GSMA Intelligence

ANALYSIS

The future of the SIM: potential market and technology implications for the mobile ecosystem

February 2017

gsmaintelligence.com • info@gsmaintelligence.com • @GSMAi

GSMA Intelligence

GSMA Intelligence is the definitive source of mobile operator data, analysis and forecasts, delivering the most accurate and complete set of industry metrics available.

Relied on by a customer base of over 800 of the world's leading mobile operators, device vendors, equipment manufacturers and financial and consultancy firms, the data set is the most scrutinised in the industry.

With over 30 million individual data points (updated daily), the service provides coverage of the performance of all 1,400+ operators and 1,200+ MVNOs across 4,500+ networks, 77 groups and 238 countries worldwide.

www.gsmaintelligence.com
info@gsmaintelligence.com

Authors

Pablo Iacopino
piacopino@gsma.com
Senior Manager

Mike Rogers
mrogers@gsma.com
Senior Analyst

Contents

1 Executive summary

The SIM has played a pivotal role in the rapid rise of mobile communications over the last three decades – today, 4.8 billion people use mobile services worldwide and there are 400 million cellular M2M connections. Through its evolution, from the traditional removable and non-reprogrammable SIM to the embedded SIM with remote SIM provisioning, the SIM has adapted itself to the latest cellular technology developments (e.g. 3G, 4G) and mobile industry requirements (new devices and use cases) while preserving its primary functions such as secure authentication and data protection.

Remote provisioning technology and embedded form factors represent a major development in the history of the SIM. This report looks at the implications from a market perspective. For consumers, SIM developments are likely to be unambiguously positive; for businesses, the implications are more nuanced, bringing both opportunities and challenges. We also examine the technology developments driving possible alternative SIM solutions and provide a qualitative assessment of the emerging use cases for the SIM.

To inform the report, we conducted primary research to gather strategic insights and views on the future of the SIM from companies across the broader mobile ecosystem – telecoms operators and non-operators, including SIM vendors, original equipment manufacturers (OEMs) and companies from a number of industries. The survey focused on use cases for the SIM; key challenges and opportunities; benefits for consumers and enterprises; and technology and innovation. (For a methodology and definitions, please see the Appendix.)

The report has been developed by GSMA Intelligence. It informs the marketplace of the rapid evolution of the SIM and potential implications rather than serving as an official policy position paper.

Remote SIM provisioning moves to the consumer handset market

The embedded SIM is already a mainstream technology in the cellular M2M market. The recent extension of the GSMA's remote provisioning specification to the mobile phone – the largest consumer mobile device in terms of number of users and associated ecosystem revenues – shows an alignment of operators, original equipment manufacturers (OEMs) and SIM vendors towards a single, de facto standardised approach.

This ecosystem alignment helps avoid industry fragmentation and potential interoperability issues. It also allows smaller service providers and OEMs to continue to have equal access to market opportunities. Although a limited number of proprietary solutions and exclusive partnerships for remote provisioning already exist in the consumer market, the move to a global and standardised technology will allow consumers to better reap the benefits of remote provisioning (such as time saving, improved security and an enhanced connected life) and continue to access a multitude of offerings and tariffs available in the market.

The transition to remote provisioning in the handset market will likely take many years

Mainstream adoption in the consumer handset market will take a number of years due to supply-side and demand-side factors. There will be a period of reconfiguration as ecosystem members gain remote SIM provisioning (RSP) experience and adjust to new manufacturing, logistical and supply chain processes, as well as a phase of customer education and associated customer service. There is also a huge installed base of handsets with a removable SIM which will remain in circulation. Handset replacement cycles are lengthening too.

We therefore expect to see a gradual transition in which multiple SIM solutions co-exist. Initial deployments are likely to be on specialist devices, or in mixed deployment scenarios with traditional physical SIMs. Ultimately, in the long term, embedded SIM adoption will be driven by OEMs implementing the technology and mobile operators enabling support for remote provisioning.

Emerging use cases for the SIM include cellular connectivity for Internet of Things devices and digital identity

As the broader mobile ecosystem continues to evolve, new use cases for the SIM are emerging across two main categories: cellular connectivity and SIM-based value-added services (VASs) that leverage the SIM's established strengths of secure authentication and data protection. These use cases broadly apply to most types of SIM but the embedded SIM with RSP is the most viable SIM option for certain Internet of Things (IoT) devices (such as smaller devices, remote locations).

The emerging use case for the SIM is in connecting to cellular networks an increasing number of IoT devices with connectivity requirements such as wide coverage and ultra reliability. Automotive leads the way, with built-in connectivity now embedded in a significant proportion of new cars. However, the role of cellular connectivity in the wider IoT connectivity market will remain marginal as the majority of IoT devices – typically in home or indoor environments – will likely be connected by radio technologies that operate on unlicensed spectrum or use gateway devices for their connectivity.

Mobile-based digital identity and authentication are also emerging SIM-based VASs, as the SIM is largely considered by both telecoms operators and non-operators as a secure hardware asset in which to store identity credentials. As we advance further into the digital age, the ability to prove a unique identity in the virtual, as well as analogue, world is becoming increasingly important for economic and social inclusion.

Market outlook: opportunities and challenges emerge for the broader mobile ecosystem

The transition to RSP will affect business models and market dynamics. The consequences are not certain at this stage and will take place over many years. However, remote provisioning will provide benefits for consumers, as well as opportunities and challenges for operators, SIM vendors, OEMs, IoT device manufacturers and service providers across many industries.

Consumers

As mobile users increasingly consume a variety of services and content over an array of connected devices and as privacy and security threats rise, the embedded SIM with RSP can support the development of a connected life across devices and use cases while providing improved security and saving time. However, a phase of end-user education is needed – particularly for consumers that are not tech-savvy – through customer-service support and simple, enhanced digital interfaces.

Industries that provide services and applications over mobile devices

The emerging service add-on model provides greater flexibility and scalability compared to an after-market model, potentially driving up global volumes and a proliferation of use cases. In the service add-on model, the connectivity functionality is built in during the manufacturing process across a number of devices (including cars), with IoT applications and services coming to market at a later stage and across multiple countries. IoT services and applications will likely take the lion's share of IoT ecosystem revenues, followed by IoT devices and – to a lesser extent – connectivity. The GSMA Intelligence survey pointed to high expectations from both telecoms operators and non-operators that automotive, utilities and healthcare will benefit from the evolution of the SIM.

Operators

Operators have an opportunity to enhance their end-user experience through new propositions that leverage the ability to connect an array of remotely provisioned SIM-enabled devices. This would drive multi-device and multi-user subscriptions, while device subsidies and financing may also evolve. Backend systems for CRM, billing and provisioning will need to be reconfigured to accommodate the move to multi-device subscriptions and, as a result, enhanced digital interfaces may become a differentiator (enhanced websites, apps and chatbots). Sachet marketing and pricing models may also be adopted as a differentiation tool.

The main challenges highlighted by operators in the survey are disintermediation and higher customer churn. With remotely provisioned SIMs, users can manage their subscriptions directly on a device. A clearer separation of the cost of the network service from the device may leave operators more vulnerable to disintermediation, given that handsets can be sold through other distribution channels. The potential combination of non-operator handset financing or leasing plans and remote SIM provisioning could present new competitive challenges for operators.

Churn may be more of a factor in markets dominated by pay as you go, since customers can switch operators more easily and price competition can intensify through short-term promotions. However, other factors such as network quality, coverage and customer service remain important considerations for customers choosing an operator. Furthermore, existing obligations with regards to know your customer (KYC) will remain, and mobile number portability processes are not currently expected to change.

SIM vendors

RSP will allow SIM vendors to streamline their manufacturing and logistics but it will also affect other components of their business models. For example, SIM vendors can provide improved IoT security solutions in a market environment exposed to risks, and their value add in the ecosystem may increasingly centre on security and trust solutions associated with personalisation and handling operator data. The M2M and consumer remote provisioning systems have also opened up new subscription management and local profile assistant (LPA) function roles, with opportunities for SIM vendors as well as operators and OEMs to fulfil these. These roles will become more refined over time as end-users and ecosystem members adjust to the new processes.

OEMs and IoT device manufacturers

As multi-country connectivity is built in during the manufacturing process and then delivered locally, OEMs and IoT device manufacturers can enhance their global propositions. This would drive up global volumes of IoT devices. Remote provisioning may also spur greater sales of companion devices in the consumer market, through their own and third-party channels, including operators. Other opportunities include the streamlining of manufacturing and logistics, and the possibility of freeing some space in the mobile handset.

Remote provisioning could further propagate the rise of a multi-MVNO model, which OEMs or internet players could consider. Recent examples include Google's Project Fi in the US. However, up to now, the strategic intent of some of these multi-MVNO models has been more about technological experimentation and business model innovation (dynamic switching, refunded data, simplified tariff structures) and less about challenging the operator's position in the market.

Technology perspective: evolving IoT requirements may spur development of alternative SIM form factors

Although the embedded SIM is expected to become the mainstream solution in the long term, new SIM form factors are being explored, driven by use case requirements and technology evolution. Security remains the key priority for use cases that require a SIM and this will become even more pertinent as the threat landscape grows more complex. As a result, the embedded SIM is the most viable solution in the market at present and indeed the survey showed that there is a strong likelihood that the universal integrated circuit card (UICC) will continue to use a hardware-based secure element for secure applications. New physical form factors are being deployed that may provide up to 90% space reduction compared to the traditional removable SIM, and permanently embedding the SIM also means there is no longer a need for standardised hardware interfaces.

Although conceptual soft SIM solutions offer distinct cost, manufacturing and logistical benefits, they are currently not defined or standardised. There are also major concerns about the security of a pure software-based SIM solution.

Longer term, further evolution of form factors with a hardware-based secure element will likely be driven by the varied IoT use case requirements, while new SIM authentication algorithms may well be evaluated to overcome low power consumption challenges. Smaller device form factors that require authentication, security and storage could benefit from deeper integration of technologies. A system-on-chip approach, such as an integrated UICC, could be a viable option and a major disruptor to mainstream adoption of embedded UICC.

In the integrated UICC model there is no separate component as the system-on-chip solution combines the secure processor (for iUICC), the baseband processor and possibly other processors into one discrete hardware component. This solution can still satisfy today's security requirements but occupies no space in the device. System-on-chip technology is also likely to evolve and, as a result, may encompass all secure platforms in the device and be the trusted element for the SIM and other secure elements.

2 Evolution of the SIM and reconfiguration of the SIM operating model

2.1 Remote provisioning technology is driving SIM evolution

The SIM card has played a pivotal role in the rapid rise of mobile communications since it was introduced in 1991. The concept of the SIM was developed in order to separate the network subscription from the device. Through its evolution, from the traditional removable and non-reprogrammable SIM to the embedded SIM with remote SIM provisioning, the SIM has adapted itself to the latest cellular technology developments and mobile ecosystem requirements while preserving its primary functions such as secure authentication and data protection.

According to GSMA Intelligence, there were a total of 7.9 billion mobile connections (including approximately 400 million cellular M2M) and 4.8 billion unique mobile subscribers[1] worldwide at the end of 2016, representing 65% penetration of the global population. This penetration is forecast to reach 73% by the end of 2020.

The traditional SIM card is a removable piece of plastic – a smart microprocessor chip built on universal integrated circuit card (UICC) technology, which is inserted into a mobile device for use on GSM, 3G UMTS and 4G LTE networks. It stores a single operator profile used for authentication and identification with the network, which is programmed during manufacture. Although the SIM card form factor has gradually shrunk since its introduction, the primary role of the SIM card has largely remained: to provide secure, identifiable and authenticated access to mobile networks.

A new approach to SIM technology was required by the evolving machine-to-machine (M2M) and Internet of Things (IoT) ecosystems. Specifically, more durable, tamper-resistant solutions were needed where the SIM profile could be updated remotely using over-the-air (OTA) technology. As a result, in recent years embedded form factors and remote provisioning technologies have been developed and deployed in some markets.

In this report we use the following definitions:

- Remote provisioning is the ability to remotely change the SIM profile on a deployed SIM card without having to physically change the SIM card itself. This capability is hardware-agnostic and can be deployed on removable and non-removable UICCs.
- The term embedded UICC (eUICC) is used to refer to a SIM card that can be remotely provisioned. Importantly, eUICC technology can be implemented on any SIM card form factor, including embedded and removable SIMs.
- An embedded SIM (eSIM) is one that supports remote provisioning and is physically integrated into the device during manufacture, such that it cannot easily be removed from the device and replaced with another SIM.

[1] A unique mobile subscriber is a person who subscribes to mobile services. It differs from a mobile connection as a unique user can have multiple connections.

Figure 1 shows the four possible variants of a SIM card based on whether the form factor is removable or embedded and whether it is reprogrammable (supports remote provisioning) or not.

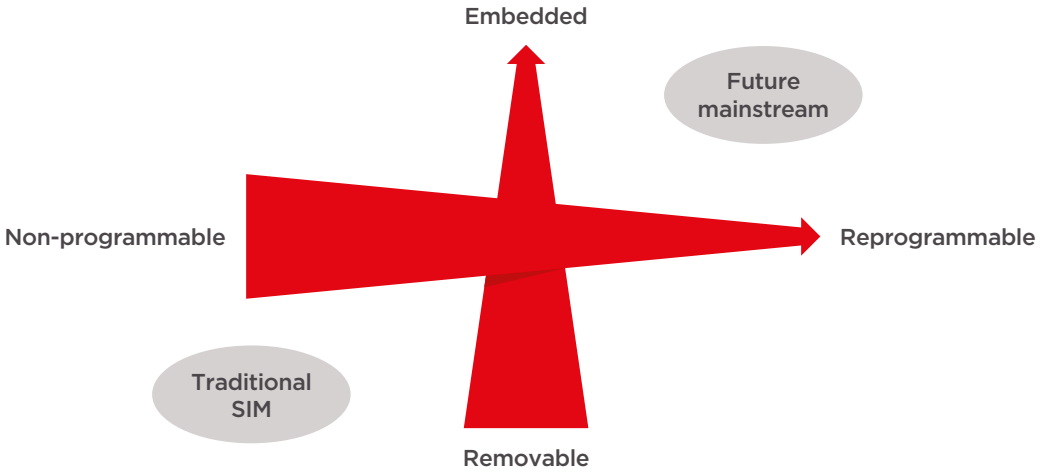

Figure 1: Types of SIM card based on form factor and programmability
Source: GSMA Intelligence

Remote provisioning technology is now widely deployed in the M2M market, where proprietary solutions and solutions based on the GSMA specification coexist. However, the GSMA's Remote SIM Provisioning Specification is now established and is the preferred, standardised approach in the market following its launch in December 2013. There are two standardised eUICC M2M form factors (MFFs): MFF1, which is solderable and socketable; and MFF2, which is soldered only. Both have the same printed circuit board footprint.

The standardisation of embedded SIM and remote provisioned technologies in the consumer market has also occurred over the last year. In February 2016 the GSMA published the technical specification for connecting consumer companion devices (such as tablets, smart watches and fitness devices). In November 2016, a specification for the consumer device market as a whole (including handsets) was released.

The release of specifications covering both device categories (M2M and consumer) is a key milestone for the industry. The GSMA will be working towards harmonisation of these specifications into a single remote SIM provisioning specification over time.

2.2 Reconfiguring the SIM operating model to new roles and processes

The evolution of the remotely provisioned SIM will affect the existing SIM supply chain dynamics, processes and distribution cycle. The management and ownership of the SIM credentials (including operator profiles) is a crucial aspect of the eUICC remote provisioning system. As such, there has been a reconfiguration of roles within the value chain for both the M2M and consumer specifications.

M2M

Two new server-based roles have been introduced to facilitate the selection and installation of subscription profiles:

- Subscription manager – data preparation (SM-DP): this acts on behalf of the MNO. It securely packages profiles to be provisioned on the eUICC and manages the installation of these profiles onto the eUICC.

- Subscription manager – secure routing (SM-SR): this ensures the secure transport of both eUICC platform and eUICC profile management commands in order to load, enable, disable and delete profiles on the eUICC in accordance with the MNO's policy rules.

Consumer

The consumer remote provisioning system architecture introduces the local profile assistant (LPA) – a piece of software that enables local profile services such as profile download and profile management, with the specific level of user interaction dependent upon device capabilities. The LPA consists of three parts:

- the LUI (local user interface) allows the end user to perform local profile management on the device

- the LPD (local profile download) plays a proxy role for the efficient download of a personalised profile which has been encrypted for a target eUICC

- the LDS (local discovery service) retrieves addresses of one or more SM-DPs from the subscription manager – discovery service (SM-DS).

Importantly, the LPA may be stored and executed in the eUICC and/or in the device; the way the LPA is implemented across different devices or device types is not specified and will be market driven. The LDS role is to enable any network to connect to any device, even if the specific device address or network location at any given point in time is unknown. This enables any network to provide a subscription to any device, should the device owner agree. Given this crucial function, it is important that the LDS is operated in a neutral and transparent manner.

From a customer's perspective, independent ownership of the online discovery service allows them to reap the benefits associated with this evolution of SIM technology. To maintain the existing level of competition among mobile operators, it is important that all operator profiles (and tariffs) are made available for selection. Only one profile can be active on a device at any point in time.

Proprietary solutions where the ownership of the online discovery service is not independent could limit customer choice, affecting competition. Although there is a viable opportunity for operators to collaborate on the ownership of this function, this may be challenging to achieve in reality due to differing business objectives.

Further to this, although the end user operator interface (ESop) is not included within the specification, it forms a crucial part of the operator/customer relationship as the operator-owned interface for a user to subscribe directly to the operator's service.

3 Emerging use cases for the SIM

As the broader mobile ecosystem continues to evolve, new use cases for the SIM emerge across two main categories: cellular connectivity and value-added services that leverage the SIM's established strengths (secure authentication and data protection). Table 1 summarises these emerging use cases.

Category	Emerging use case	Most suitable type of SIM	Industries likely to benefit the most	Devices likely to benefit	Merits of the SIM
Cellular connectivity	**Machine/device authentication and connectivity in the IoT market**	Reprogrammable embedded for some use cases. Any type of SIM for other use cases	• Automotive • Utilities • Healthcare • Agriculture	• Connected cars • Smart meters • Sensors	• Wide coverage • Ultra reliability
Value-added services	**Mobile-based digital identity and authorisation**	Any SIM (reprogrammable or non-reprogrammable; removable or embedded)	• Public administration • Public transportation • Banking, finance, insurance • Healthcare • Education	• Handsets • Wearables	• Security • Wide coverage • Wide adoption

Table 1: Emerging use cases for the SIM
Source: GSMA Intelligence

3.1 New use cases for cellular connectivity: the rise of the mobile Internet of Things

The emerging Internet of Things ecosystem will drive a proliferation of new devices, applications and services – for both individuals (e.g. connected homes and cars) and enterprises (e.g. connected workplace, connected industrial devices) – that require secure authentication, connectivity and, in most cases, remote management. All categories of respondents to the survey largely concurred that machine/device authentication and connectivity is a strong emerging use case for the SIM over the next five to ten years.

However, it's important to consider the role of cellular connectivity in the IoT ecosystem as several connectivity options are being deployed to best suit a variety of devices, use cases, network requirements (reliability, availability and latency) and other needs (such as low/high data volumes, low/high device/service cost, low/high energy consumption).

Cellular versus non-cellular connectivity

The majority of IoT devices – typically in indoor environments – will likely be connected by radio technologies, such as Wi-Fi and Bluetooth, which operate on unlicensed spectrum and are designed for short-range connectivity. Other IoT devices that require wide-area network coverage, coverage on the move, lower latency and ultra reliability will likely be primarily connected by cellular networks using licensed spectrum. This cellular connectivity will be provided by either traditional cellular networks (2G/3G/4G/5G) or the emerging low power, wide area networks (EC-GSM-IoT, LTE-M and NB-IoT).

The mobile networks currently available (2G/3G/4G) will likely account for a minority share of total IoT device connections; however, 5G has the potential to further strengthen a hyper-connected society and the role of cellular connectivity. The aim of the 5G concept is to integrate LTE (in licensed and unlicensed bands), Wi-Fi and cellular IoT technologies, together with at least one new 5G radio interface. International bodies, including 3GPP and ITU, are working to standardise 5G. Commercial services are not expected until the early 2020s.

The survey pointed to high expectations from both telecoms operators and non-operators that automotive, utilities and healthcare will benefit from the evolution of the SIM over the next five to ten years (see Figure 2).

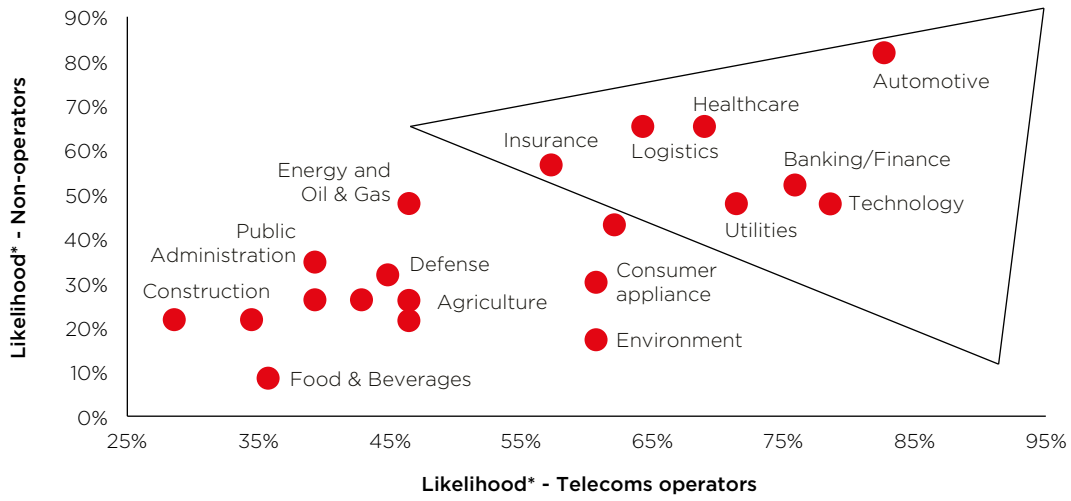

Figure 2: Industries likely to benefit the most from the evolution of the SIM
Question: Which industries are likely to benefit the most from the use/evolution of the "physical SIM" (e.g. smart card, embedded) over the next five to ten years?
**Likely + Very Likely as a percentage of total responses. Scale: Very Unlikely, Unlikely, Moderately Likely, Likely, Very Likely.*
Source: GSMA Intelligence

New authentication algorithms for IoT may be required

Identification and authentication of devices play a significant role in the security protocols for IoT, particularly in a heterogeneous network environment where there will be different requirements in terms of frequency and speed of communication, the amount of data required to be communicated and security levels. As a result, SIM authentication processes for 5G may evolve to accommodate the proliferation in device types and requirements. This will require collaboration among industry stakeholders as 5G moves from standardisation to commercial deployment.

Low power consumption is a critical requirement for many classes of IoT device, but some may not have the required computing resources (memory, power, storage etc.) to support the current authentication protocols. As a result, new more efficient algorithms for authentication and authorisation may need to be evaluated. In the survey, an overwhelming majority of respondents thought that new algorithms for authentication would be required. This view was supported by both telecoms operators and non-operators.

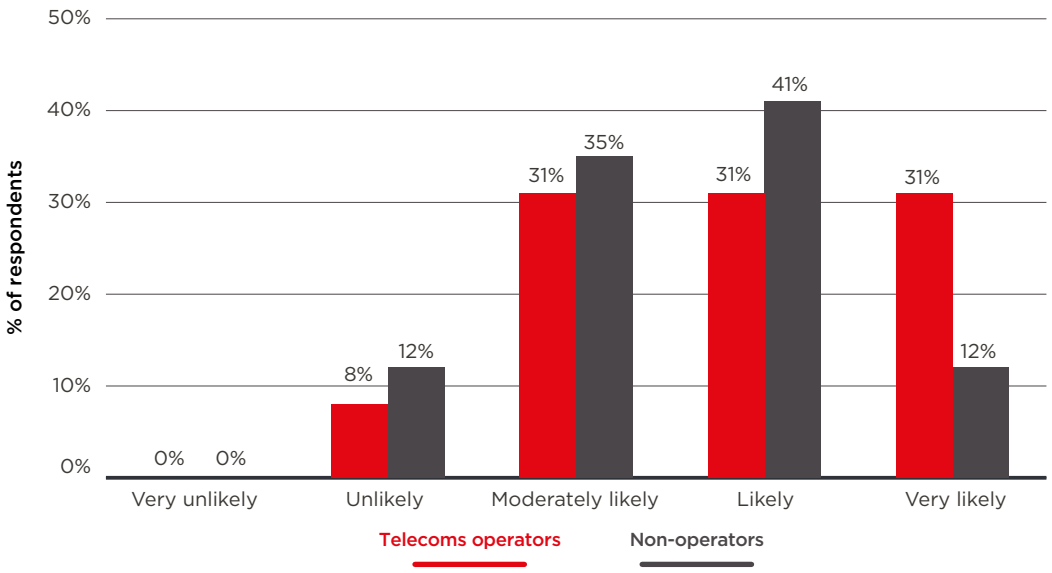

Figure 3: Need for new authentication algorithms for IoT
Question: Looking at the potential evolution of "Authentication" and "Security", which of the following scenarios are most likely to happen? "IoT will require new algorithms for authentication".
Source: GSMA Intelligence

Cellular M2M forecast – 1 billion connections worldwide by 2020

According to GSMA Intelligence, the number of cellular M2M connections (2G/3G/4G) will grow three-fold worldwide between 2015 and 2020, reaching 1 billion. Nearly half of the connections will be in Asia Pacific, followed by North America and Europe.[2]

This growth rate could accelerate if certain market conditions are achieved. Possible growth stimulators are:

- additional government policies in key sectors such as utilities, smart cities, automotive and healthcare
- module cost reduction
- low-cost standardised solutions for specific requirements (e.g. low data, long battery life)
- increased API standardisation
- greater assurance of end-to-end security
- industry-wide collaboration to drive scalability, go-to-market and a standardised approach worldwide.

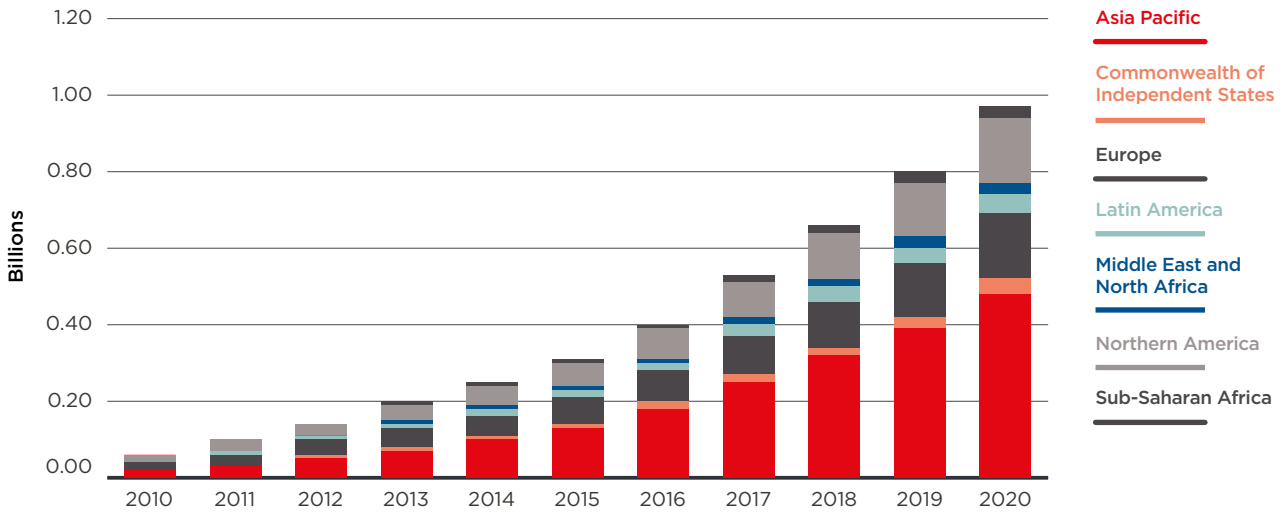

Figure 4: Cellular M2M connections worldwide – current trajectory
Source: GSMA Intelligence

[2] The forecast counts M2M connections that access mobile networks ("cellular M2M") and excludes consumer electronic devices such as smartphones, phablets, tablets and e-readers.

3.2 Digital identity and authentication as emerging SIM-based value-added services

Several initiatives have been tested and deployed around new functions and use cases that leverage the SIM's established strengths (secure authentication and data protection) to support the provision of value-added services such as mobile payments, identity, ticketing and couponing/loyalty. These services go beyond the traditional and established functions of the SIM.

According to the survey, digital identity is the value-added service most likely to gain momentum, as the SIM is largely considered by both telecoms operators and non-operators (OEMs, SIM vendors, industries) as a secure hardware asset on which to store identity credentials. As we advance further into the digital age, the ability to prove a unique identity in the virtual world, as well as the physical world, is increasingly important for economic and social inclusion.

The storage of personal digital certificates and the use of the SIM to authorise access (e.g. to an office, bank, airport gate, cinema, sports/music venue) are also considered fairly likely to be adopted.

Mobile operators boast a good position to support mobile identity initiatives worldwide; they have the largest widespread communication system due to wide cellular network coverage of the population, wide agent distribution, and billions of customer relationships (4.8 billion unique subscribers in 2016, 5.7 billion by 2020[3]). They are also already subject to identity-related requirements (e.g. mandatory SIM registration and know-your-customer, or KYC, obligations for communications services).

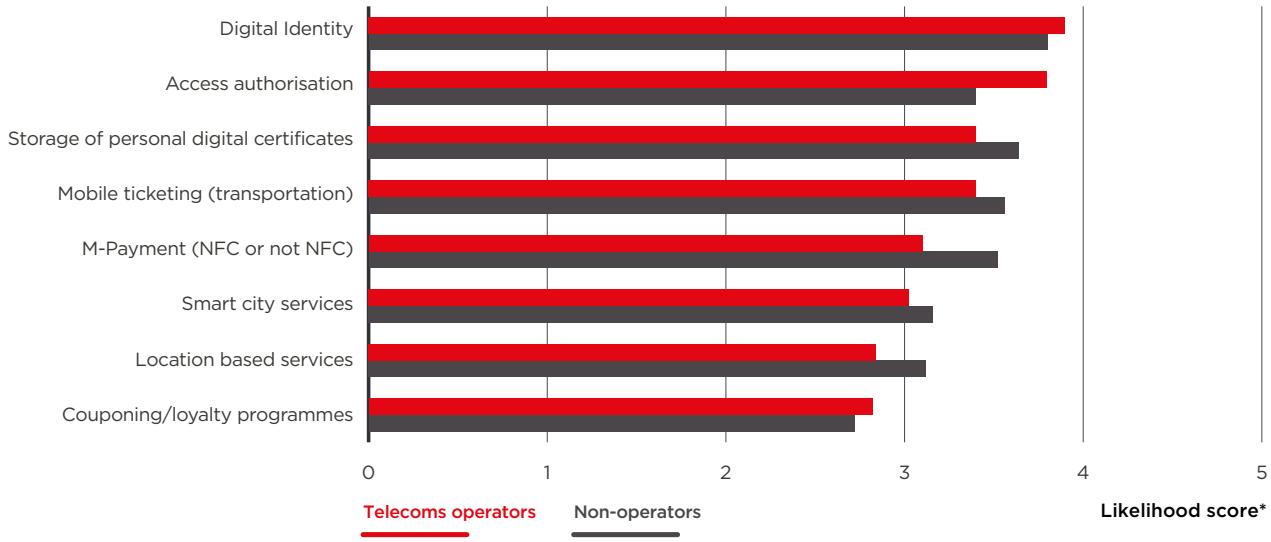

Figure 5: Value-added services as use cases for the SIM over the next five to 10 years
Question: Looking at existing/potential use cases for the "physical SIM" (e.g. smart card, embedded), which of the following are most likely to emerge/gain strength over the next five to 10 years?
**Overall likelihood score (1=lowest; 5=highest). Scale: Very Unlikely, Unlikely, Moderately Likely, Likely, Very Likely.*
Source: GSMA Intelligence

[3] Source: GSMA Intelligence

Potential services include:

- verifying government-issued identity credentials against a centralised database in real time
- authenticating identity in transactions
- certifying and time-stamping documents and signatures
- introducing or complementing national identity systems, such as for birth registration, driving licences and other public sector uses.

Although some leading mobile operators have successfully deployed solutions across multiple countries, the deployment of SIM-based mobile payment and mobile ticketing services continues to lose momentum. This is mostly due to the presence of established alternatives such as host card emulation (HCE) for mobile payments, the success of mobile payment services provided by global companies (e.g. Apple, Google, Samsung) and industry fragmentation, particularly in the public transport industry.

SIM-based smart city services are considered less likely to find success than other VASs because short-range connectivity (e.g. local area network connections including Wi-Fi, Bluetooth, device-to-device and Ethernet) and – to a lesser extent – LPWA wireless networks offer more suitable solutions. Nevertheless, the number of smart city IoT initiatives deployed by mobile operators – regardless of SIM-based connectivity – in partnership with governments, city planners and digital service providers will likely continue to grow as mobile operators can bring their expertise in connectivity and data analytics. Main areas include smart transport solutions to reduce congestion and optimise use of public transport; waste management and smart environment solutions; remotely connected CCTV and automated incident detection; parking; and smart street lighting.

3.3 Other use cases for cellular connectivity face challenges

In the consumer market, the uptake of SIM-based companion devices (e.g. tablets, smart watches and fitness trackers) continues to grow slowly, mostly due to the use of smartphones as a gateway and limited standalone use cases for wearables. However, the release in November 2016 of specifications for the consumer device market as a whole could strengthen operators' multi-device consumer propositions and incentivise adoption of embedded SIM-based companion devices.

According to the survey, IoT devices are likely to benefit the most from the evolution of the SIM, followed by smartphones, wearables and tablets. Within this positive outlook for IoT devices, telecoms operators are slightly more positive about the market outlook than non-operators, which may reflect higher expectations of cellular connectivity compared to non-cellular connectivity in the wider IoT connectivity ecosystem.

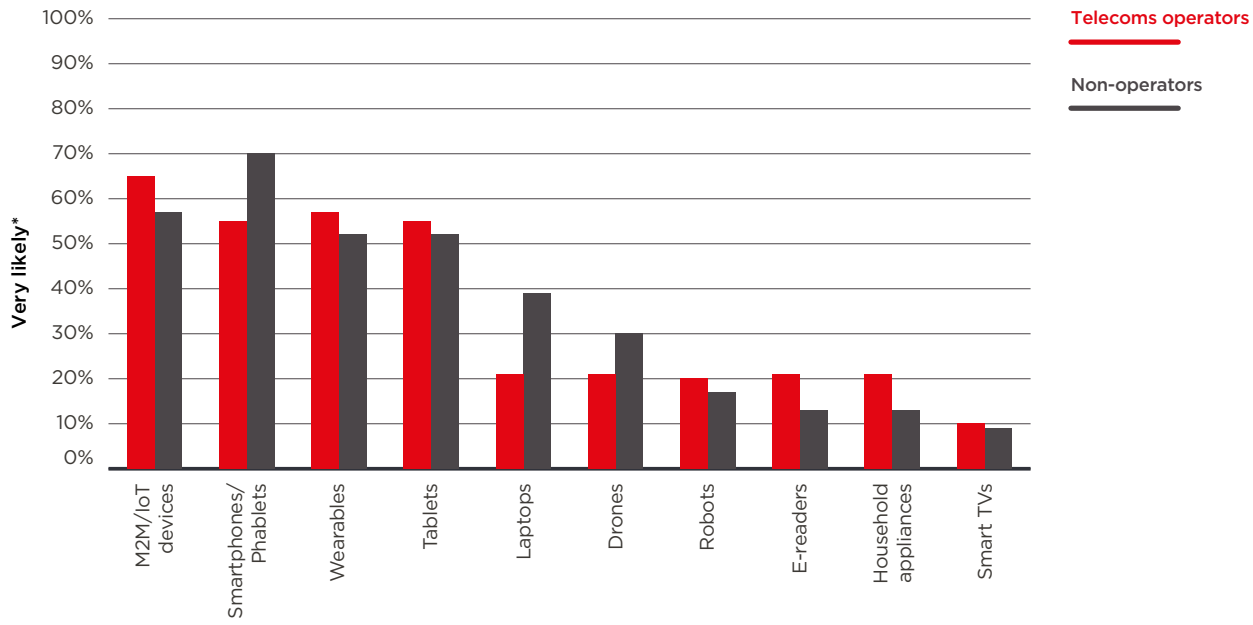

Figure 6: Devices/machines likely to benefit the most from the evolution of the SIM
Question: Which devices/machines are likely to benefit the most from the use/evolution of the "physical SIM" (e.g. smart card, embedded) over the next five to 10 years?
**Very Likely as a percentage of total responses. Scale: Very Unlikely, Unlikely, Moderately Likely, Likely, Very Likely.*
Source: GSMA Intelligence

Following the November 2016 release of specifications for the consumer device market as a whole, smartphones may benefit from the transition to an embedded SIM model as OEMs free up space in devices for other applications. Operators may take the initiative to launch multi-device subscriptions centred on the smartphone. The outlook for the adoption of remotely provisioned SIMs in the handset market and the possible implications for the mobile ecosystem are discussed in the *Market perspective* chapter.

Wearables are the second most likely device to benefit from the evolution of the SIM according to operators, and are ranked highly among non-operators too. The embedded SIM with RSP eliminates the need to incorporate SIM housing components and helps maximise the space available in the device. Furthermore, the November 2016 release of specifications that covers all consumer mobile devices (including handsets) could spur greater adoption of companion devices as consumers connect all their mobile devices to a single subscription. However, the key challenge in the cellular connected wearables market is the development of their own core functionality and standalone value-added services beyond fitness and healthcare.

For the time being, drones represent a weaker use case compared to other devices. However, Silicon Valley giants (e.g. Amazon, Google and Facebook) have made significant R&D investments in this market recently, while the venture-capital community has fuelled the growth of dozens of new start-ups in the space. Some mobile operators such as Verizon Wireless in the US have announced their intention to launch SIM-based plans for drones. The number of use cases for drone technology is growing across three main categories – industrial applications, connectivity and internet access, and logistics and delivery. Although most use cases remain at the prototype and testing phases, cellular connectivity could play a role in the logistics and delivery-related use cases.

4 Technology perspective

4.1 New use case requirements may spur development of alternative SIM form factors

The rise of the M2M and IoT ecosystems is driving a vast and rapidly changing set of use cases and devices that demand identification, authentication and security. This demand will only intensify as the development of 5G moves from standardisation to commercial availability at the end of the decade. However, new form factors using alternative technologies are being explored, and these could be used to service the growing range of requirements.

Table 2 summarises the main alternative solutions to the SIM (a removable or embedded UICC) as mentioned by respondents in the survey, for the use cases related to cellular network connectivity.

Security	Identification, authentication, authorisation	Remote management
• Device hardware and certificates • Embedded secure element • Soft SIM • Software token on device • System on chip • Trusted execution environment	• Device-based solutions • Embedded secure element • Mobile apps • SD card • Soft SIM • System on chip • Trusted execution environment	• Cloud • Device management solutions • Embedded secure element • Soft SIM • Software solutions • System on chip • Trusted execution environment

Table 2: Main alternatives to SIM as noted in the survey*

**Alternative solutions listed by survey respondents, in alphabetical order.*

Source: GSMA Intelligence

Taking account of these alternatives, we below analyse some of the main advantages and disadvantages of the embedded SIM with three alternatives: integrated UICC or iUICC (a system-on-chip solution), the soft SIM and the trusted execution environment (TEE).

An embedded SIM (eSIM) supports remote provisioning and is physically integrated into the device during manufacture, such that it cannot easily be removed from the device and replaced with another SIM.

- ✓ Based on a solution (UICC) that is undisputed in servicing almost 8 billion connections
- ✓ Advanced security underpinned by a mix of hardware and software cryptophytic algorithms
- ✓ Independent hardware-based secure element that can be certified
- ✓ Reduces logistical and manufacturing costs compared to a traditional removable SIM
- ✗ Takes up physical space within the device (versus soft SIM, iUICC or TEE), which may impact flexibility
- ✗ Cost may be a barrier for cheap devices (such as sensors)

An integrated UICC (iUICC) is conceptually a system-on-chip (SoC) solution in which the UICC is integrated as a separate secure processor core alongside other cores. This is not currently standardised by ETSI but there is a work item looking at standardising platforms such as iUICC. SoC solutions would integrate a secure processor that leverages external non-volatile shared memory, using cryptographic means to protect the data. The iUICC solution is meant to meet or exceed the current UICC's level of security.

- ✓ Evolution of the system-on-chip approach that is common in mobile device architecture
- ✓ Reduces physical space requirements and is more cost effective
- ✓ Security benefits versus a pure software solution (soft SIM, TEE)
- ✗ Currently not standardised
- ✗ There are assurance concerns as this is a different model that is new to the industry

The soft SIM is not standardised and there are varying definitions of the concept. For the purposes of this report, a soft SIM is a collection of software applications and data that performs all the functionality of a SIM card but does not reside in any kind of secure data storage or use a secure processor. Instead, it is stored in the memory and processor(s) of the communications device itself (i.e. there is no SIM hardware).

- ✓ Saves space within the device and no physical integration required
- ✓ No cost to device manufacturer and simplifies value chain
- ✓ Simplified deployment model
- ✗ Soft SIM is a concept that has not been standardised
- ✗ No clear security certification due to software-only architecture
- ✗ More susceptible to security breaches given architecture design. Cannot ensure critical data loads are secured
- ✗ Uncertainty as to whether it would be a viable authentication mechanism

Trusted execution environment (TEE) is a secure area of the main processor in a smartphone or connected device which ensures that sensitive data is processed and protected in an isolated, trusted environment.

- ✓ Cost effective and removes some supply chain and logistical complexities
- ✓ Ease of integration and application updates
- ✗ A UICC application running within the TEE is currently not standardised
- ✗ TEEs use shared memory
- ✗ There are assurance concerns as this is a different model that is new to the industry

4.2 As threat landscape develops, hardware-based secure element approach remains key

While all four of the above solutions have their merits and drawbacks, security remains the priority for use cases that require a SIM. This will become even more pertinent as the threat landscape becomes more complex, particularly in the high-end IoT and smartphone markets. As a result, the embedded SIM, which uses a hardware-based secure element, is deemed the most viable solution in the market at present and is fit for purpose to serve the evolving use case requirements. According to the survey, 70% of telecoms operators and 79% of non-operators viewed it as either likely or very likely that SIM applications will continue to use a hardware-based secure element for storage and execution.

However, in the longer term, a further evolution of the SIM card form factor with a hardware-based secure element will likely be driven by the varied use case requirements in the IoT markets. In particular, smaller device form factors that require authentication, security and storage may benefit from deeper integration of technologies.

A system-on-chip approach, such as an integrated UICC, could be a viable option if certification and security challenges can be overcome. This approach is considered quite likely to happen over the next five to 10 years according to the survey respondents, with 82% of telecoms operators and 72% of non-operators viewing it either likely or very likely that the UICC architecture will migrate to a more integrated approach such as an iUICC.

In the integrated UICC model there is no separate component as the system-on-chip solution combines the secure processor (for iUICC), the baseband processor and possibly other processors into one discrete hardware component. This solution can still satisfy today's security requirements but occupies no space in the device. System-on-chip technology is also likely to evolve and, as a result, may encompass all secure platforms in the device and be the trusted element for the SIM and other secure elements.

Although software-based SIM solutions offer distinct cost, manufacturing and logistical benefits, they are not currently defined or standardised. There are currently major concerns about the security of software-based solutions for use cases that require a SIM. The survey shows that, overall, respondents viewed the possibility that UICC will become a fully software-based platform as less likely (see Figure 7). However, there are a range of IoT connectivity options that do not necessarily require a SIM and where user equipment may be authenticated within the software layer. The development of alternative solutions will ultimately be market driven, but there are barriers to overcome in terms of security, certification, regulation, industry acceptance and collaboration among industry players.

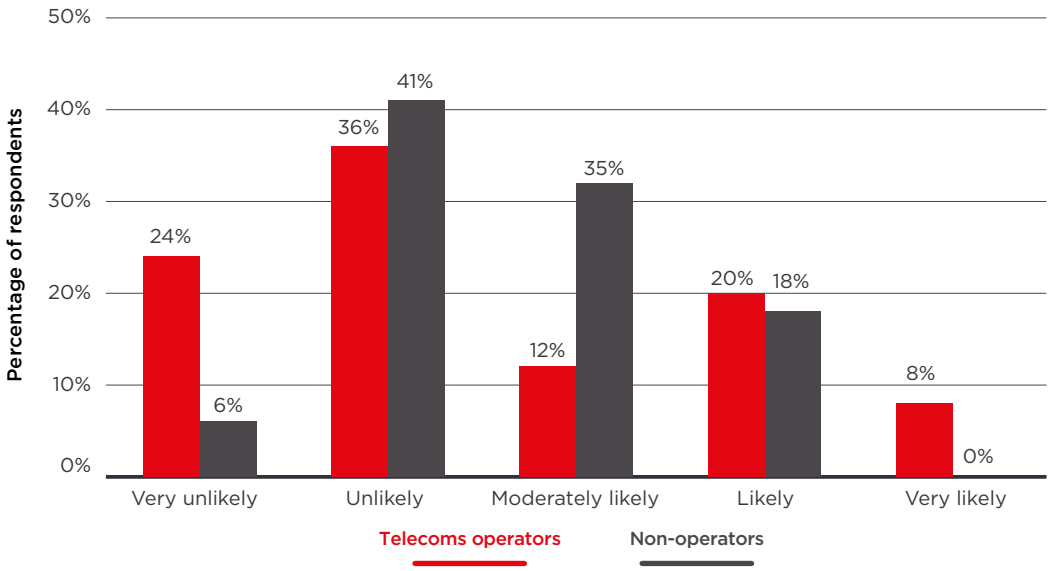

Figure 7: Likelihood that the UICC will become a fully software-based platform

Question: Looking at the potential evolution of the "UICC-physical SIM platform" (e.g. smart card, embedded), which of the following scenarios are most likely to happen? "The UICC will become a fully software-based platform".

Source: GSMA Intelligence

5 Market perspective

5.1 Transition to remote provisioning in handset market will likely take many years

The embedded SIM with remote provisioning has been embraced as a mainstream technology in the cellular M2M market, having addressed many of the limitations of using the traditional removable SIM. In the consumer market, a number of leading mobile ecosystem companies – including operators, OEMs and SIM vendors – have supported the November 2016 launch of the second phase of the GSMA's remote provisioning specification, which now covers the consumer market as a whole.

Although a limited number of proprietary solutions for remote provisioning in the consumer market already exist, recent ecosystem collaboration on the GSMA specifications for remote provisioning consumer devices shows that the industry has aligned to a single, de facto standardised approach; this helps avoid market fragmentation and possible interoperability issues.

Moreover, the standard remote provisioning specification will ensure that smaller service providers and OEMs continue to have equal access to market opportunities.

As consumers increasingly access and consume a variety of services and content through their array of connected devices, and as privacy and security threats rise, the remotely provisioned embedded SIM can support the development of a connected life while providing improved security. Consumers can use a plethora of devices, all securely connected to ubiquitous mobile networks. They can also save time through faster subscription sign-up and swapping, for example.

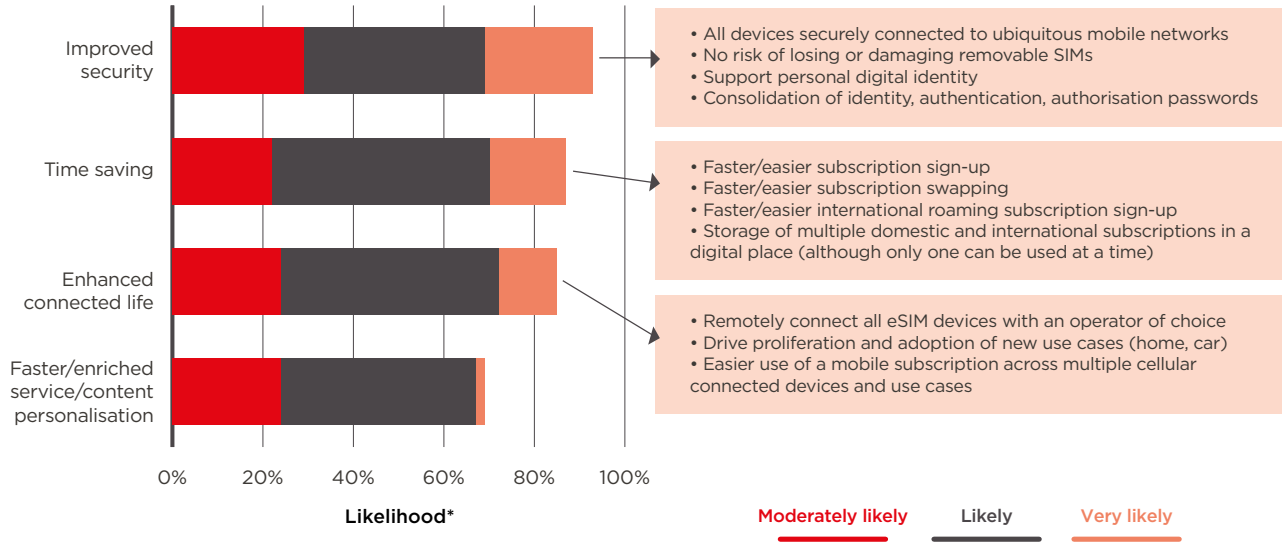

Figure 8: Benefits for consumers

Question: How likely will consumers benefit from a proliferation of "physical SIM" (e.g. smart card, embedded) use cases?.

**Moderately Likely + Likely + Very Likely as a percentage of total responses. Scale: Very Unlikely, Unlikely, Moderately Likely, Likely, Very Likely.*

Source: GSMA Intelligence

Mainstream adoption of a standardised remote provisioning technology in the handset market will likely take a number of years due to supply-side and demand-side factors. There will be a period of reconfiguration as ecosystem members adjust to new manufacturing, logistical and supply chain processes, as well as a phase of customer education and associated customer service. There is also a huge installed base of handsets with a removable SIM that will remain in circulation, and handset replacement cycles are lengthening. The average handset replacement cycle is two to three years in most developed markets and four years in the majority of emerging markets.

We therefore expect to see a gradual transition. The traditional removable SIM (which contains a single operator profile) will likely continue to account for the majority of connections in the mid-term, but will co-exist with multiple SIM model solutions. Initial deployments are likely to be on specialist devices, or in mixed deployment scenarios with traditional physical SIMs. Ultimately, long-term adoption will be driven by OEMs implementing the technology and mobile operators enabling support for remote provisioning. Table 3 shows some potential adoption paths by key category of device, related to the adoption of GSMA standardised (e)UICCs.

	Traditional solution	Removable SIM with RSP	Dual removable and embedded SIM with RSP	Embedded SIM no RSP	Embedded SIM with RSP
Form factor	Removable	Removable	Removable + Embedded	Embedded	Embedded
Reprogrammable	✖	✔	✔	✖	✔
Current and potential SIM adoption scenarios*					
Handsets	✔	Near to mid-term		Longer term	
Tablets	✔	Near to mid-term[4]		Longer term	
Wearables					✔

Table 3: Embedded SIM adoption scenarios in the consumer market
**related to adoption of GSMA standardised (e)UICCs*
Source: GSMA Intelligence

[4] Proprietary reprogrammable and embedded SIM solutions exist in the tablet market. Most notably, the Apple SIM for select versions of its iPad range.

The adoption of embedded SIMs will likely occur in three phases:

- Removable SIM cards capable of supporting remote provisioning (removable eUICC) expand into the handset and tablet markets.
- The initial array of devices incorporating embedded SIMs contain a removable SIM card slot. This rationalises the manufacturing requirements for OEMs, which can distribute one device to work globally, accommodating markets where embedded SIMs may take longer to be embraced.
- Longer term, fully embedded SIM solutions (with no removable slot) become prevalent in both handsets and tablets.

Embedded SIM adoption in the consumer wearable market remains at a nascent stage; the specification only launched in February 2016. Solutions such as the Samsung Gear S2 and Gear S3 were launched in 2016, incorporating cellular connectivity using a GSMA-specified embedded SIM. Although global sales of connected devices such as wearables have somewhat underperformed compared to initial expectations, an embedded SIM remains an attractive option to provide flexibility and connectivity, allowing the device to operate independently of a smartphone.

As discussed in the technology perspective, a system-on-chip approach – such as an integrated UICC – could be a viable option in the longer term and a major disruptor to mainstream adoption of embedded SIM. Digital ecosystem fragmentation and slow business model innovation are other potential barriers to adoption of the embedded SIM over the next few years as highlighted by the survey.

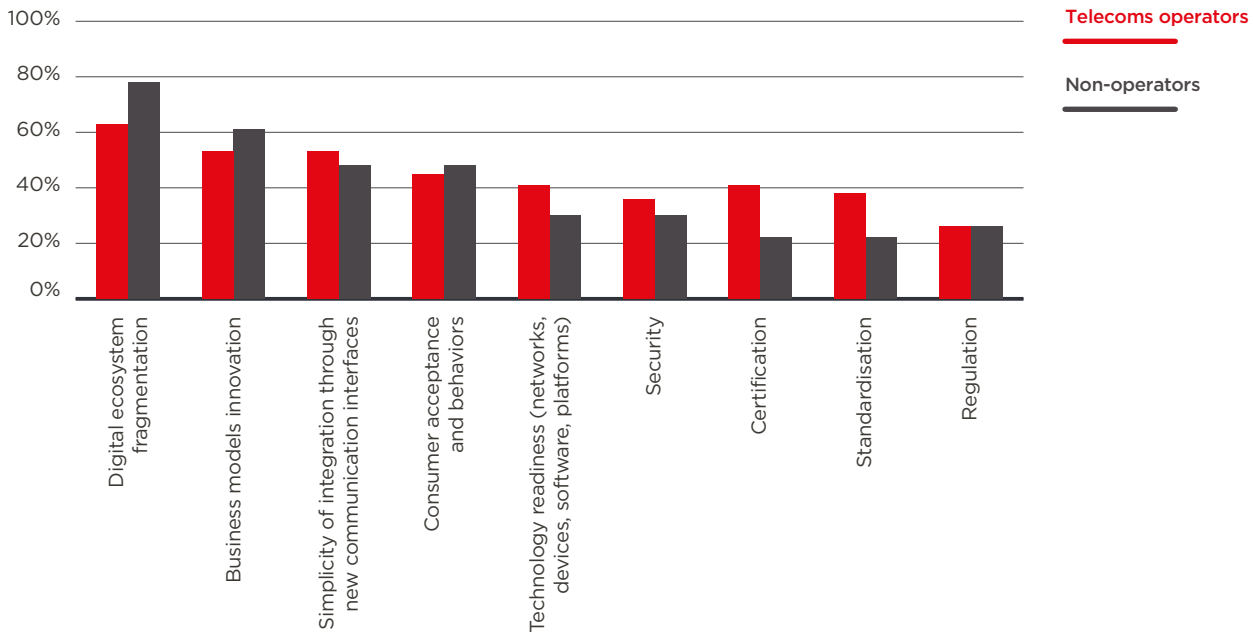

Figure 9: Main barriers to mainstream adoption of the embedded SIM

Question: What are the main challenges to the proliferation of "physical SIM" (e.g. smart card, embedded) use cases over the next five to 10 years?

Barrier and Big Challenge as a percentage of total responses. Scale: Not a challenge at all, Small challenge, Moderate challenge, Big challenge, Barrier.

Source: GSMA Intelligence

5.2 Challenges and opportunities are emerging for the mobile ecosystem

The transition to a remotely provisioned SIM provides new challenges and opportunities for the mobile ecosystem and will affect operator business models and market dynamics. The result of this impact is not certain at this stage and will take place over a number of years.

Remote provisioning introduces challenges for mobile operators…

The survey provides insight into the main operator challenges associated with the evolution of the SIM towards remote provisioning (Figure 10).

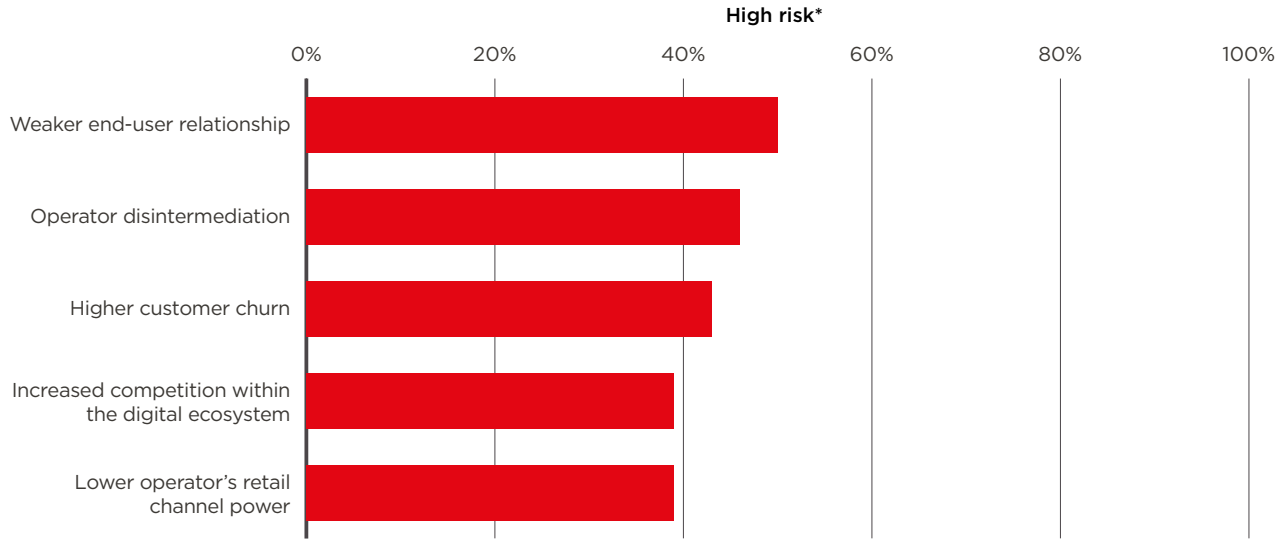

Figure 10: Main operator challenges
Question: What are the main telecoms operator concerns/risks associated with the future/evolution of the "physical SIM" (e.g. smart card, embedded)?
**High risk as percentage of total. Scale: Low Risk, Moderate Risk, High Risk.*
Source: GSMA Intelligence

The key change that a remotely provisioned SIM enables in the broader customer journey is that users can manage their subscription directly on a device, which further accelerates customer relationship virtualisation. A clearer separation of the cost of the network service from the device may leave operators more vulnerable to disintermediation given that handsets can be sold through other distribution channels (rather than operator channels). Indeed, while operators are one of the primary channels for handset sales, particularly in developed countries, their share of the global handset distribution channel has declined in recent years.

Furthermore, with a slowdown in smartphone sales in developed markets, OEMs are differentiating their business models in order to improve their customer relationships. For example, Apple launched its iPhone Upgrade Program, a leasing scheme in which a subscriber chooses the operator service via Apple and is able to upgrade to the latest iPhone every 12 months. Handset financing plans have been widely embraced in the US since their launch in 2013, but if handset financing takes off on a larger scale and in other markets, this segment may be subject to greater competition from other stakeholders (such as OEMs, third-party retailers and financial services companies). The potential combination of non-operator handset financing plans and remote SIM provisioning – in which a consumer has flexibility over the choice of network service – may present significant new competitive challenges for operators.

Remote provisioning is, initially, likely to be a factor primarily in devices used with prepaid accounts (which are not typically tied to a single operator) or SIM-only deals (where the SIM is used in conjunction with a device that has been purchased separately). Churn may increase in markets dominated by pay as you go, since customers can switch operators more easily, and price competition could intensify through short-term promotions. However, this does not necessarily mean that a customer will choose to switch networks. Other factors such as network quality, coverage and customer service are important considerations for customers in choosing an operator. Furthermore, existing obligations with regards to KYC such as identity and credit checks will remain, and mobile number portability processes are currently not expected to change.

Remote provisioning could further propagate the rise of a multi-MVNO model, which OEMs or internet players might consider. Examples include Google's Project Fi in the US. In such cases, they may contract with multiple network operators in an individual market or across multiple countries and become the key interface for customers across devices and connectivity. However, up to now the strategic intent of some of these multi-MVNO models has been more about technological experimentation and business model innovation (dynamic switching, refunded data, simplified tariff structures) than about challenging the operator's position in the market.

...but also offers opportunities for operators and the broader mobile ecosystem

The transition to standardised remote provisioning technology will open up new opportunities, or strengthen existing industry trends, for all sectors in the mobile ecosystem – telecoms operators, SIM vendors, OEMs and IoT device manufacturers and IoT industries. These opportunities, as outlined in Table 4, include new revenue streams in IoT, the rise of a subscription management role, enhanced consumer propositions and the streamlining of manufacturing and logistics.

The emerging service add-on model provides greater flexibility and scalability compared to an after-market model, potentially driving up global volumes and a proliferation of use cases. In the service add-on model, the connectivity functionality is built in during the manufacturing process across a number of devices (including cars), with IoT applications and services coming to market at a later stage and across multiple countries. IoT services and applications will likely take the lion's share of the IoT ecosystem revenue, followed by IoT devices and to a lesser extent connectivity.

Operators	• Enhanced B2C propositions through multi-device and multi-user subscriptions and device subsidies or financing. This includes enhanced digital interaction through websites, apps and chatbots. • Provide cellular connectivity to devices that have certain connectivity requirements such as wide coverage and ultra reliability. • Streamlining of manufacturing and logistics and a possible role in subscription management.
SIM vendors	• Take a subscription management role in the M2M and consumer markets. • Provide greater IoT security solutions in a market environment increasingly exposed to security issues. • Streamlining of manufacturing and logistics.
OEMs and IoT device manufacturers	• Greater global propositions as multi-country connectivity is built-in during manufacturing process and delivered locally at a later stage. • Greater sales of IoT devices in the M2M market and companion devices in the consumer market through all channels, including telecoms operators. • Streamlining of manufacturing and logistics, and freeing up of device space.
Industries	• Provide an increasing number of IoT services and applications through a service add-on model delivered locally. • Take a leading role in the emerging IoT ecosystem: services and applications will likely take the lion's share of the IoT revenue.

Table 4: Key benefits and opportunities for mobile ecosystem
Source: GSMA Intelligence

In addition to IoT revenue opportunities, the M2M and consumer remote provisioning systems open up new subscription management and LPA function roles, with opportunities for ecosystem members including SIM vendors, operators and OEMs to fulfil such roles. In the consumer system, the online discovery profile service will become more refined over time as end-users and ecosystem members get used to the new processes.

Mobile operators can enhance their end-user experience through customer propositions that leverage the ability to remotely provision an array of embedded SIM devices (including cars). Many operators already provide customers with shared data plans across devices and family members. However, the release of specifications for all consumer mobile devices can accelerate this trend.

Operators can add companion devices such as embedded SIM-enabled wearables, tablets or connected cars to a consumer's main data plan, thus improving take-up rates for those services and strengthening their acquisition and retention activities. They could also offer convergent plans with multiple devices under a single contract with the consumer more easily than they would with traditional removable SIMs. Customer segmentation and product innovation are important enablers as the range of offerings varies from individual to household propositions, and from off-the-shelf offerings to create-your-own package options – the latter have been successful in driving quad-play adoption in some Western European markets.

Greater sales of companion devices or connected cars – as a result of either data plan upgrades or the provision of a single subscription across multiple devices – would drive cellular data traffic up and improve customer experience and loyalty. Virtual reality devices can play a key role too. CRM and billing systems will need to adapt to possible changes deriving from multi-device subscriptions, and enhanced digital interfaces may become a differentiator (enhanced websites, apps, customer-support tools and chatbots). Sachet marketing and pricing models may also be adopted as a differentiation tool.

Operators could also differentiate their device offerings over time. Handset subsidies have been used for many years to drive postpaid subscriptions, particularly during the smartphone take-off period. The embedded SIM may offer a new wave of handset subsidies for operators, or the introduction of handset financing on a larger scale, as a way to evolve the customer relationship. It could also spur the adoption of companion devices through upgrade plans and subsidy and financing.

The development of the embedded SIM may also further strengthen the ongoing convergence between connectivity and content as a way to differentiate and enhance customer propositions in a changing ecosystem. Operators globally are increasingly investing in the development of exclusive mobile-only or at least mobile-first content to drive data traffic and subscriber loyalty. Prominent examples include Verizon's millennial-focused Go90 app, AT&T's planned streaming TV service based on DirecTV content, and Singtel's HOOQ in Asia. Many telecoms operators already provide customers with offerings that include content bundled with a mobile subscription, across three main segments – movies, sports and music.

Appendix

Methodology

This report was produced using a combination of primary research and analysis of key drivers, benefits, challenges and implications for mobile ecosystem players.

GSMA Intelligence conducted primary research in September and October 2016, by means of an online survey and phone interviews, to gather strategic insights and views on the future of the SIM from companies in the broader mobile ecosystem.

Both telecoms operators and non-operators participated in the survey; the respondent mix was approximately 60%/40% respectively. Surveyed organisations included:

- telecoms operators
- SIM vendors
- original equipment manufacturers (OEMs)
- companies from across a number of industries.

The survey covered several perspectives on the future of the SIM in the mobile ecosystem: potential use cases (e.g. services, industries, devices); key challenges and opportunities; benefits for consumers and enterprises; and technology and innovation.

Definitions

This report uses the term SIM to refer to the overall concept, including the hardware-based secure element and software applications and processes.

This is different from the concept of a soft SIM, which we define as a collection of software applications and data that performs all of the functionality of a SIM card but does not reside in any kind of secure data storage or use a secure processor. Instead, it is stored in the memory and processor(s) of the communications device itself (i.e. no SIM hardware).

Term	Definition
HCE	Host card emulation (HCE) is the architecture that makes a mobile phone act like a smart card. This could allow, for example, a mobile phone to be used in a payment transaction at point-of-sale instead of a contactless smart card.
NFC	Near-field communication (NFC) is a wireless technology that can transfer information between two devices within centimetres of each other. Detailed explanations of NFC can be found on the GSMA website.
Profile	A combination of file structure, data and applications provisioned onto, or present on, a UICC or eUICC.
- Operator profile	A profile with a primary purpose to enable access to a specific operator network.
- Operational profile	A profile containing one or more network access applications, associated network access credentials, operators' applications (e.g. SIM toolkit) and third-party applications.
- Provisioning profile	Similar to an operational profile. When installed on an eUICC, it enables access to communication network(s), only to provide transport capability for eUICC management and profile management between the eUICC and an SM-SR.
Remote provisioning	The ability to remotely change the SIM profile on a deployed SIM without having to physically change the SIM itself.
Secure element	A tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data.
SIM card	The subscriber identity module (SIM) card is the piece of hardware that stores the identity of the user and the related security keys that are used to authenticate users on a mobile network and validate the device being used.
Soft SIM	A collection of software applications and data that performs all of the functionality of a SIM card but does not reside in any kind of secure data storage or use a secure processor. Instead, it is stored in the memory and processor(s) of the communications device itself (i.e. no SIM hardware).
TEE	The trusted execution environment (TEE) is a secure area of the main processor in a smartphone or connected device which ensures that sensitive data is processed and protected in an isolated, trusted environment.
UICC	A universal integrated circuit card (UICC) is a physically secure computing device that conforms to the specifications written and maintained by the ETSI Smart Card Platform project. The SIM card is just one example of a UICC. Some banking cards and identity cards are also based on UICC architecture. A UICC can be any form factor.
- eUICC	The name given to a UICC capable of supporting remote provisioning such as the GSMA Embedded SIM Specification.
- iUICC	An integrated UICC (iUICC) is conceptually a system-on-chip (SoC) solution in which the UICC is integrated as a separate secure processor core alongside other cores. This is not currently standardised by ETSI but there is a work item looking at standardising platforms such as iUICC. SoC solutions would integrate a secure processor that leverages external non-volatile shared memory, using cryptographic means to protect the data. The iUICC solution is meant to meet or exceed the current UICC's level of security.

Table 5: Definitions of terms

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601