simalliance
Security | Identity | Mobility

eUICC for:
Smart metering

INTRODUCTION

What is a smart meter?

The term ‘smart meter’ covers a variety of residential, commercial and industrial solutions monitoring a full range of utilities, including electricity, water and gas. The overall market is set to be worth $19.98 billion by 2022, with residential applications representing 84% of total deployments (Source: MarketandMarkets).

Regulation and renewable energy are driving growth...

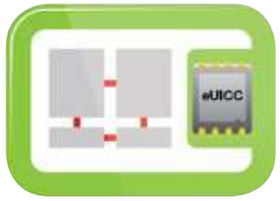
The global expansion of smart meter deployments has been driven in part by governmental regulation, due to a requirement for real-time power consumption data to better manage renewable energy sources. For example, the European Union aims to replace 80% of electricity meters across member states with smart alternatives by 2020 (Source: European Commission). The United Kingdom has gone further, mandating the installation of smart meters across all residential and commercial properties by 2020 (Source: UK Government).

The growth of smart meters is also indicative of the rapid global rise in IoT and M2M use-cases. Gartner has predicted that there are currently 8.4 billion connected devices in use worldwide, and this is poised to increase to 20.4 billion by 2020 (Source: Gartner).

What is a UICC?

UICC (Universal Integrated Circuit Card) is the hardware used in mobile devices that contains SIM and / or USIM applications enabling access to GSM, UMTS / 3G and LTE networks. (Source: GSMA – an industry association representing mobile network operators (MNOs)).

It is the most widely distributed secure application delivery platform in the world.



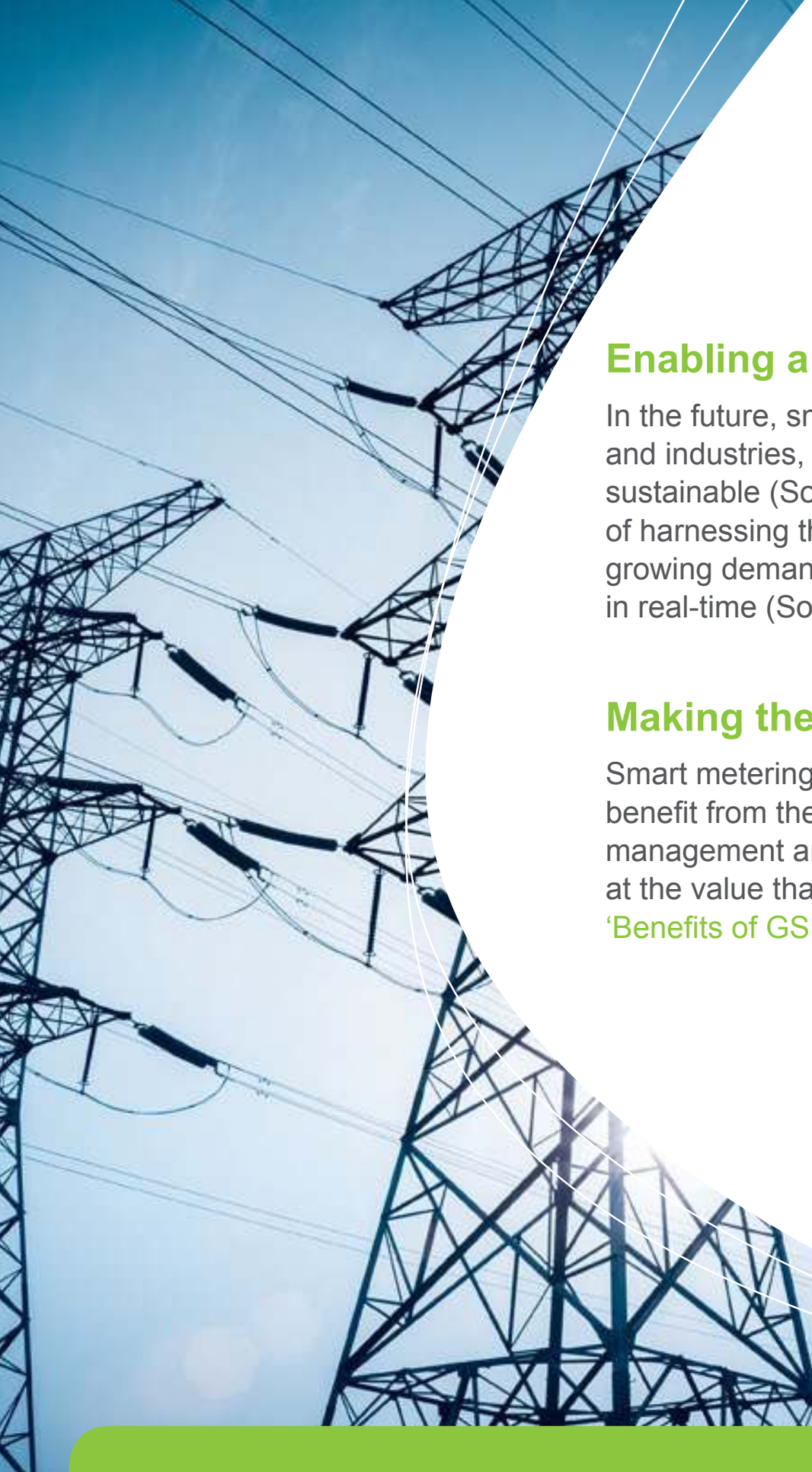
What is an eUICC?

eUICC, also known as an embedded UICC or eSIM, refers to a UICC which:

- Is capable of hosting multiple network connectivity profiles (as defined by GSMA).
- Supports secure over-the-air (OTA) remote SIM provisioning as well as updates to the operating system (OS), keys, application and connectivity parameters, according to GSMA and GlobalPlatform Specifications.
- Securely executes sensitive services.
- Includes soldered (MFF1, MFF2, etc.) and traditional removable (2FF, 3FF, etc.) form factors.

Aim of eBook

This eBook explores the nature of certain security and logistical challenges posed by smart metering deployments, and suggests how the eUICC can be utilised to successfully address them.



Enabling a ‘sharing economy’

In the future, smart metering deployments will be a key enabler of smart cities and industries, delivering the data required to ensure services are efficient and sustainable (Source: GSMA). In addition, smart metering opens up the possibility of harnessing the huge power of the ‘sharing economy’ to manage and meet ever-growing demand for utilities by diverting resources to where they are needed most, in real-time (Source: Huffington Post).

Making the case: the value of the eUICC in smart metering

Smart metering is just one of many use cases within the utilities sector which can benefit from the eUICC. Other examples include demand response, utility data management and distributed utility resource management. For a more detailed look at the value that eUICC technology can bring across these use cases, please read ‘Benefits of GSMA Embedded Specification for the Utilities Sector’.

Smart metering is just one of many use cases within the utilities sector which can benefit from the eUICC.

SMART METERING DEPLOYMENTS: **WHAT ARE THE CHALLENGES?**

As is well documented, the development and deployment of IoT and M2M solutions present various industry stakeholders with unprecedented security and logistical challenges.

Smart meters are no different.

Security challenges of smart meter deployments

- **Threat to critical infrastructure** – Utility networks are classed as critical infrastructure, which is defined as an asset or system essential to the maintenance of vital societal functions (Source: European Commission). Disruption of critical infrastructure can have a significant political, economic and social impact. With the increasing connectivity of utility networks presenting an expanded threat-landscape, smart meters are high-value targets for cyber-attackers.

- **Energy theft / tampering** – Smart meters with inadequate security could be vulnerable to being tampered with by dishonest third parties wishing to make illegal gains from energy theft. Besides the resulting commercial losses for the utility company, any threat to the integrity of data transmitted could have an adverse impact on services, since utility companies utilise smart meter data to manage and regulate supplies.

- **Firmware / software authenticity and integrity** – It is imperative that the authenticity and integrity of the firmware / software within a smart meter is not compromised by malicious actors. For example, a hacker could ‘reflash’ the firmware / software of a smart meter to decrease consumption.

- **Privacy breaches** – Unless properly protected and encrypted, power consumption data which is stored on or transmitted by smart meters could make it possible for unauthorised entities to identify or anticipate the behaviours of individual households. For example, what time a householder typically leaves the house for work, goes to sleep or when they are on vacation. Needless to say, this exposes the household to the risk of malicious intent (e.g. burglary), if the data falls into the wrong hands. To prevent this from happening, a solution is needed which offers flexible connectivity while protecting the confidentiality, integrity and privacy of data exchange over the network.

- **Unauthorised network access** – Beyond the threat posed to individual meters and associated data, there is the serious prospect of poorly protected smart meters allowing attackers an entry point to the wider network.

In this instance, while the data or device is of relatively little interest to the attacker, there is an opportunity to cause major disruption to utility supplies and / or the underlying connectivity network.

A solution is needed which offers flexible connectivity while protecting the confidentiality, integrity and privacy of data exchange over the network.

Advanced security is key to countering these threats.

The eUICC is built on the most widely distributed and secure application delivery platform in the world (UICC), which is certifiable and specified by the GSMA. As it retains all the security benefits of the UICC, and the various discrete Secure Element (SE) form factors such as embedded Secure Elements (eSE), it is the most secure option for protecting highly sensitive use cases. It also has significant advantages associated with remote provisioning and management.

For device makers and utility companies who do not initially require cellular connectivity, an eSE is an alternative option to effectively address the key security challenges outlined.

The eUICC is built on the most widely distributed and secure application delivery platform in the world.

What is a Secure Element?

A Secure Element (SE) is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.
(Source: GlobalPlatform).

Logistical challenges of smart meter deployments

- **Connectivity** – While there are various connectivity options which enable two-way communication between smart meters and associated servers, cellular and mobile IoT connectivity offers a number of distinct advantages for utility companies. These include broad reach across most inhabited areas, lower infrastructure costs, reduced installation costs and quick implementation times. When compared to other wireless technologies, cellular networks offer higher bandwidth and a consistent, universal approach thanks to the UICC / eUICC authentication. This enables utility providers to make safe and secure remote firmware upgrades to smart meters in order to update features and / or provide new services. This would be extremely complex and difficult via a non-cellular network connection. Additionally, the security of mobile networks has been proven over decades. A particular feature of their success has been device and network authentication, ensuring that only authorised devices can be connected. This offers lower cost and risk of security breaches in utility device networks.

- **Miniaturisation** – As devices get smaller, in line with consumer expectations of convenience and minimal disruption to daily life, there is a need for smart meters, particularly those for residential use, to follow trend. Smart meters can therefore also benefit from the miniaturised components, including the eUICC and eSE, that are utilised in other consumer devices.

The security of mobile networks has been proven over decades.

- **Post-issuance personalisation and remote management of meters in the field** – Based on UICC technology, which is recognised as the globally established, standardised way of securely accessing cellular networks, the eUICC offers remote provisioning and management advantages to smart meter deployments. Due to the dispersed and often inaccessible nature of smart meters in the field, plus the 10-15 year lifecycle of a smart meter, MNO profiles, software, firmware and application updates and upgrades, which are required over the course of its lifetime, need to be managed remotely. As already stated, cellular connectivity is required to provide the necessary bandwidth and universal consistency to efficiently manage firmware updates and upgrades.

Without a solution to address this challenge, utility providers will be required to activate and maintain their smart meters via expensive and complex site visits, which can cost between €25-€80 per time. When extrapolated across an installed base of millions of devices, this represents a significant cost-burden for utility providers (Source: GSMA, ESMIG, SIMalliance and Beecham Research). Indeed, high installation and ongoing management costs have been identified as a key factor that could temper the growth of the smart metering market (Source: MarketandMarkets).

The **eUICC** (based on the proven, established and secure UICC platform) is **certified and specified by the GSMA to deliver secure cellular connectivity.**

When combined with the considerable benefits of **remote management** and a **more compact design**, the eUICC is clearly **well-positioned to effectively address the logistical challenges posed by smart metering deployments.**

HOW CAN THE eUICC **OVERCOME THESE CHALLENGES?**

The eUICC is already widely deployed across various M2M and IoT use cases and its role in enhancing security and reducing complexity is widely recognised.

Enhancing security

There are myriad reasons why the concept and design of the eUICC make it the most secure option and the best way to deliver advanced security to smart metering deployments:

De facto security platform

An eUICC is still a physical hardware SIM product which, like UICCs and SEs, supports the execution of sensitive applications such as payment, access control and biometrics. This is combined with the ability to support OTA remote SIM provisioning and management. It is a discrete, tamper resistant hardware module with its own processing power and data storage, and is therefore isolated from those resources of the device, protecting data and keys stored and executed within it against hacking, tampering and unauthorised access. This means it retains all of the security benefits of traditional removable SIMs and SEs. It is also certifiable and specified by GSMA. When correctly developed, implemented and distributed, eUICC solutions are uniquely positioned to deliver the advanced security required for smart metering deployments.

Remote security updates / upgrades

In parallel, the eUICC has the potential to provide security not only now, but in the future. Remote software upgrades and OS patches could be utilised to address emerging security challenges and threats. This flexibility and reactivity will be essential to ensure the long-term security of smart meter deployments.

eUICC solutions are uniquely positioned to deliver the advanced security required by smart meters.

The eUICC, together with the cellular connectivity it brings, is based on a highly efficient, advanced and security-certifiable process landscape.

Secure process landscape

Advanced security comes not only from the eUICC, but also the correct execution of the various related data management processes. For example, the exchange and transmission of sensitive data – such as that used for billing, network authentication or the protection of encryption keys – requires a huge degree of trust between the stakeholders involved. The eUICC, together with the cellular connectivity it brings, is based on a highly efficient, advanced and security-certifiable process landscape, borne through decades of successful partnerships between MNOs and SE vendors.

Soldered form factor

Finally, the eUICC delivers physical security benefits. As it can be soldered and is tamper-resistant, it cannot be stolen and used fraudulently.

Reducing complexity / increasing flexibility

The eUICC is well placed to overcome many common logistical challenges associated with smart meter deployments:

Secure cellular connectivity

As utility companies increasingly seek to utilise cellular and mobile IoT technology to enable the connectivity of their smart meter base, the eUICC, based on the proven, established and secure UICC platform, is certified and specified by the GSMA.

Remote profile provisioning and management

eUICCs offer OTA remote provisioning capabilities, which enable a practice known as late operator binding. Smart meters can be shipped, on a mass market scale, directly to the installation locations, where the correct network profile can be downloaded OTA upon connection to the GSMA Remote SIM Provisioning for M2M system. If a change of MNO is subsequently required, OTA remote provisioning can again be used to remove an existing profile and download a new network profile directly to the device.

Reduced site visit requirements / cost

Thanks to the remote provisioning and management capabilities offered, eUICCs can, in parallel, remove the requirement for time-intensive site visits (costing between €25-€80 per visit and potentially spanning millions of devices), leading to a considerable reduction of operational costs.

Miniaturisation

Due to its compact nature, the eUICC is better suited for mass volume deployments than removable SIM cards, which are several times larger. This is especially appropriate for residential smart meters.

Thanks to remote provisioning and management capabilities, eUICCs can lead to a considerable reduction of operational costs.

Low power

The eUICC may be optimised for low power consumption. Where battery life is a consideration, this is a distinct advantage.
This makes the eUICC suitable in cases where a power supply is not available, for example in the smart metering of water, gas and heat.

Ruggedisation

Since it is embedded, and capable of being managed remotely, an eUICC is a prerequisite for devices to be effectively waterproofed (sealed) and ruggedised for use in extreme physical environments.

Safety in hazardous environments

Due to the absence of physical connectors for soldered form factors, which conduct electrical currents, an eUICC is safer to use in hazardous environments than a removable SIM, particularly where inflammable materials and gases are present. This makes them suitable for use in gas meters, where gas leaks are possible.

CHALLENGES OF **SMART METERING DEPLOYMENTS**

	Security Challenges					*Logistical Challenges*		
eUICC features / functionality	Critical infrastructure threat	Energy theft / tampering	Software / firmware integrity	Privacy breaches	Unauthorised network access	Connectivity	Post-issuance mgmt	Miniaturisation
Remote provisioning & mgmt	✘	✘	✘	✘		✘	✘	
Tamper resistant	✘	✘	✘	✘	✘			
Isolated	✘	✘	✘	✘	✘			
Encryption	✘	✘	✘	✘	✘			
GSMA certified	✘	✘	✘	✘	✘	✘	✘	
Multiple connectivity profiles						✘	✘	
Soldered		✘						
Small size								✘

THE ROLE OF THE **SE INDUSTRY**

The importance of security and simplicity within smart metering deployments, and the reliance of this use case on cellular and mobile IoT technologies, means that the existing assets of the SE industry are now more relevant than ever within this ecosystem:

- An established IT infrastructure capable of remotely managing the lifecycle of global UICC / eUICC deployments;
- Advanced understanding of cellular connectivity / MNO requirements;
- Developed ‘trust’ relationships with MNOs, a long-established and secure process landscape.

SE vendors have the most extensive and proven experience in providing secure OS for UICC / eUICC, secure subscription and data management services, remote provisioning capabilities and a comprehensive understanding of MNO requirements, built over many decades and founded on a trusted relationship. These core competencies can be transferred and tailored to various IoT and M2M use cases, such as smart metering, leaving the SE industry best placed to deliver the strongest available device security and reduced complexity to the utility sector.

CONCLUSION

- The eUICC is already delivering enhanced security and significantly reducing complexity for smart metering deployments across the world.
- SE vendors are an enabling stakeholder within this emerging ecosystem; their traditional core competencies translate to support and facilitate the continued deployment of secure and stable smart metering solutions.
- SE vendors have established the infrastructure, processes and relationships required to successfully manage the lifecycle of deployed UICCs / eUICCs.
- Smart metering is just one of many use cases within the utilities sector which can benefit from the eUICC. Other examples include demand response, utilities data management and distributed utilities resource management. Indeed, there are predicted to be 111 million eUICC deployments within the utilities industry by 2020 (Source: GSMA).
- For a more detailed look at the value that eUICC technology can bring across these use cases, please read 'Benefits of GSMA Embedded Specification for the Utilities Sector.'

About SIMalliance (Security, Identity, Mobility)

SIMalliance is the global, non-profit industry association which advocates the protection of sensitive connected and mobile services to drive their creation, deployment and remote management across multiple industries and use cases, including IoT.

The organisation promotes the essential role of a tamper resistant secure hardware component in delivering secure applications and services across all devices that can access wireless networks SIMalliance facilitates and accelerates delivery of secure connected services globally, by:

- anticipating market needs and developing associated, enabling specifications;
- collaborating with industry stakeholders to ensure that new use cases and business models can be simply and securely supported;
- clarifying and recommending existing technical standards relevant to the implementation of strong device security;
- promoting the availability of its members' standardised, global security infrastructure, together with an established process landscape, which offers an instant solution to many challenges associated with bringing mobile services to market and managing them remotely.

SIMalliance members represent approximately 90% of the global SIM card market.

www.simalliance.org

simalliance
Security | Identity | Mobility