The Importance of Secure Elements in M2M Deployments: An Introduction

February 2014

Contents

The Importance of Secure Elements in M2M Deployments

1. Introduction

According to many sources, the global machine-to-machine (M2M) market is on the verge of significant and rapid expansion. Technavio analysts forecast the global M2M market to grow by approximately 26% between the period 2012-2016, while the GSMA predicts that mobile connected devices will reach the 12 billion mark in 2020.

This highly anticipated boom in the M2M market is being fuelled by two key factors:

- The benefits offered by cellular connectivity between devices are relevant to many vertical markets. The result is the limitless potential emergence of new M2M applications across many different sectors.
- There is no saturation limit for the M2M market as it is not restricted by human population statistics.

As with most markets, however, growth in the M2M sector will be hindered without standardisation. With the continued rise in deployments of M2M applications across diverse geographical and vertical markets worldwide, key operational challenges are emerging based on the M2M business model. In summary, the distributed nature of M2M terminals (many of which are in hard to reach locations) makes it difficult to manage and maintain both terminals and applications and many M2M services require the highest levels of security.

To ensure further progress, the question that must now be answered by the industry is: 'How best to deliver an open and reliable ecosystem which supports remote programmability and automated device and application security management?' SIMalliance responds that a key element is the presence of the Secure Element (SE) and an associated remote management infrastructure. A SE is defined by SIMalliance as a dedicated hardware component with specialised software. Use of a SE in M2M deployments can deliver against two key requirements specific to the M2M environment: remote programmability and high levels of application security.

SIMalliance promotes the importance of deploying any type of SE form factor when delivering highly secure applications via a cellular network, but places the greatest emphasis on the embedded secure element (eSE) and in particular the embedded UICC (eUICC) because these are the most widely established SE form factors used globally in M2M applications today.

2. An Overview of the M2M Market

M2M stands for 'machine to machine' communication. Eurosmart defines M2M as 'an ecosystem which allows the communication between two pieces of equipment through the exchange of data over a wireless network or by direct (wired) connection without human intervention'.

The potential for cellular connectivity in M2M is vast. A Berg Insight report published in October 2013[1], estimates that in 2012 shipments of cellular M2M devices increased by 15.3% to a new record level of 54.9 million units and the worldwide number of cellular M2M subscribers reached 134.9 million. It also predicts that the shipment of cellular M2M devices will reach 185 million units in 2018, growing at a Compound Annual Growth Rate (CAGR) of 24% each year. GSMA support this concept of growth, with estimates that

[1] Global Wireless M2M Market, Berg Insight, October 2013

mobile connected devices will reach the 12 billion mark in 2020. In 2012, SIMalliance members shipped 5 million M2M (MFF2 form factor) SIMs; a number which represents 42% growth on the previous year. In light of such opportunity, the dominant market motivation for driving further growth in M2M has shifted to the pursuit of revenue generation; connected devices are now recognised as a key vehicle through which service providers can deliver added value and services.

Further growth in shipments is expected in the coming years thanks to the combination of two factors: firstly, there is an increasing range of applications across many different verticals, led currently by connected cars and smart metering, and secondly, there is no saturation limit for the M2M market, since it is not restricted by population statistics.

2.1 Market growth: the challenge and the enablers

A key challenge which must be addressed to support further sector growth is posed by the M2M operational model. The process of operating fleets of machines running diverse applications is very different from operating communities of 'human' subscribers. Many M2M applications use millions of unattended terminals in various remote, sometimes difficult and inaccessible locations. This leaves them vulnerable to external threats and attacks and renders it challenging for M2M service providers to maintain and manage both the terminal hardware and the applications they are running.

The lifecycles of M2M equipment in the field and M2M applications have to be much longer than those associated with consumer applications. Ongoing management and maintenance of both hardware and software is therefore essential to preserve the longevity of M2M equipment and applications.

Another consideration is that the M2M ecosystem is far more complex than that needed to deliver consumer services. M2M deployments tend to involve a greater number of stakeholders and in many cases reliability of service has to be guaranteed contractually between ecosystem actors and the service provider. As such, all actors in the supply chain have to agree on and adhere to the highest levels of service quality and reliability.

To address these challenges, a complex ecosystem which is capable of remotely and automatically managing device and application security, is required. The processes and management capabilities implemented by the ecosystem must offer the appropriate levels of security and reliability.

For this reason, SIMalliance supports the idea that secure elements (SEs) embedded within M2M equipment, alongside an associated remote management infrastructure, are key enablers of M2M market growth.

3. The Benefits of Embedded Secure Element (eSE) Technology in an M2M Context

A SE (a dedicated hardware component with specialised software) is essential when delivering highly secure applications via a mobile network. All SEs provide a safe execution environment whatever their form factor.

In an M2M context, the embedded SE (eSE) is the most widely established form of SE used globally today - specifically the embedded UICC (eUICC).

The eUICC is based on UICC technology and is globally established as a tamper resistant security platform that enables secure and reliable access to cellular networks. The eUICC is also a proven application platform that provides interactivity and connectivity to the applications it carries. The sheer volumes (billions) of UICCs which have been deployed globally by mobile networks operators (MNOs) over the years testify to the technology's interoperability and security levels

The eUICC addresses requirements specific to the M2M environment: better integration of the UICC with the device (so that it cannot be stolen or tampered with, for example), high security and remote programmability, most commonly used for remote subscription management.

From a functionality perspective, there is no difference between the eUICC and the most advanced UICCs currently available. An eUICC can offer:

- Capability to store several Network Access Applications (NAAs) to allow a seamless adaptation to GSM, UMTS, CDMA and even LTE networks.
- Secure storage of network access credentials, authentication algorithms and customer specific data and configuration details.
- Multi-application capability to store other specific security applications, in addition to the applications that are usually used in the Cellular mobile world.
- Standardised highly secure over-the-air (OTA) updates of credentials, applications and data.

Crucially, the eUICC offers a significant operational benefit when applied to the M2M sector: subscription operations can be undertaken remotely. 'Subscription operations' refer to the management and maintenance of the details of individual subscribers to a mobile network. Another name for UICC is SIM (Subscriber Identity Module) and the UICC or SIM identifies a subscriber to a digital mobile service and details the special services the subscriber has elected to use. Since the eUICC has a dual role, both carrying a subscription (i.e. the details of the person authorised to use the UICC technology to access the mobile network) and acting as an application platform, it offers service providers, MNOs and their partners secure remote management capability for their value added services located in the eUICC. As the lifecycle of an application is usually far shorter than that of its host terminal – many of which can last for up to 20 years in the M2M sector – service management capabilities, enabled by remote management, are essential to support new, or many iterations of, applications that may evolve over the terminal's lifecycle.

Thanks to its remote subscription management capabilities, the eUICC can also offer advantages related to industrial product lifecycles in M2M. Equipment may sit in warehouses for long periods of time before being shipped to their final location and connected to a MNO; this enables devices and terminals to be mass produced even though they may be destined for deployment in different countries. As such, the geographical destination of a M2M device (and subsequently the connecting MNO) is not always known at the time of manufacture. The need for remote provisioning has been heightened by this growing requirement for the late configuration of M2M terminals (when the UICC/eUICC is personalised after it is shipped). There is also an increasing requirement for more sophisticated modules containing eUICCs, which have the ability to comply with multiple and changing regulatory environments, connectivity and service providers.

There are instances when an additional SE (independent of the eUICC) may be deployed to host a secure application:

- When a secure application does not require a cellular subscription to be hosted in the same secure hardware (e.g. the application communicates via non-cellular network connectivity).
- When independence between a secure application and a cellular subscription is beneficial / desirable.

Like the eUICC, the secure element is an open secure application platform that is able to execute code, process data flows, store data and manage credentials. Service providers can implement their application in a distributed way, among the eSE, terminal and back end system.

4. The Importance of Security

Aside from presenting a solution to the various operational challenges, the eSE (either eUICC or independent) plays a significant role in ensuring that appropriate security levels are created and maintained

in M2M deployments. M2M services may become a prime target for security threats in the future, because of three key factors:

- A large majority of M2M terminals will be unattended during most of their operational lifetime.
- A number of high value M2M applications may be attractive to hackers because they offer lucrative returns or because they provide a means to achieve an unlawful agenda.
- There are likely be a higher number of connected devices than phones or consumer devices in the future, since the potential scale of the global M2M market is much larger.

M2M will receive a considerable amount of data from the field and decisions will need to be made automatically in some cases. Security therefore is a key element in the value chain and it must be at the heart of the design and implementation process at both the system level and when considering the individual components of the deployment. With security threats constantly evolving however, it is equally important that the security levels of system components can be upgraded regularly and with ease. All security measures have a limited lifespan, which means that security upgrades must be performed at regular intervals, particularly on terminals and equipment with long lifecycles.

5. Conclusion

While there are instances where an alternative form of SE may be viable, when a secure application does not require a cellular subscription, for example, these instances are few and far between relative to the extent and diversity of the market for M2M. Indeed so fast is the pace of global M2M uptake that industry stakeholders must take a pragmatic approach to security and interoperability if they are to capitalize on the opportunities in hand. This means opting for tried a tried and tested secure application platform which is universally supported, remotely programmable, and deployable on a mass scale, today. With these considerations in mind, the eUICC stands head and shoulders above. In 2014, there is simply no viable substitute.

For more information on SIMalliance, please visit www.simalliance.org