features which answer to more general requirements. Over-The-Air (OTA) update is one of the features present in the secure microcontroller which answers to a specific need expressed in D5.1 [11] and D7.2 [15]. A mechanism can indeed enables the M2M server to replace one key or more when it is necessary. This feature can also be used to update a firmware or an applet in a secure way.

As explained in D5.1 [11], "*However, one important way to add value through an SE is to observe that it typically comes personalized with a unique credential (...)*". The personalization is also a feature offered by the secure microcontroller. This personalization can occur at different stage of the lifecycle (manufacturing, deployment, etc.).

The lack of standard communication protocol (SWP is the only available communication bus) makes mandatory the use of a protocol translator, which is presented hereafter.

2.2.2.2 Configurable bridge

The configurable bridge was designed for EXALTED. The primary objective of this component is to extend SWP connectivity of the secure microcontroller through a low-cost silicon device with a very small foot print (<1,5mm²) and a low power design. The architecture is built around a dedicated 16-bit microcontroller with internal clock generator managing hardware blocks through its embedded software.

The main criterion which had to be taken into account during the conception of the SE is the choice of the communication protocol to implement between the SE and the host microcontroller. This protocol shall be an industry standard easy to interface with to ensure the highest compatibility and shall provide a high speed link. The Serial Peripheral Interface (SPI) was chosen for these two reasons.

The bridge configuration is determined by its environmental connectivity that is taken into account at the initialization of the SE and can be different at each power-up. It is made possible by the fact that the configurable bridge is a RAM based component which means that it loses its configuration each time it is turned off.

The initialization is managed from the secure microcontroller through the SWP link. At power up, a dedicated firmware is loaded into the configurable bridge using the SWP boot loader. So it is conceivable to update the firmware of the configurable bridge stored in the secure microcontroller to improve its capacities. Thanks to the

In our application, the configurable bridge is used as SPI slave / SWP master.

2.3 Application

2.3.1 Software interface

In order to base the interface of the SE on a standard to enable portability, there is running task in another work package of the project that implements the SIM Alliance Open Mobile API [3] in C Language. Only a header file (.h) is provided and still, the communication with the configurable bridge part of the SE has to be implemented in the host microcontroller. This component is depicted as the SE Communication Layer in the Figure 2-4:

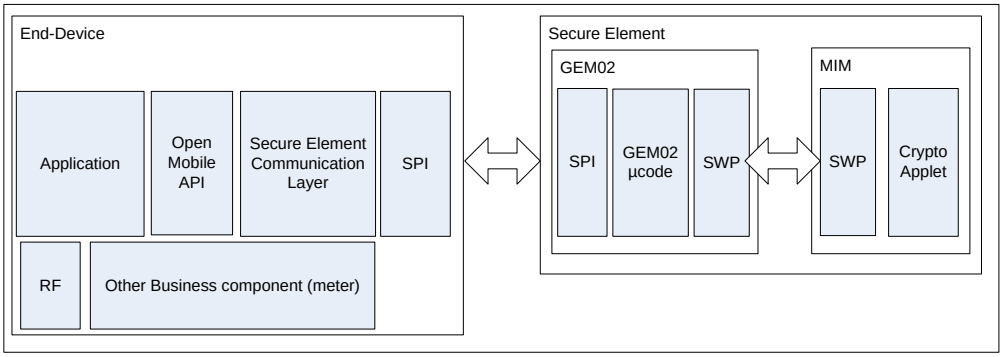

Figure 2-4: Software architecture

2.3.2 Available applets

Concerning the algorithms, only secret key-based algorithms are offered by the current release of the SE (full list of available algorithms and keys size will be published at the end of the validation phase). Public keys within certificates and private keys are not handled by this release of the crypto applet.

Thanks to the Operating System (OS) architecture, based on a Java Virtual Machine (JVM), the SE presents an interesting flexibility. The end user can easily develop an applet implementing new functions. This new applet can be send through the whole network due to the OTA update feature. The SE also offers the possibility to manage keys (storage, update, deletion). These keys can have different length, depending on the targeted application.

As described in the first chapter, the SE plays an important part of the self-diagnostic as it has to secure this mechanism. That is why the device offers the possibility to check data integrity and to guarantee diagnostic and healing operations.

2.3.3 Typical communication flow

The way to use the SE can be described as follows:

- Authentication
- Select the cryptographic applet
- Ask for a cryptographic action and get the result

Several applications may reside in the SE. This is why the application needs to select the crypto applet first. It is called *applet* because it is very similar to a Java applet even if it doesn't derive from the same class.

One "Select" command is required to select the applet. Before being allowed to use the applet, an authentication is needed. It has to start by a "Verify" to send the PIN secret value to the applet.

Once the applet is selected and the authentication is done, a “Start-Cipher” command and then several “Cipher” command according to the size of the data to process can be sent.

As explained above, the SE works in a client / server way. A typical communication flow is summarized in a high-level way in Figure 2-5:

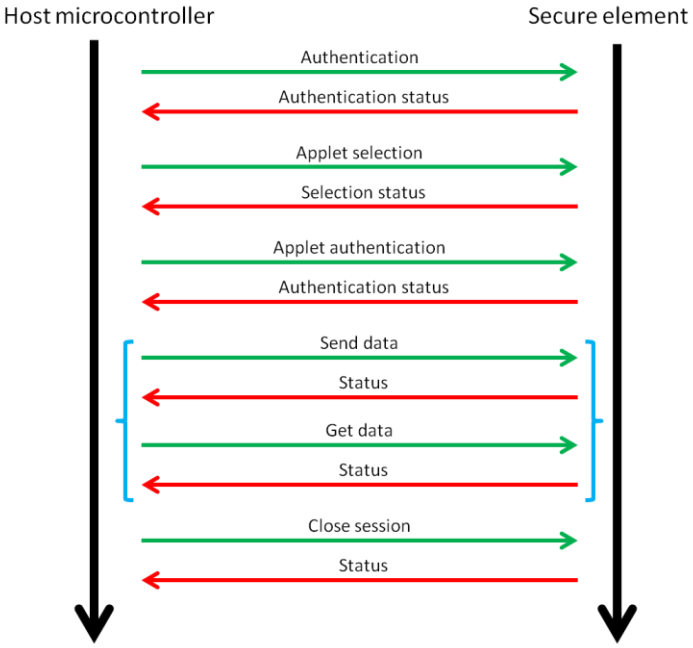

Figure 2-5: Sequence diagram

The different phases are defined as follows (This flow may have to be adapted depending on the specificities of the selected applet):

Authentication
This step is mandatory for the host microcontroller to authenticate itself to the SE. It prevents the SE to be used with another host microcontroller. This authentication is a local action which is executed each time the host microcontroller turns on the SE.

Applet selection
The host microcontroller can, through this command, select the embedded applet it wants to use (integrity check, ciphering, etc.).

Applet authentication
The distant application shall perform this authentication to have the right to use the selected applet.

Data management
The SE receives the data sent by the host microcontroller which have to be treated by the previously selected applet. The SE manages the data as blocks.

End of session
Once all the data have been processed by the SE, the host microcontroller shall close the session.

2.4 General characteristics

2.4.1 SPI communication interface

2.4.1.1 Description

This section describes the SPI interface for synchronous communication between the SE package and the host controller. The interface is based on a four-line, master/slave communication. An IRQ signal has been added to fit with the targeted client / server application. All signals are defined as follows:

- **SCLK**: Serial clock (from master to slave)
- **CS**: Chip select (from master to slave, active low)
- **MOSI**: Master Output / Slave Input (Data from master to slave)
- **MISO**: Master Input / Slave Output (Data from slave to master)
- **IRQ**: Interrupt signal (from slave to master)

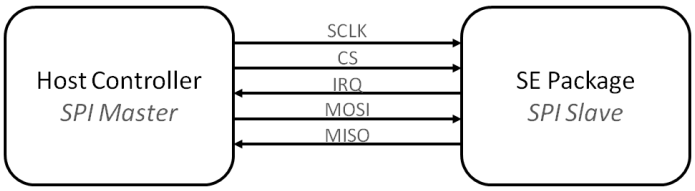

Figure 2-6: SPI bus

IRQ is a dual-purpose line:

- When the SPI bus is not busy, driving IRQ low indicates to the master that the SE Package has data to transmit
- When the master initiates a transfer by driving CS low, driving IRQ low indicates to the master that the SE Package is ready to receive data

2.4.1.2 Data modes

Four communication modes are available (MODE 0, 1, 2, 3) – that basically define the SCLK edge on which the MOSI line toggles, the SCLK edge on which the master samples the MISO line and the SCLK signal steady level (that is the clock level, high or low, when the clock is not active). Master and slave pair must use the same set of parameter for a communication to be possible.

Each mode is formally defined with a pair of parameters (Table 2-1):

- Clock polarity (CPOL): specifies an idle low / high clock
- Clock phase (CPHA): specifies when data are captured and propagated by the master

Parameters	SPI mode
CPOL = 0, CPHA = 0	0
CPOL = 0, CPHA = 1	1
CPOL = 1, CPHA = 0	2
CPOL = 1, CPHA = 1	3

Table 2-1: SPI modes

The SE supports only SPI mode 0 (CPOL = 0 / CPHA = 0):

- The data are sampled on a rising edge (low → high transition) of SCLK
- The data are propagated on a falling edge (high → low transition) of SCLK

Figure 2-7 depicts the behaviour of each SPI signal for mode 0 (SS# is CS):

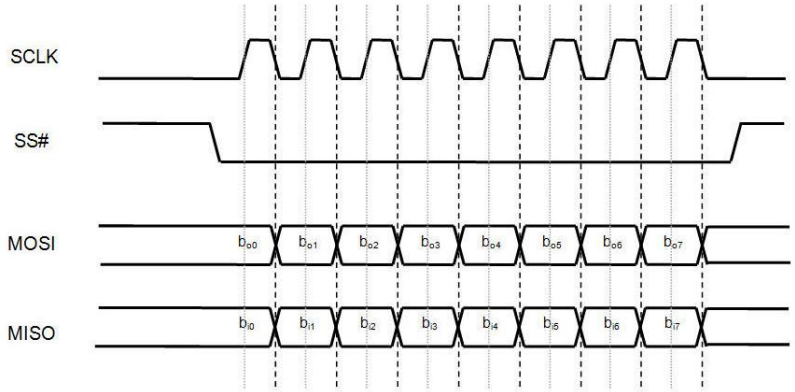

Figure 2-7: Supported SPI mode

2.4.1.3 Protocol

This session describes the protocol used over the SPI interface to enable communication with the SE Package. Each packet passing over the SPI bus has the following structure:

- Operation code: 1 byte
- Packet data length: 2 bytes (MSB first)
- Packet data: from 5 to 261 bytes
- CRC: 1 byte (XOR operation between byte of the packet data field)

Operation Code	Packet Data Length	Packet Data	CRC
1 byte	2 bytes	x bytes	1 byte

Figure 2-8: Packet format

2.4.1.4 Messages

To achieve all transactions, two types of messages are available. All the transactions can be decomposed with these two types.

Master Write Transaction

This message is used by the host to send a command to the SE.

1. The host drives CS low and waits for IRQ assertion
2. The SE Package drives IRQ low when ready to receive data
3. The host performs the transaction and sends the packet
4. After last byte of data, CS is driven high by the master
5. The SE Package drives IRQ high

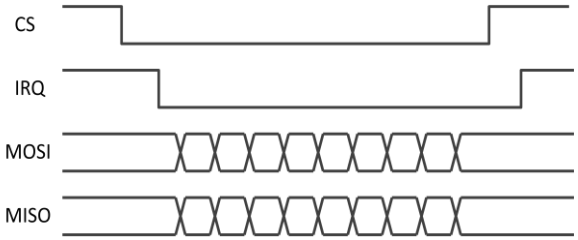

Figure 2-9: Master's write transaction

Master Read Transaction

This message is used by the SE to warn the host that there are data to be retrieved.

1. The SE Package drives IRQ low signalling to the host that data is available
2. The host drives CS low
3. The host sends three bytes to get the operation code and the payload length
4. The host fetches the rest of the packet
5. The host drives CS high
6. The SE Package drives IRQ high

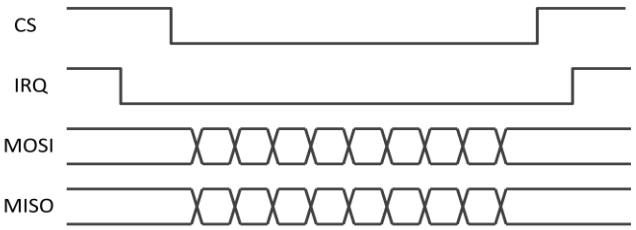

Figure 2-10: Master's read transaction

2.4.2 Application information

2.4.2.1 Packaging

The final product will be available in a QFN24 package. This package was chosen on account of several advantages:

- Good thermal and electrical performances
- Small sized "near chip scale" footprint
- Perimeter I/O pads to ease PCB routing

Figure 2-11 shows the external aspect of the chosen package:

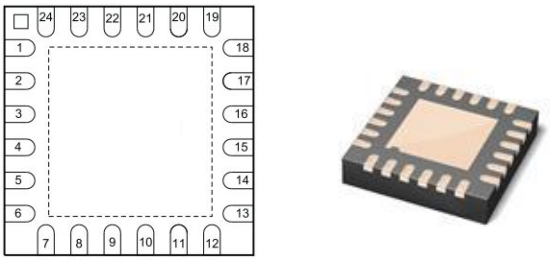

Figure 2-11: SE Packaging

During the engineering phase, the SE is presented in a DIL24 package as shown in Figure 2-12:

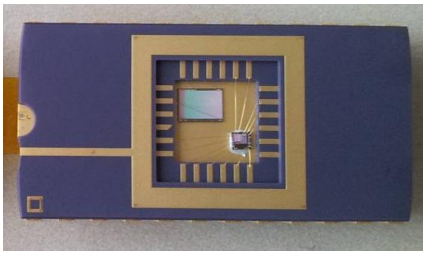

Figure 2-12: SE DIL24 prototype

2.4.2.2 Pin out

To limit the possible unwanted interactions with the SE, only useful silicon pads are wire bonded. Table 2-2 describes the pin assignment for engineering and final packages:

Pin	Name	Description
1	Vcc	Main power supply
7	MISO	SPI communication
8	MOSI	
9	CS	SPI Chip Select
10	SCLK	SPI Clock
11	IRQ	Interrupt
13	GND	Common ground pad

Table 2-2: SE pin assignment

All pins which are not described in Table 2-2 shall be left non-connected.

2.4.2.3 Typical application

Figure 2-13 describes the typical SE application. The Bill of Material (BoM) is limited to two decoupling capacitors (C1, C2) defined as follows:

- C1: 10µF, tantalum
- C2: 0.1 µF

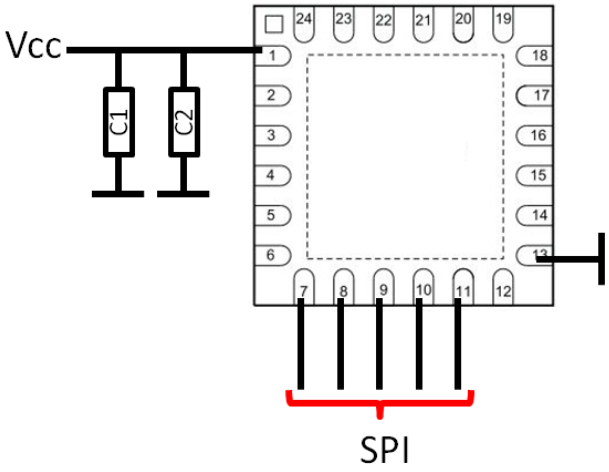

Figure 2-13: Typical SE application

As explained previously, the SE can be switched off if there is nothing to do. The Vcc shall be controlled by the host microcontroller to make it possible.

2.4.3 Electrical characteristics

2.4.3.1 Absolute maximum ratings

		MIN	MAX	UNIT
Supply voltage	Operating ambient temperature rang	-40	85	°C
Storage temperature range		-50	125	°C
ESD	All pads, according to human-body model		4	kV

Table 2-3: Absolute maximum rating

2.4.3.2 Recommended operating conditions

	PARAMETER	MIN	MAX	UNIT
Ta	Operating ambient temperature range	-40	85	°C
Vcc	Operating supply voltage	2.7	3.3	V

Table 2-4: Recommended operating conditions

2.4.3.3 DC characteristics

	PARAMETER	TEST CONDITIONS	MIN	TYP	MAX	UNIT
I_{cc}	Power supply current	Full speed internal clock All peripherals activated	6.13	6.33	6.47	mA
		Standby	100	105	110	µA

Table 2-5: DC characteristics

2.4.3.4 SPI

AC characteristics

	PARAMETER	TEST CONDITIONS	MIN	TYP	MAX	UNIT
T_{SCK}	SCK period	Slave, Rx and Tx	500			ns
D_{SCK}	SCK duty cycle	Slave		50%		
t_{IB}	Inter-byte time	Slave, Rx	8			µs
V_{IL}	Input Low Voltage	Vcc = 3v	0.2xVcc			V
V_{IH}	Input High Voltage	Vcc = 3v			0.7xVcc	V
V_{OL}	Output Low Voltage	Vcc = 3v	-0.3		0.4	V
V_{OH}	Output High Voltage	Vcc = 3v	0.7xVcc		Vcc+0.3	V

Table 2-6: AC characteristics

SPI communication characteristics

	PARAMETER	VALUE	COMMENTS
CPOL	Clock polarity	0	Negative Clock Polarity
CPHA	Clock phase	0	Data sampled on MISO on clock rising edge
BO	Bit Order	MSB first	Most Significant Bit first

Table 2-7: SPI communications characteristics

3 Pairing

3.1 Objectives

Setting up a secure communication channel between devices is a crucial part of secure communications. Secure device pairing means setting up a secure association with relevant keys, identifiers and cryptographic algorithms for subsequent secure communications between two devices. Without any previous association between the devices, creating the association in secure, easy and intuitive fashion presents many challenges.

Pairing plays a major role in secure communications. It specifies which device can access the network and grants its rights. Therefore, it is essential to define completely how a device is integrated in the network through pairing. Once the pairing is done, the only way to initiate new pairing is to break the previous one. It is done by the gateway through a specific command. During this association, two main points are addressed: authentication and data security. It is vital to prevent attackers from being able to enter the network and to get security keys. A key management scheme shall be defined to keep the security level and prevent the system of unwanted pairing.

3.2 Pairing mechanisms

3.2.1 Using out of band trusted communication channel

As a part of the security association, the devices need to create a shared secret. For this purpose, the devices run a key establishment procedure (traditionally based on Diffie-Hellman) to create the shared secret. If this initial setup is created in an unauthenticated wireless environment, it is easy for an adversary to make the two legitimate devices to believe that they are communicating with each other while in reality, they are communicating only with an opponent reading, modifying and relaying messages (Man-in-the-Middle attack).

“Out of band” means that the provisioning link will not rely on the main communication interface but on a secondary and distinct one. In the case of a capillary network, the secure channel could be setup by a physical contact between a device and the gateway like a simple wire or a close communication like Near Field Communication (NFC). It enables a secure transient association. A Man in the Middle attack is impossible over this channel: the secret exchange can be performed safely.

3.2.2 Using in band integrity region

Certain types of devices do not offer the possibility to add another interface for an out of band pairing (small sensors for example). It is still possible to setup a secure pairing by shrinking the communication range: proximity verification is provided.

It can be done by adding an analogical controlled attenuator between the RF module and the antenna. Once the pairing succeeds, the attenuation is relaxed and the communication range recovers its initial characteristics.

3.2.3 Using passphrase

To address mass pairing situation, the authentication through a passphrase is an efficient way to proceed. The device is manufactured with a unique hardcoded passphrase. It can be assumed that the network user gets all these passphrase easily and can provide them to the gateway associating the right MAC address.

The user is then able to spread the devices on the field. Given that the gateway is aware of the MAC address / passphrase couple, it is easy to base authentication on a hash comparison.

3.2.4 Using certificate

Another way to fit with mass pairing situation is to rely on a certificate exchange scheme. Certificates are provided by Certificate Authorities (CA) and written in the gateway. The device will then use a generic authentication process to become a trusted element of the gateway. Key sharing to secure the communication can then happen.

For this pairing mechanism, gateway and device manufacturer need to ask certificates to a CA.

3.2.5 Manufactured pairing

In a case of mono-vendor system (built-in capillary network for example), it is possible to manually establish a pairing while manufacturing or during personalization. All needed pairing data are written in the gateway and the devices. When the system is turned on, all devices are already trusted devices.

Manufactured pairing could also be temporary and restricted to the single task of reaching the provisioning server and downloading its profile during initial auto configuration phase.

This pairing is suitable for small networks on which only one entity is supposed to work (automotive for example).

3.3 Relevance to EXALTED

Keeping in mind all the requirements made for the use cases, we can define a three-level pairing within EXALTED:

1. The lowest pairing level is set up between the SE and the host microcontroller. It prevents someone from:
    a. removing the SE and addressing it with another microcontroller to tamper it
    b. replacing the SE and trying to corrupt the host microcontroller

2. The second step is the most common pairing mechanism: it is the way for a device to be granted an access in a network. In EXALTED, it refers to the pairing within the capillary network (Non-LTE-M devices only are affected, given that LTE-M device network authentication is already managed by a SIM).

3. The most high-level pairing is the application bootstrapping (ensuring an E2E security) as defined in D5.1 [11]. It allows (or not) a distant application to get data from a specific sensor or actuator in a M2M device. It is really useful in the case of a M2M device which can be accessed by different applications without giving a full access to each of them. The pairing between the distant application and the device creates a common specific context (encryption rules, keys, etc.).

The first level of pairing shall be handled during the manufacturing of the M2M device: a secret key can be shared between the two components during a personalization process. SE and host microcontroller can easily authenticate each other that way. In order to improve the efficiency of this pairing, a key renewal mechanism can be set up locally between the two devices.

The second and third level of pairing depends on the use case. We describe the different options in the following chapter.

3.4 Use cases

As explained above, each use case presents constraints that are really different regarding the application domain (e-Health is, for example, a highly critical subject due to the type of data conveyed).

3.4.1 Intelligent transportation system

The ETSI Technical Committee Intelligent Transport System has produced a technical report as a result of threat, vulnerability and risk analysis of radio communications in an ITS [18]. The document is a technical report which identifies requirements for vehicle to vehicle and vehicle to roadside network infrastructure applications.

In this use case, we have to make a distinction between different branches. We can consider at first the traffic optimization where communications between vehicles (gateway vehicle with multi-hop scenario) or with information sensors (parking, road signs, etc.) happen. The certificate-based pairing seems to be the best option for the two levels of pairing because it guarantees interoperability in a multi-brand environment.

Fleet management has also to be taken into account. In this case, the whole on-board system (LTE-M gateway, GPS, tyre pressure / engine temperature sensor, etc.) is often set up by the vehicle manufacturer or an Original Equipment Manufacturer (OEM). The manufactured pairing brings here a good flexibility in the second level of pairing: all the communication links between the gateway and the devices are configured during the production phase. Regarding application bootstrapping, all the information headed to the devices are sent through an out-of-band trusted communication channel (like NFC) to the gateway which forwards the data.

3.4.2 Smart metering and monitoring

Pairing used in this use case depends mainly on the application scale (home, industry, environmental).

Concerning the home application (smart metering, home automation, etc.), an out-of-band or an in-band within integrity region pairing (depending on the device type) are conceivable to be allowed to access the network. The user can easily access the gateway and put the device in close vicinity, either with cables or through short range communication.

When it comes to environmental monitoring, the constraints evolve a lot. This scenario is based, as described in D2.1 [6], on a "*(...) large scale of deployment, with the devices having to cover huge geographical areas, while no human intervention should be required*". We are here facing a mass pairing situation which can be made easier by using passphrase pairing.

3.4.3 E-Health

A patient must be monitored due to a specific disease which needs to gather a lot of continuous vital sign data. The doctor can lends to the patient, for a defined period (a week or a month), a fully working monitoring system. The pairing (level 2 and 3) is done by the professional and renewed at each use. It can be done through software by plugging the gateway and the devices in the computer, i.e. in an out-of-band manner. Secrets are exchanged safely and the system is quickly set up. The patient wears the complete system until all data are collected and sent. He brings then the system back.

In the case of a personal use driven by the willingness of people wanting to monitor themselves, the certificate-based application pairing seems to have the lead. It can prevent people from using fake medical devices which can potentially be harmful.

4 Conclusion

This report has addressed the device improvement needed to enhance communications and components lifespan in LTE-M architecture.

In a first step, we analysed the results about Self-Diagnostics and energy equalization to understand how they can be combined in the device improvement task. It is demonstrated that taking into account these results can lead to a real improvement in the M2M networks.

Next, we presented the prototype showing the implementation of a reliable, energy-efficient and secure mechanism within EXALTED: the SE. The first point was to explain where the SE could find its place within the EXALTED system by analyzing the results released in D2.3 [7] concerning the whole architecture and D5.1 [11] concerning security aspects. Gathering a secure microcontroller and a configurable bridge allowed us to bring the needed security to fit with the three defined use cases. The main objective was to implement a high level of security without trade-off between performance, reliability and power consumption.

We finally described how a right chosen pairing can overcome the constraints related to the use cases defined in this project. A three-level generic pairing was defined to describe precisely each scenario. As a result, we found that these different mechanisms are just a matter of implementation and can be all supported by the architecture.

The next step is now to consider the integration of the SE and the concepts presented here in the test beds defined in D7.2 [15], especially test bed 3 which contributes to the security framework where the SE plays an active role.

LIST OF ACRONYMS

Acronym	Meaning
3GPP	Third Generation Partnership Project
CH	Cluster Head
CLF	Contactless Front End
DM	Device Management
DME	Device Management Entity
DnD	Diagnostic and Decision module
GW	GateWay
ITS	Intelligent Transportation System
JVM	Java Virtual Machine
LTE	Long Term Evolution
LTE-M	LTE for Machines
M2M	Machine-to-Machine
MAC	Medium Access Control
MIM	Machine Identity Module
OMA	Open Mobile Alliance
OS	Operating System
SDM	Self Diagnostic Modules
SMM	Smart Metering and Monitoring
SWP	Single-Wire Protocol

References

[1] ETSI TS102613 Smart Cards; UICC-Contactless Front End (CLF) Interface; Part1; Physical and data link layer characteristics.
[2] ETSI 102671 Smart Cards; Machine to Machine UICC; Physical characteristics
[3] SIMAlliance Open Mobile API, Website
[4] SPI Block Guide v03.06, Freescale Semiconductor
[5] http://www.ict-exalted.eu/about-us/workpackages/wp6.html
[6] FP7 EXALTED D2.1 – "Description of baseline reference systems, scenarios, technical requirements & evaluation methodology"
[7] FP7 EXALTED D2.3 – "The EXALTED system architecture (final)"
[8] FP7 EXALTED D3.3 – "Final report on LTE-M algorithms and procedures"
[9] FP7 EXALTED D4.3 – "Device management"
[10] FP7 EXALTED D4.4 – "Traffic aggregation"
[11] FP7 EXALTED D5.1 – "Security and provisioning solutions"
[12] FP7 EXALTED D6.1 – "Optimizing a Linux operating system for M2M devices"
[13] FP7 EXALTED D6.2 – "Final specification of the energy efficiency implementation"
[14] FP7 EXALTED D6.3 – "Final specification of the reliable device implementation"
[15] FP7 EXALTED D7.2 – "Integration of selected algorithms into platforms & interfaces finalization"
[16] Brecht Wyseur, White-Box cryptography http://www.whiteboxcrypto.com/research.php
[17] Open Mobile Alliance – "DM DiagMon Architecture v1.0"
[18] ETSI TR 102893 V1.1.1 (2010-03) ITS Security; Threat, Vulnerability and Risk Analysis