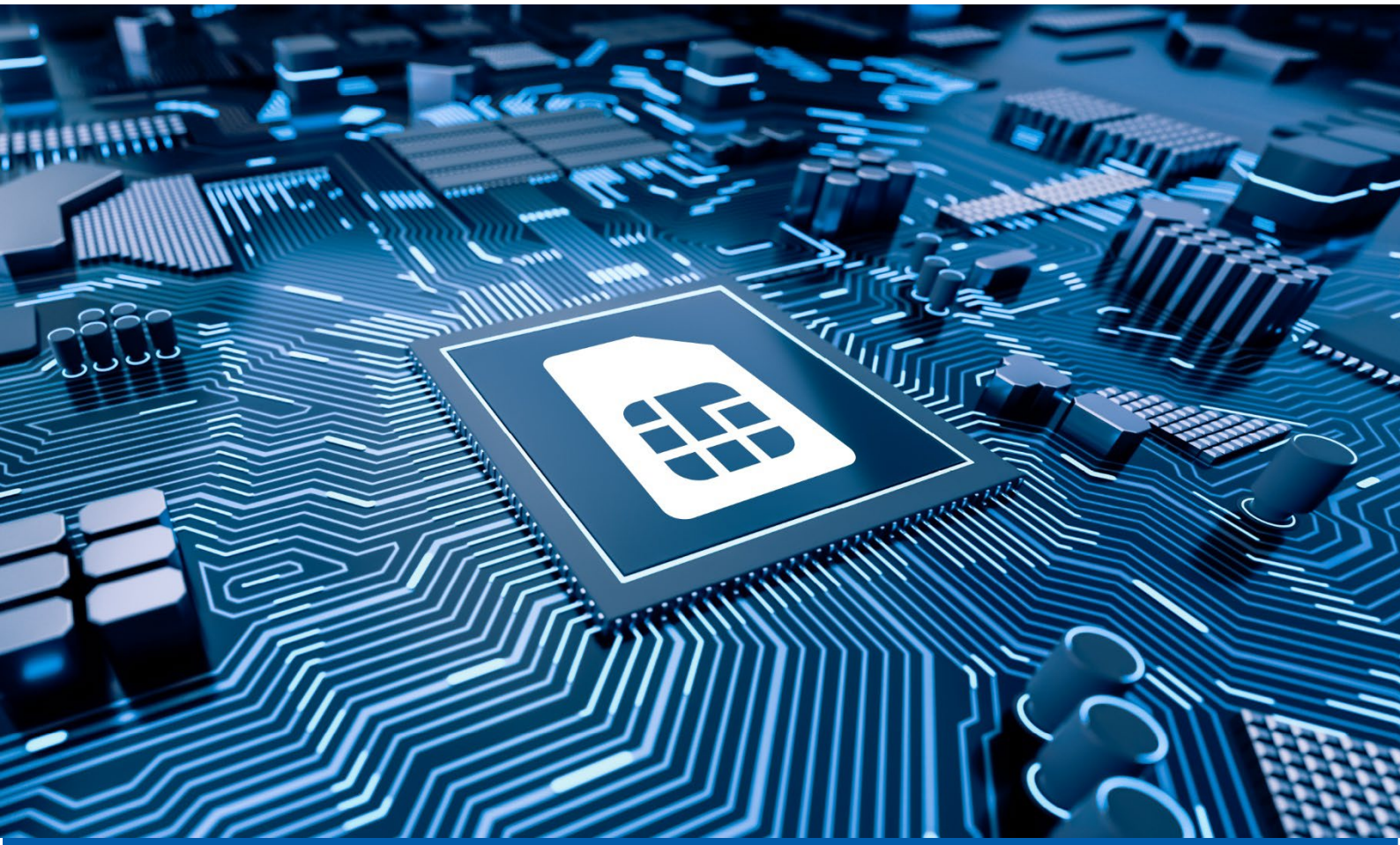
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



EMBEDDED SIM ECOSYSTEM, SECURITY RISKS AND MEASURES

MARCH 2023

About ENISA

The European Union Agency for Cybersecurity (ENISA) is the EU agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU cybersecurity act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with EU Member States and EU bodies, and helps Europe prepare for the cyber-related challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the EU's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

Contact

To contact the authors, please use: team@enisa.europa.eu.

For media enquiries about this paper, please use: press@enisa.europa.eu.

Editors

Georgia Bafoutsou, Maria Papaphilippou, Evangelos Kantas, Marnix Dekker (ENISA)

Acknowledgements

We would like to thank Konstantinos Panagos who was contracted to support ENISA in the preparation of this report.

We also would like to thank the experts of the European Competent Authorities for Secure Electronic Communications (ECASEC EG) for reviewing the report and providing useful input.

Finally, we would like to acknowledge the experts who answered our questionnaire and shared their comments: Remi Van De Calseijde (Liberty Global), Daan Planqué- van Hardeveld (KPN), Panagiotis Drakontis (WIND Hellas) and Ignace Vanoverschelde (Proximus).

Legal notice

Copyright notice

PDF ISBN 978-92-9204-598-2 doi:10.2824/161297 TP-05-22-387-EN-N

CONTENTS

1. INTRODUCTION 8

1.1 SECURITY OF ESIMS 8

1.2 POLICY CONTEXT 8

1.3 TARGET AUDIENCE 9

1.4 PREPARATION OF THIS REPORT 9

1.5 STRUCTURE OF THIS REPORT 9

2. ECOSYSTEM AND USAGE IN EUROPE 11

2.1 ESIM ECOSYSTEM 11

2.2 ESIM BENEFITS AND DRAWBACKS 13

2.3 SIM MARKET AND USAGE IN EUROPE 14

3. ESIM DEPLOYMENTS 16

3.1 SIM EVOLUTION 16

3.2 ESIM ARCHITECTURE 16

4. SECURITY CHALLENGES AND RISKS 21

4.1 OVERVIEW OF SECURITY CHALLENGES AND RISKS 21

5. PROPOSED SECURITY MEASURES 26

5.1 GOVERNANCE AND RISK MANAGEMENT 26

5.2 OPERATIONS MANAGEMENT 28

5.3 HUMAN RESOURCES SECURITY 28

5.4 SECURITY OF SYSTEMS AND FACILITIES 29

5.5 MAPPING TO THE ENISA GUIDELINE 30

6. CONCLUSIONS 31

ANNEX 32

List of abbreviations

Abbreviation	Definition
CAGR	Compound Annual Growth Rate
CI	Certificate Issuer
CSP	Communication Service Providers
EECC	European Electronic Communications Code
EIS	Embedded Universal Integrated Circuit Card Information Set
eSIM	Embedded Subscriber Identity Module
eUICC	Embedded Universal Integrated Circuit Card
GSMA	Global System for Mobile Communications Association
ID	Identification
IoT	Internet of Things
ISD-P	Issuer Security Domain – Profile
ISD-R	Issuer Security Domain – Root
iSIM	Integrated Subscriber Identity Module
LPA	Local Profile Assistant
M2M	Machine to Machine
MNO	Mobile Network Operator
OEM	Original Equipment Manufacturer
OTP	One-time passwords
PKI	Public Key Infrastructure
PRD	Permanent Reference Document
QR code	Quick Response code
RoT	Root of Trust
SAM	SIMjacked attack message
SAS	Security Accreditation Scheme
SAS-SM	Security Accreditation Scheme for Subscription Management

SAS-UP	Security Accreditation Scheme for UICC production
SIM	Subscriber Identity Module
SM-DP+	Subscription Manager – Data Preparation+
SM-DS	Subscription Manager – Discovery Server
SM-SR	Subscription Manager – Secure Routing
SMS	Short Message/Messaging Service
SO	Security Objective
UICC	Universal Integrated Circuit Card

EXECUTIVE SUMMARY

eSIM is the generic term used for the embedded form of a SIM (subscriber identity module) card. Like a normal SIM card, the eSIM identifies a subscriber within a mobile network operator's (MNO) network. Unlike a normal SIM, the eSIM is built into the device, hosted on tiny chips that provide storage for the mobile subscription details in digital format. Both the tiny chip and the software are embedded in the device, with eSIMs being rewriteable by all mobile network operators (MNOs). The credentials required to sign into the MNO's network are downloaded directly.

eSIMs are found in a wide range of products, such as smartphones, wearable devices, tablets, computers, medical internet-of-things (IoT) devices, home automation and security systems, connected cards, and handheld point-of-sale devices. eSIM technical specifications are standardised by industry bodies and allow for power efficiency, remote SIM provisioning and interoperability. eSIM-compatible devices are gaining momentum now that major operating systems such as Android, IOS, and Windows 10 support them.

There are multiple advantages to using eSIMs over traditional SIMs. Devices can become flatter, more waterproof and more resistant to dust, and the eSIM's small size leaves more room for other features. End users can also rewrite their eSIM, for example, to get a local pre-paid phone when abroad.

For MNOs, logistics and support are simplified and new business opportunities are presented, since eSIMs can provide connectivity to IoT devices more easily, which then become 'smart' within an IoT ecosystem.

eSIMs also present security opportunities. For example, if the device is stolen, it is easier for the MNO to switch the user profile. It is also harder for a thief to discard the SIM card after stealing the device.

On the other hand, eSIMs present new security challenges and risks. For example, the arrival of eSIMs has opened up the possibility of eSIM swapping ([1]). Another challenge is the security of eSIM profile provisioning. End users can download a profile directly onto their devices. This could be targeted by attackers, who could push a new profile onto a device and take it over.

This paper provides an overview of eSIM technology and of the eSIM ecosystem, market potential and usage in Europe, along with an overview of the security challenges and risks.

It can be useful for national authorities competent for the security of electronic communications in the context of providing relevant guidelines to the MNOs and also when auditing their security measures for mitigating the risks for eSIMs and safeguarding the eSIM provisioning processes. MNOs can also use the findings of this paper to improve their security posture as far as security of eSIMs is concerned.

Key findings include the following.

([1]) ENISA, *Countering SIM-Swapping – Overview and good practices to reduce the impact of SIM-swapping attacks,* 2021 (https://www.enisa.europa.eu/publications/countering-sim-swapping).

- Security challenges identified are associated to software attacks like eSIM swapping, memory exhaustion and undersizing memory attacks, inflated profile and locking profile attacks. Cybercriminals can cause unavailability of services or gain access to sensitive information.
- There have been very few reported cybersecurity breaches involving eSIMs in Europe since 2010.
- The findings show that there are no major technical vulnerabilities currently known that could be exploited by attackers to compromise user data or take control of user devices, but there are some weaknesses in terms of software design that could be exploited by hackers to gain access to sensitive information stored on eSIMs.
- It is quite likely that the expected large-scale IoT deployment will result to new attacks not yet explored, which can point out existing vulnerabilities of the new technology that have not been revealed so far.

1.INTRODUCTION

1.1 SECURITY OF ESIMS

The embedded subscriber identity module (eSIM) is a new evolution of the subscriber identity module (SIM) card and is being developed by both standardisation bodies and technology companies.

The eSIM ecosystem is based on the principles of open standards, interoperability and privacy by design. It includes service providers (eSIM issuers), device manufacturers (e.g. smartphones, tablets and other devices), mobile network operators (MNOs) and SIM card manufacturers.

The eSIM allows devices to connect to mobile networks without the need for a physical SIM card. Devices can be provisioned with an encrypted profile, which contains subscriber information, network configuration and other relevant data. This offers greater flexibility, convenience and security for users.

eSIM security incidents that have reached the media, mostly have to do with eSIM swapping attacks such as the following incidents.

- Attackers hijacked a device's eSIM and then took over the banking apps linked to the device number, resulting in large amounts of money being siphoned from the accounts and converted to bitcoin ([2]).
- Attackers got access to sensitive documents (including immigration documents and passport copies) via eSIM swapping. Using these documents, the attackers tried to open new banking accounts ([3]).
- Attackers used eSIM swapping to get access to a device and the subscriber's social media accounts, which they used to post racially charged messages ([4]).

The European Commission has identified the security of eSIMs as a priority for the digital single market, and has tasked the European Telecommunications Standards Institute with delivering an eSIM standard.

The eSIM is expected to make mobile connectivity more flexible and secure, by reducing the number of physical SIM cards required to operate a mobile device.

1.2 POLICY CONTEXT

The European Electronic Communications Code (EECC) ([5]) aims to protect consumers irrespective of their chosen communication tool, focusing on the functionality (electronic communication) rather than on the underlying technology or implementation choices.

([2]) Turner-Cohen, A., 'Sydney man wakes up to find he had lost $52,000 in terrifying phone hack', *News.com.au*, 2022 (https://www.news.com.au/finance/money/costs/sydney-man-wakes-up-to-find-he-had-lost-52000-in-terrifying-phone-hack/news-story/3ffd94e41142776b5ac336c55f09dd06).

([3]) Allen, F., 'Hack Horror – I lost all my £19,000 life savings after hackers took control of my phone – here's the chilling sign to look out for', *The Sun*, 2021 (https://www.thesun.co.uk/tech/17114889/phone-hack-life-savings-sim-scam/).

([4]) Alexander, J., 'Twitter CEO Jack Dorsey's account was hacked', *The Verge*, 2019 (https://www.theverge.com/2019/8/30/20841288/jack-dorsey-ceo-twitter-account-hacked-chuckle-gang-shane-dawson-james-charles).

([5]) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (OJ L 321, 17.12.2018, p. 36) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972).

Promoting the interests of consumers in the European Union constitutes one of the code's general objectives, as set out in Article 3(2) of the EECC:

In the context of this Directive, the national regulatory and other competent authorities …, the Commission and the Member States shall …:

[…]

promote the interests of the citizens of the Union … by maintaining the security of networks and services, by ensuring a high and common level of protection for end-users through the necessary sector-specific rules …

Security is one of the general objectives of the EECC, as outlined in Article 3 of the EECC:

The EECC also contains specific security requirements for electronic communication providers, including aspects such as the confidentiality of communications. Most of the security requirements are set out in Articles 40 and 41 of the EECC, though its recitals also provide guidance on these requirements.

The ENISA *Embedded SIM Deep Dive* aims at contributing to the EU cybersecurity strategy ([6]) and, more specifically, to ongoing policy initiatives relating to the security of mobile networks and information systems, especially concerning eSIM technology. It streamlines and consolidates available information on cyberthreats and their evolution.

1.3 TARGET AUDIENCE

This document strives to provide guidance to national authorities competent for the security of electronic communications, supervising the implementation of Articles 40 and 41 of the EECC. It may also be useful for policy experts in the Commission, experts working in the telecom sector, industry associations and other bodies with roles in standardisation and mobile security.

1.4 PREPARATION OF THIS REPORT

The study presented in this report uses a four-tiered methodology consisting of:

- desktop research taking stock of relevant literature on the topic;
- a review of the initial draft by the members of the European Competent Authorities for Secure Electronic Communications Group and targeted stakeholders from the industry;
- communication with the stakeholders to gather additional input;
- analysis and consolidation of information.

The information derived from the first three steps of the process was used in order to prepare and further customise the subsequent step. The information collected was analysed and consolidated in order to provide tangible results in line with the purpose of this study.

1.5 STRUCTURE OF THIS REPORT

The report consists of six sections. Section 1 includes a short introduction of the policy context, the target audience and the methodology used to prepare this report. In Section 2, a general presentation of the eSIM ecosystem is provided alongside the key players involved. Section 3

([6]) European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade*, 2020 (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0).

includes a brief description of the evolution of SIM cards, and the advantages and disadvantages that eSIMs have to offer. In this section, emphasis is placed on the current market and the usage of eSIMs. Section 4 provides an overview of the major security challenges and risks currently identified by both academia and the industry and Section 5 includes the proposed security measures. Concluding remarks are provided in Section 6.

In the Annex are cited good practices and initiatives from standardisation bodies and relevant organisations to secure the usage of eSIMs.

2. ECOSYSTEM AND USAGE IN EUROPE

2.1 ESIM ECOSYSTEM

The traditional SIM card, which is owned by network operators and issued to their end customers, is a standalone component independent from the device. It is required for end users to access the service of a particular MNO or virtual MNO, thus creating a lock-in effect. If the end user wishes to change network operators, they must set up a new contract with another operator and receive a new SIM card. To finally change operator network, they also have to physically swap the SIM cards.

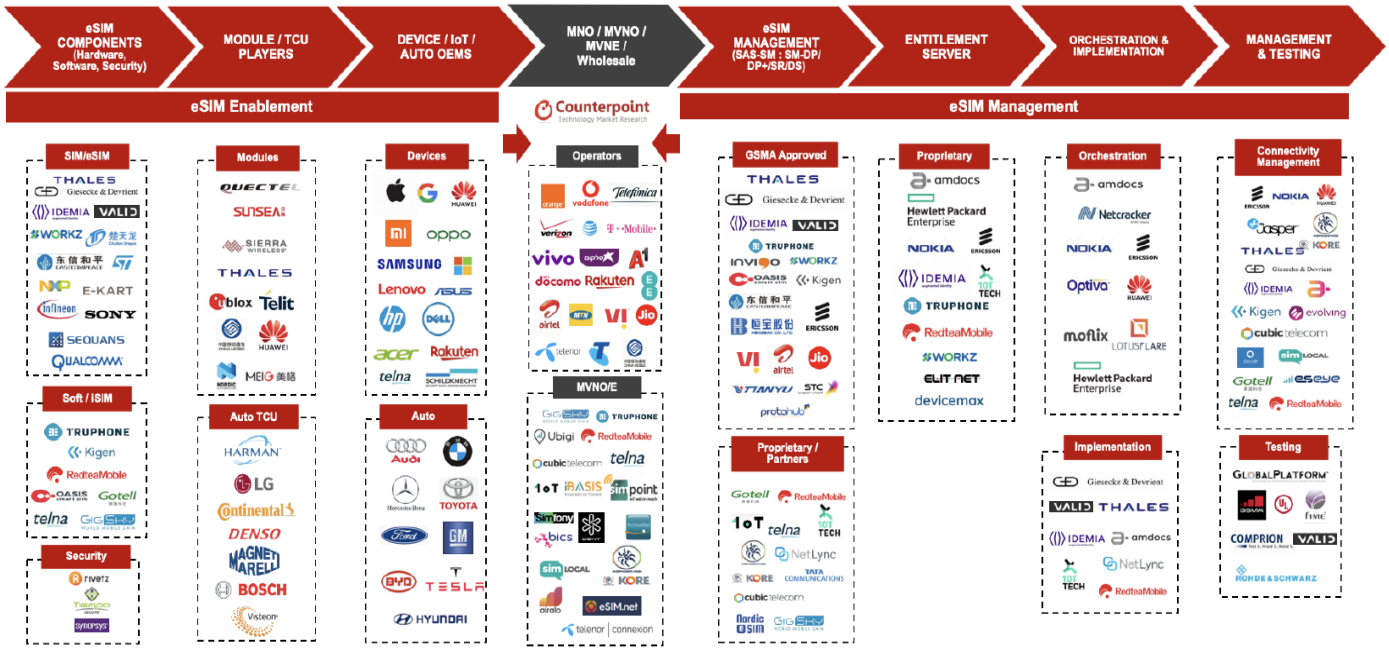
In contrast, the eSIM is a programmable SIM card, offering remote provisioning. It can be embedded in any type of device for either the consumer or the machine-to-machine (M2M) market. In particular, these types of SIM cards revolutionise and modify the current relationships between subscribers and network operators, by offering end users the ability to select multiple network-operator subscriptions without having any physical access to the device (i.e. swapping SIM cards).

End users purchase a device embedded with an eSIM without any pre-installed connection to a mobile network. Afterwards, the MNO profile, which includes all the necessary data linked to a subscription, can be selected, purchased and activated remotely. End users also have the ability to install and manage different profiles, through the subscription manager – data preparation+ (SM-DP+) servers.

eSIMs are currently gaining momentum in the consumer and M2M market, offering new opportunities and benefits for all stakeholders of the mobile economy.

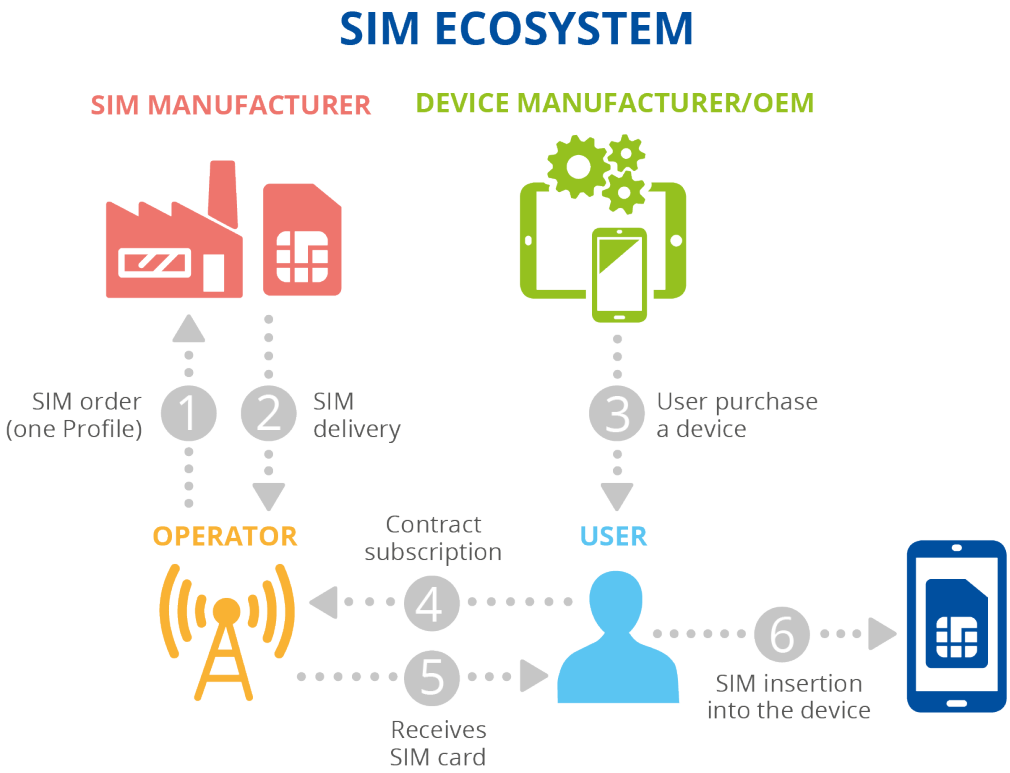
The eSIM industry includes different entities contributing to different aspects of the eSIM life cycle. In Figure 1, the current view of the industry ecosystem is presented, while in Figures 2, 3 and 4, the end-customer view of the ecosystem is presented.

Figure 1: Overview of eSIM industry ecosystem



(Source: Counterpoint, *White Paper – LEADER – eSIM adoption and benchmarking* ([7]), 2022)

Figure 2: Overview of end-customer traditional SIM ecosystem



([7]) https://www.counterpointresearch.com/whitepaper-leader-esim-adoption-opportunities-benchmarking/

Figure 3: Overview of end-customer eSIM ecosystem

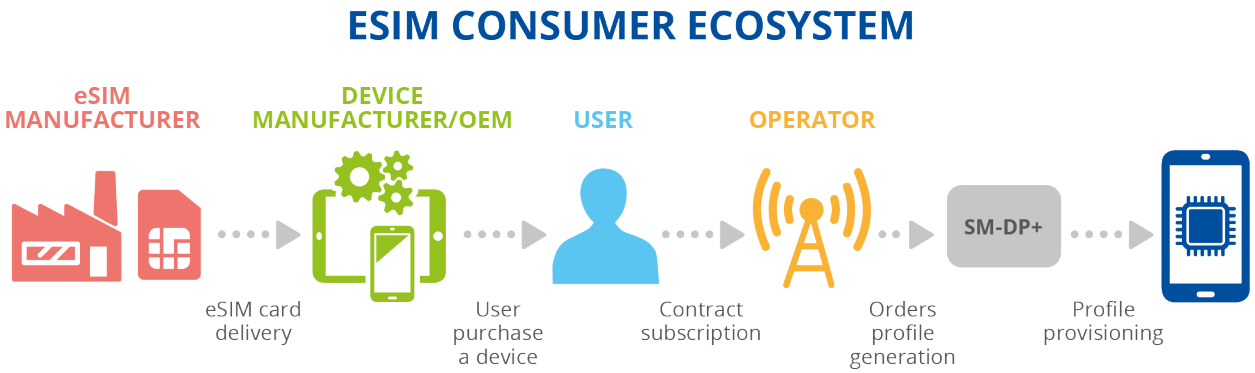
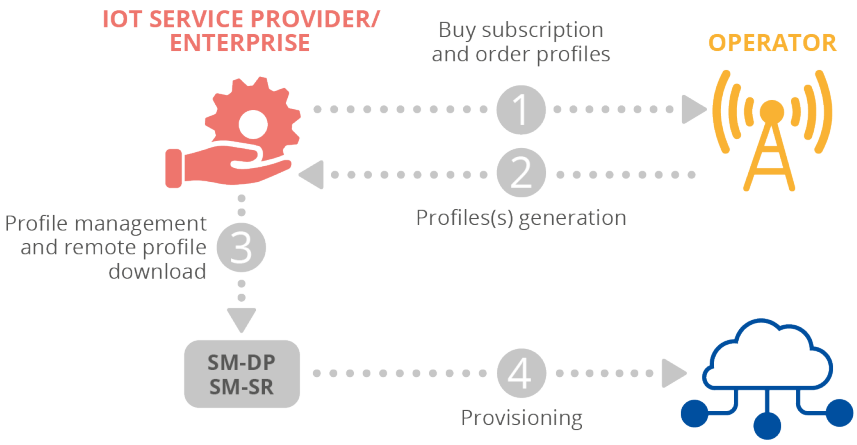


Figure 4: Overview of M2M eSIM ecosystem



2.2 ESIM BENEFITS AND DRAWBACKS

The change from the traditional removable SIM card to an eSIM provides multiple benefits for the involved stakeholders.

- **SIM manufacturers** gain access to new markets by providing the infrastructure and services that remotely provision SIMs, while the reduced space coming from the embedded design also has a positive impact on device designs, enabling additional functionalities (e.g. space saving for a bigger battery).
- **MNOs** gain new distribution models of subscriptions for consumer and M2M devices. They are able to provide quick tests for customers ('trials' of their network), while maintaining the same security levels. At the same time, they can reduce the substantial logistical costs for procurement and distribution to commercial channels previously associated with traditional SIM cards.
- **Business customers** gain flexibility and efficient management of their extensive numbers of M2M devices, with the comfort of no additional compromises on the existing SIM-card abilities.

- **End users** gain simplified management of their subscriptions with an equivalent level of security to that of the removable SIM card (e.g. the ability to easily switch between MNOs even while travelling, buy and install an eSIM online, etc.).

Potential drawbacks of the eSIM technology for end users include the following:

- The process of replacing a device (i.e. when a device breaks, etc.), can be cumbersome. Users have to retrieve and re-install their eSIM profiles from the cloud.
- Device tracking, as there is constant connection to a cellular network.
- The possibility of eSIM card data being hacked from the cloud hosting.

2.3 SIM MARKET AND USAGE IN EUROPE

The eSIM market has grown substantially in recent years, with at least 232 mobile service providers having launched eSIM services across nearly all European countries and in a total of 82 countries worldwide.

Moreover, according to the latest numbers of eSIM shipment volumes given by the Trusted Connectivity Alliance, eSIM shipments collectively reported in 2021, reached 337 million units – a 9 % increase on the 309 million reported in 2020.

Forecasts suggest that this will translate into a market of over 1.2 billion annual eSIM shipments in 2025 ([8]) ([9]). Regarding M2M solutions, eSIM is viewed as the preferred option for long-term internet-of-things (IoT) deployments, with forecasts suggesting that approximately 1.1 billion profiles will be active in 2025 compared to 32.6 million in 2019 (a compound annual growth rate (CAGR) of 82 %) ([9]).

Overall, amid the COVID-19 crisis, the global market for eSIMs is currently estimated at EUR 622.7 million in 2022 and projections suggest it will reach approximately EUR 1.7 billion by 2026, thus growing at a CAGR of 28 %.

Within Europe, the German market is predicted to grow at a CAGR of 27.7 %, while the rest of the European market is expected to reach EUR 178.6 million by 2026 ([10]).

However, despite the significant commercial growth in the availability of devices with an eSIM, the market adoption is relatively low regarding its long-term uptake, with one key issue being consumer awareness. In particular, research by the Global System for Mobile Communications Association (GSMA) indicates that only 20 % of consumers in the 25–34 age group are aware of eSIMs ([11]).

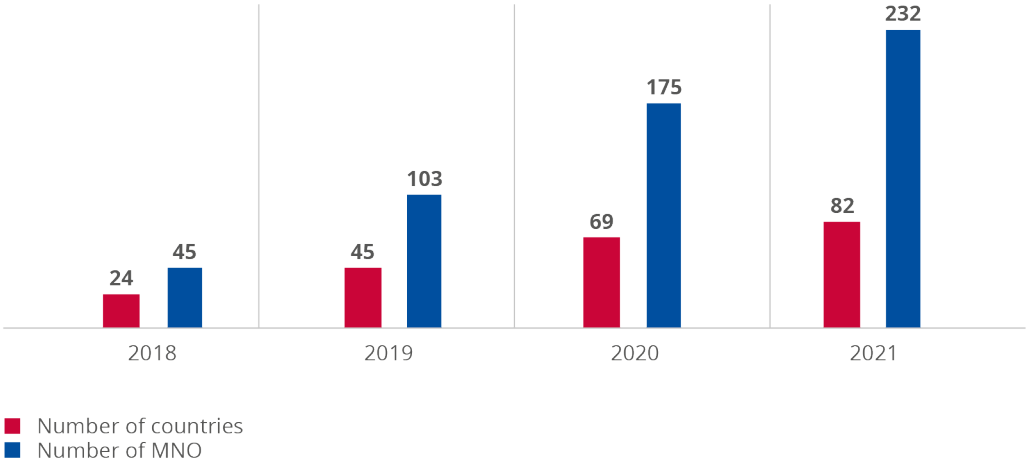
Another issue that might affect market adoption concerns network operators and their fear of losing direct access to the consumer. Specifically, through the adoption of eSIM, consumers will gain a flexible way to manage profiles between different MNO networks on the same device,

([8]) Trusted Connectivity Alliance, *eSIM: Delivering flexible control and dynamic security over a connected objects lifetime*, 2022 (https://trustedconnectivityalliance.org/technology_overview/esim/#:~:text=The %20latest %20view %20of %20eSIM,to %20reach %20337 %20million %20units).
([9]) Kaleido Intelligence, *Kaleido Connectivity Vendor Hub H2 2021: Competitive analysis*, 2021 (https://www.cisco.com/c/dam/en/us/solutions/internet-of-things/iot-control-center/pdfs/white-paper-sp-kaleido-connectivity.pdf).
([10]) Global Industry Analysts, *eSIM – Global Market Trajectory & Analytics Report*, 2022.
([11]) Iacopino, P., Popov, A., 'eSIM: State of the consumer market and the road ahead', *GSMA Intelligence*, 2021 (https://data.gsmaintelligence.com/research/research/research-2021/esim-state-of-the-consumer-market-and-the-road-ahead).

which will redefine the competitive market of MNOs by breaking the existing lock-in effect (i.e. a SIM card being tied to a single MNO) ([12]).

Challenges notwithstanding, the market has been steadily growing, with the GSMA forecasting that by the end of 2022, more than 500 million smartphone connections globally – out of the total 8.3 billion SIM connections – will use eSIMs, with Europe leading the way with the fastest adoption rate ([13]). In addition, by the year 2025, it is predicted that 2.4 billion smartphone connections will use eSIMs globally, representing approximately 30 % of the total connections.

Figure 5: Overview of the number of MNOs and countries offering commercial eSIM services (**Error! Bookmark not defined.**)



([12]) Srinivasan, A., 'How will eSIMs drive the IoT revolution?', *Counterpoint Technology Market Research,* 2017 (https://www.counterpointresearch.com/how-will-esims-drive-the-iot-revolution/).
([13]) GSMA, 'eSIM adoption and global market trends', *eSIM Summit MWC22*, 2022 (https://www.gsma.com/iot/wp-content/uploads/2022/03/MWC22-eSIM-Summit-Master.pdf).

3. ESIM DEPLOYMENTS

This section defines the functional architectures required to support the remote provisioning and management of eSIMs for the consumer and M2M solutions.

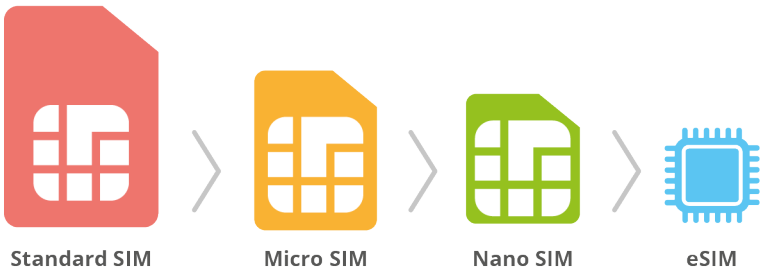
3.1 SIM EVOLUTION

Since 1990, the SIM card has been the primary piece of MNO-supplied equipment used by consumers to achieve secure and authenticated access to mobile networks. Over the years, the size of the physical card has been greatly reduced, resulting in smaller and thinner devices and more hardware-space availability for other features ([14]).

The physical card is a piece of external hardware, built on universal integrated circuit card (UICC) technology, that a consumer can remove from the device. During its manufacturing, the card is programmed with an MNO-defined profile, which provides the necessary information to authenticate access to a mobile network. To avoid issues relating to SIM sizes for commercial devices, most of the MNOs provide physical SIM cards in three different sizes, namely standard (2FF), micro SIM (3FF) and nano SIM (4FF). The nano SIM is widely used in new smartphones.

Recently, alternative SIM solutions have been deployed on M2M and commercial devices, focusing on embedded and remote provisioning. However, despite these changes, the fundamental role and elements of the SIM are still intact.

Figure 6: SIM card evolution



3.2 ESIM ARCHITECTURE

The eSIM technology involves an embedded SIM or embedded universal integrated circuit card (eUICC) set directly into a device, offering the same level of security as traditional physical SIM cards while supporting the ability to own multiple profiles with additional secure over-the-air update capabilities. The GSMA has created solutions suited for two different types of channels; end-user consumers and M2M solutions.

eSIMs are not to be confused with integrated SIMs (iSIMs) or virtual SIMs, as they are all different solutions. For example, eSIMs are physical SIMs that are permanently placed in devices (consumer or M2M), cannot be removed and are thus integral to the device, whereas iSIM is the next generation of SIM technology. iSIM moves the SIM from a separate chip into a dedicated silicon area which sits alongside the application processor and/or cellular radio on a

([14]) GSMA, *Understanding SIM Evolution*, 2015.

purpose-built system-on-chip ([15]). iSIMs have been developed following the need for improvements in size, power consumption and costs from the manufacturers as IoT devices increasingly grow in popularity, and the need to authenticate devices, issue security updates and add more services once these devices are active around the world.

Finally, a virtual SIM is a cloud-based mobile service number which can be used from any device via an application. Virtual SIMs are also not physically attached to a device and work as SIM card emulations. Virtual SIMs are expected not to bind to particular countries and to provide affordable phone numbers.

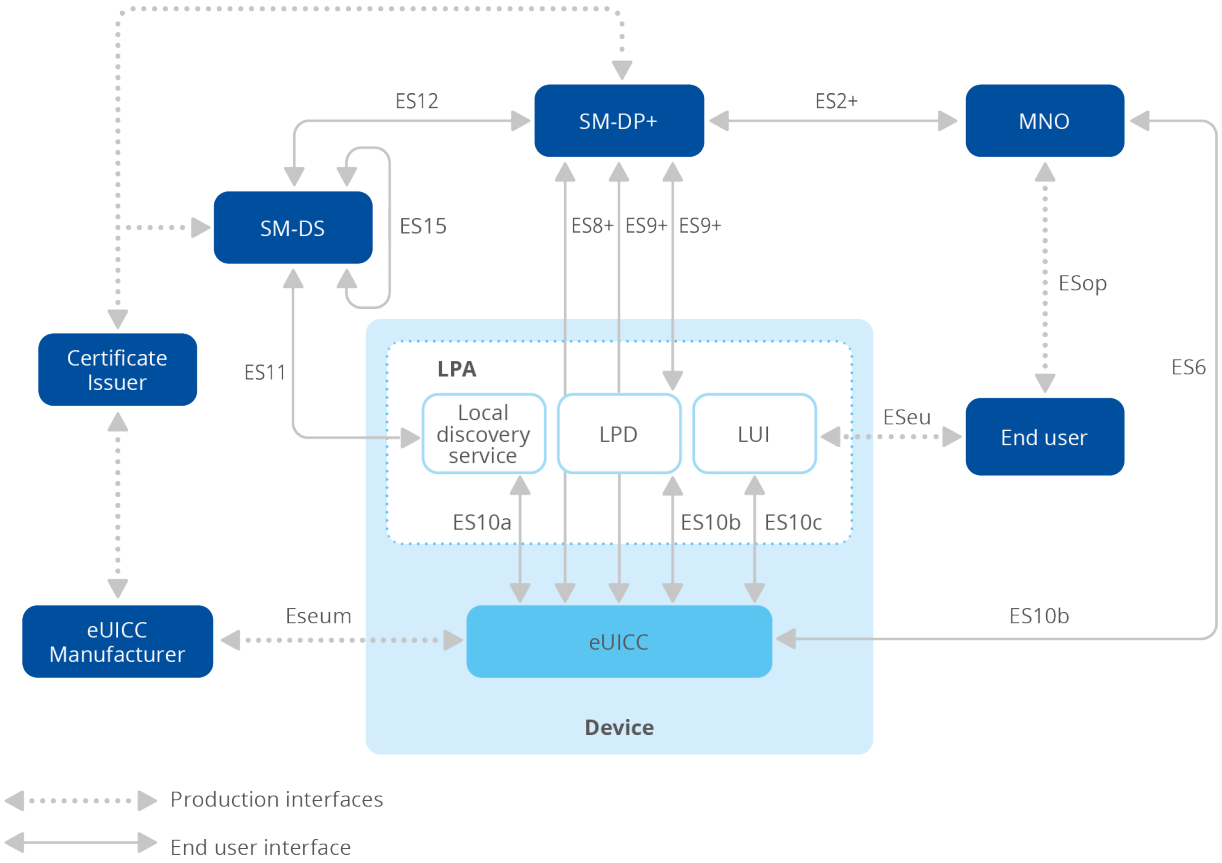
3.2.1 Consumer solution

The remote SIM provisioning for the consumer solution is based on end users managing their devices and the profiles within them. The solution follows a client-driven model and is organised around four elements: the SM-DP+, the subscription manager – discovery server (SM-DS), the local profile assistant (LPA) and the eUICC. Different entities participate in the architecture provided in Figure 7.

- The **eUICC** is a secure element that contains one or more subscription profiles.
- The **LPA** assists with the download of profiles and secures the end-user interface on the device that is used for local control.
- The **eUICC manufacturers** are responsible for issuing the eUICCs to the consumer device manufacturers. The eUICC element contains the initial cryptographic configuration and security architecture, and may also contain the LPA integrated into the eSIM.
- **Consumer device manufacturers** are responsible for implementing the LPA elements on consumer devices.
- **MNOs/communication service providers** (CSPs) have access to the SM-DP+ element. When a customer selects their preferred CSP, the service provider initiates the process of provisioning a profile package. Subsequently, the MNO specifies the characteristics, features, and applications of the profile that apply to the target eUICC.
- The **SM-DP+** element is responsible for creating profiles and for their security and management, when requested by an MNO.
- The **SM-DS** provides the necessary mechanisms to notify the local discovery service within a device that the SM-DP+ element wants to communicate with it. The element sends an event registration message to the SM-DS for a target consumer device.
- A **certificate issuer** (CI) is considered a trusted third party, whose responsibility is to authenticate entities (e.g. the eUICC manufacturer, SM-DP+ or SM-DS) and provide digital certificates which enable entities to securely communicate. According to the GSMA, security certification issuers ([16]) include both cybertrust and digicert.
- A **subscriber/end user** is a customer who holds a contract with a CSP and uses the consumer device and the related services.

([15]) Kigen, *What Is an Integrated SIM (iSIM)* (https://kigen.com/products/isim/).
([16]) GSMA, *GSMA Certificate Issuer* (https://www.gsma.com/esim/gsma-root-ci/).

Figure 7: GSMA proposed eUICC remote provisioning system for consumer solutions ([17])



3.2.2 M2M solution

The remote provisioning for the M2M solution is much simpler, as human interaction (i.e. end users) is not required and everything is remotely managed. It uses a push model with a server in charge of provisioning and managing profiles, and is organised around three elements, the subscription manager – data preparation (SM-DP), the subscription manager – secure routing (SM-SR) and the eUICC element ([18]). Different entities participate in the architecture provided in Figure 8.

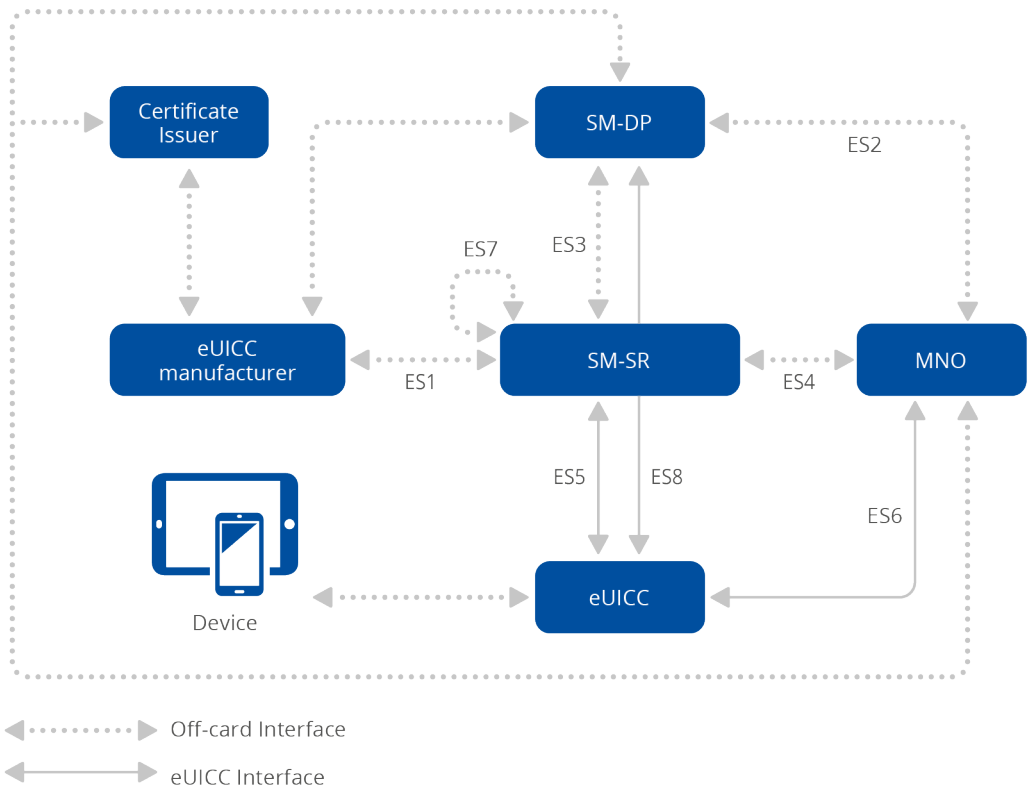
- The **eUICC** is a secure element that contains one or more subscription profiles.
- **eUICC manufacturers** are responsible for issuing the eUICC element containing a provisioning profile and/or operational profiles, and for delivering them to the M2M manufacturers.
- **M2M device manufacturers** are responsible for building M2M devices comprised of the eUICC and the communication module.
- **MNOs** provide mobile-network connectivity. MNOs must select at least one SM-DP element and have a direct interface to the SM-SR element. When a customer selects their preferred MNO, the download of a particular provisioning profile to the target eUICC element begins. This includes the checking and validation steps conducted by the MNO on the certification and capabilities of the target eUICC. Afterwards, when the download and installation of the provisioning/operational profile is complete, the eUICC

([17]) GSMA, *Embedded UICC Protection Profile*, 2018 (https://www.gsma.com/newsroom/wp-content/uploads/SGP_05_v1_1.pdf).
([18]) GSMA, *Business Process for Remote SIM Provisioning in M2M*, 2015 (https://www.gsma.com/iot/wp-content/uploads/2015/02/CLP.05-v1.0-BPD.pdf).

element sends a confirmation to the MNO, and the MNO can then manage the enabled profile on the target eUICC over the air.

- The **SM-DP** acts on behalf of the MNO and is responsible for the preparation, storage, and protection of MNO profiles, while also downloading and installing profiles onto the eUICC. Additionally, it is responsible for managing profile enabling and deletion requests from the eUICC through the SM-SR.
- The **SM-SR** is responsible for securing the link between the SM-DP and the eUICC (for the delivery of MNO profiles), while also acting as a profile manager, with the ability to enable, disable and delete them. A key characteristic of the SM-SR is that it uses pre-shared key cryptography and can only be associated with a single eUICC, however it is also possible to change the eUICC during the lifetime of the eSIM.
- A **Certificate Issuer (CI)** is considered a trusted third party, whose responsibility is to authenticate entities (MNO, eUICC manufacturers, etc.) and provide digital certificates which enable entities to securely communicate.

Figure 8: GSMA proposed eUICC remote provisioning system for M2M solutions ([19])



Although the two solutions (M2M and consumer) have several similarities in terms of architecture and elements used, they are inherently technically different and cannot overlap in an implementation that serves both consumer and M2M. Table 1 showcases the main overall differences and similarities between the two solutions.

([19]) See Footnote 18

Table 1: Similarities and differences between the consumer and M2M solutions

Elements and services	Consumer solution	**M2M solution**
Sample devices	Mobile phones, laptops, tables, smartwatches	Sensors, cars, machinery
System used	SM-DP+	SM-DP
Model type	Client driven	Server driven, based on push-model
Remote activation	End user manages the device and the profiles within it.	Yes, without requiring human interaction
Rely on the eUICC element	Yes	Yes
Requires certificate issuer (CI)	Yes	Yes
Use of cryptography	Public key infrastructure (PKI) based authentication is used and therefore any eUICC and SM-DP+ can connect, so long as they share the same root PKI certificate.	Authentication with the SM-SR uses a pre-shared key and only allows a single SM-SR to communicate with the eUICC.
Unique characteristics	LPA and SM-DP+	SM-SR

4. SECURITY CHALLENGES AND RISKS

The introduction of eSIMs enables the technological transition from the traditional physical cards to embedded cards for devices. Devices supporting the eSIM technology hold many advantages over those with traditional physical SIM cards (see Chapter 3), as they can provide additional security features and greater flexibility for the customers. However, while eSIMs could be highly beneficial for mass-produced devices, they are still considered a relatively new and expanding technology carrying major security risks for all relevant stakeholders.

To adequately explain these security threats, this chapter focuses on current or potential cybersecurity challenges and risks of eSIMs, including references to past attacks and media reports.

4.1 Overview of security challenges and risks

From a security perspective, one key distinction between traditional SIM cards and eSIMs is that devices with physical SIMs are susceptible to both hardware and software attacks, while devices with eSIMs are only susceptible to software attacks.

This aspect narrows the list of security threats and challenges, since eSIMs cannot be physically removed and placed in other devices and they require verification from MNOs in order to be enabled.

However, while they introduce novel and improved mechanisms of identity management, they also present a great opportunity for malicious creativity ([20]).

Risk 1: eSIM swapping

Profile swapping may lead to the deactivation of all profiles and a loss of connectivity. Specifically, by obtaining the necessary personal data, an attacker can claim that the device is damaged and gain access to the subscriber's account on the MNO's portal, initiate an eSIM swap and then scan the displayed QR code to activate the profile and successfully conduct the swap attack.

Malicious access to eSIMs in modern consumer devices is more difficult, since there are additional security layers such as biometric authentication (i.e. face and fingerprint identification, etc.). The target devices are tracked through their constant connection to a cellular network, thus enabling some level of traceability and security.

When these eSIMs are in IoT devices used in factory environments, they can be updated with a new configuration to make them more efficient. Therefore, this mechanism can be maliciously used in order to get the devices to join an attacker's remote network, where data can be manipulated or added to the device ([21]).

([20]) In case of a security incident, please refer to the ENISA *Technical Guideline on Incident Reporting under the EECC*.

([21]) Trend Micro, *From SIMjacking to Bad Decisions – 5G security threats to non-public networks*, 2019 (https://www.trendmicro.com/vinfo/au/security/news/internet-of-things/from-esim-jacking-to-fake-news-threats-to-5g-and-security-recommendations#SIMjacking).

An industry-reputable software that can achieve SIM-swapping attacks is 'Simjacker' ([22]). Simjacker's attack begins when a simjacked attack message (i.e. an SMS (short message/messaging service)) is sent to the targeted subscriber. This message is sent from another handset, either a global system for mobile communications modem or an SMS-sending account connected to an application-to-person account, containing a series of SIM toolkit instructions, and is specifically crafted to be passed on to the eUICC within the device ([23]).

However, in order for these instructions to work, this specific attack exploits the presence of the S@T browser on the eUICC using it as an execution environment. The absence of this particular browser will lead to a failed attack.

These on-card attacks could be utilised to fulfil purposes such as:

- unauthorised profile tampering/management, which enables access to or modification of the content of a profile, leading to:
  - profile disabling/deletion, (i.e. denial of service),
  - profile switching, resulting in a loss of connectivity,
  - profile swapping, resulting in the deactivation of all enabled profiles and a loss of connectivity;

- unauthorised identity tampering, leading to:
  - identity interception, where an attacker may intercept the subscriber's credentials,
  - unauthorised identity management;

- unauthorised access to a mobile network, leading to:
  - fraud (e.g. performing illegitimate actions),
  - misinformation (e.g. sending SMS/multimedia messaging service messages with malicious content, etc.);

- compromising a device (consumer or M2M), leading to:
  - privacy leakage and information retrieval (e.g. information on the eUICC, etc.),
  - malware spreading (e.g. forcing a browser to open a particular web page with malware located on it, etc.),
  - espionage (e.g. location-retrieving attacks, etc.).

Risk 2: Memory exhaustion

Memory exhaustion is a type of denial-of-service attack, in which attackers work on depleting the memory resources of a computing system in order to prevent it from providing its services to legitimate users ([24]).

The GSMA's eUICC specifications define a remote-provisioning procedure, called 'Download & Install', that transmits subscriber profiles from an MNO to an eUICC and installs these profiles onto the eUICC. The communication channel that enables this transmission (between the eUICC and the SM-SR) is the issuer security domain – root. In the next steps of the procedure, the issuer security domain – profile (ISD-P) creation takes place on the eUICC, which will hold

([22]) AdaptiveMobile Security, *Simjacker Technical Report*, 2019 (https://simjacker.com/).
([23]) Mc Daid, C., 'Simjacker – next generation spying via SIM card vulnerability', *AdaptiveMobile Security*, 2019 (https://blog.adaptivemobile.com/simjacker-next-generation-spying-over-mobile).
([24]) Wang X., 'Memory and state exhaustion denial of service', *Encyclopedia of Cryptography and Security*, Springer, Boston, MA., 2011 (https://doi.org/10.1007/978-1-4419-5906-5_270).

the profile. During this step, memory is assigned and the profile's unique application identifier is set ([25]).

The GSMA's specifications also include potential error handling of the 'Download & Install' procedure. However, the specified error handling is only limited to timeout response messages to the SM-DP, when the response message from the eUICC is not received (i.e. is lost) by the SM-SR during a specified time frame. This particular action opens up the possibility of attacks that fill a part of the eUICC's memory with an empty ISD-P. These types of attacks are named memory exhaustion attacks.

In the eSIM context, this type of attack could be applied to exhaust the eUICC's memory through repeated attacks. These attacks work as follows:

a. Affect the SM-SR, so that it cannot receive any return message from the eUICC and thus is not able to update the eUICC information set (EIS) file.
b. 'Orphan' the ISD-P and the designated memory space on the eUICC, so that it does not have any association with any entity (i.e. an MNO). This can lead to a great financial loss for MNOs, as it stops them from providing network service ([26]).

It should also be noted that because of the profile being 'orphaned', neither MNOs nor the SM-DP have the ability to delete it, which makes recovery of the device impossible.

In addition, safe mechanisms (such as the 'MasterDelete' command) cannot function in a device compromised by a memory exhaustion attack, as these procedures only work on fully installed profiles.

The attack cannot be traced, as the only evidence is a lost message.

Risk 3: Undersizing memory

A compromised or malicious SM-SR component can be responsible for an attack that prevents MNOs and SM-DPs from installing subscribers' profiles on eUICCs.

The attack works as follows:

The EIS file has fluctuating fields, such as the 'remainingMemory' field. The SM-DP makes a request to SM-SR enabling it to return an EIS file, which has already been modified regarding its 'remainingMemory' data to zero. This has a direct effect on new profile uploads, as the SM-DP cannot create an ISD-P.

This type of attack can also not be traced or suspected on an old device, which contains multiple profiles inside it. In particular, the attack could become unnoticeable if the compromised SM-SR component set the memory value to a specific threshold between zero and the minimum size of a profile ([27]).

Risk 4: Inflated profile

([25]) GSMA, *Remote Provisioning Architecture for Embedded UICC*, 2016.
([26]) Meyer, M., Quaglia, E. A. and Smyth, B., 'Attacks against GSMA's M2M remote provisioning', *Financial Cryptography and Data Security – 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26 – March 2, 2018 revised selected papers*, Springer, Heidelberg, 2018, pp. 243–252.
([27]) Meiklejohn, S. and Sako, K. (eds), *Financial Cryptography and Data Security – 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26 – March 2, 2018 revised selected papers*, Springer, Heidelberg, 2018.

An inflated profile attack could be initiated either by a compromised SM-DP component or from a malicious MNO. An MNO could easily learn the available memory of a particular device, through the 'getEIS' function, and then request a creation of a profile according to the available memory size, thus exhausting the available memory in the eUICC.

This would not only result in memory exhaustion but would also affect other network operators, as they would not be able to store profiles on the eUICC. Likewise, a compromised SM-DP component could launch an inflated profile attack by constructing a 'createISDP' request containing a modified required memory field.

This type of attack can be suspected by the SM-SR, however in a scenario where the malicious MNO defines a particular profile that does not consume all the available memory, but instead leaves some that is not enough for a new profile, the attack will be more successful[28].

Risk 5: Locking profile

According to the GSMA's specifications on profile management, a particular set of policy rules, which are initiated by the MNOs, are stored inside each profile (POL1). These rules can only be changed when a profile is enabled by the MNO that owns the profile.

Furthermore, a specific policy rule named 'CannotBeDisabled' locks an eUICC to a profile, thus forcefully locking a device to a particular network. It should be also noted that in 4G networks, once a device with an eSIM becomes unlocked, it is not possible to reverse this action.

In order for a device to be locked to a particular MNO, a malicious MNO will have to install a profile with a modified POL1 file. This action will result in a notification being sent directly to the previous MNOs that own other profiles in the device, stating that their profiles have been disabled. However, since the MNOs do not own the compromised profile, they cannot disable nor delete it, and thus the eUICC of the device is locked to a malicious profile. These attacks can be state-sponsored (i.e. during cyberwarfare), supply chain attacks or be launched by hackers that maliciously acquire an operator's certificates and consequently block devices.

An MNO could use such tactics for opportunistic reasons. More specifically, in a scenario in which a subscriber wishes to unlock its M2M devices, the MNO can simply delay the unlocking process of the devices, thus preventing other competitor MNOs from enabling new profiles on the eUICC of the devices. This can have a direct effect on the subscriber and on the competitor MNOs.

Risk 6: Protocol attacks

To induce a protocol attack, an attacker persuades potential victims (subscribers) to install a malicious application on their device, or even compromised apps containing malicious codes in SDKs.

Currently, the number of active rooted devices might be higher than expected[29], and consequently the exposure to potential attacks requiring root access may increase.

([28]) See Footnote 22

([29]) This is not necessarily due to targeted hacking-oriented activities, but because there is a practice in the current market of restricting functionalities of certain electronic devices just by applying a software procedure. Therefore, average users possessing a minimal set of technical skills can unleash all the processing power and/or functionalities of the respective device by enabling root access

Moreover, according to a study on app piggybacking, the Android packaging model in particular, offers substantial opportunities for malware attackers to piggyback malicious code in popular apps, which can then lead to attacks spreading to a large user base ([30]).

The feasibility of these attacks relies on the lack of security awareness that the majority of users have. By granting specific privileges to malicious or compromised apps, attackers can have access to and acquire sensitive information, such as phone numbers, sent messages, and more. Furthermore, for rooted devices, an attacker could potentially also access all files in the device, by sending command response protocol commands for invoking specific functions (i.e. application protocol data units). It should be noted that after acquiring security files (application protocol data units, personal identification number code, etc.) as plaintexts, the attacker could also launch attacks such as 'man in the middle' and traffic eavesdropping ([31]).

Risk 7: Attacks on the MNOs and other entities in the eSIM supply chain

Attacks could also target the MNO directly, or even other entities in the eSIM supply chain. Attackers target software developers, product manufacturers and suppliers and access secure source codes, build malicious processes or update current mechanisms by infecting legitimate apps to distribute malware.

Attacks of this kind may lead to a total loss of trust of the affected party in the provisioning delivery supply chain, malware spreading and information leakage.

([30]) Li, L., Li, D., Bissyandé, T. F., Klein, J., Le Traon, Y., Lo, D. and Cavallaro, L., 'Understanding android app piggybacking: A systematic study of malicious code grafting', *IEEE Transactions on Information Forensics and Security*, Vol. 12, No 6, 2017, pp. 1269–1284.

([31]) Zhao, J., Ding, B., Guo, Y., Tan, Z. and Lu, S., 'SecureSIM: rethinking authentication and access control for SIM/eSIM', *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 2021, pp. 451–464.

5. PROPOSED SECURITY MEASURES

The following paragraphs include security measures that could mitigate the above-analysed risks.

The security measures are divided into four categories –governance and risk management, operations management, human resources security and security of systems and facilities process and technical – and have been mapped to the ENISA security objectives (SOs) as per ENISA's *Guideline on Security Measures under the EECC* ([32]).

Note that neither the list of risks nor the list of security measures is exhaustive.

5.1 GOVERNANCE AND RISK MANAGEMENT

SM1 Risk management and certification

MNOs and other key stakeholders in the eSIM ecosystem are encouraged to include the eSIM in their risk management process. The entire end-to-end eSIM lifecycle should be addressed, taking into account the security principles of confidentiality, integrity, and availability.

The longevity of eSIMs, especially in IoT implementations, combined with the importance of IoT applications when included in critical sectors (as defined in the updated network and information systems (NIS) directive – NIS 2 directive([33])), should be factored into the risk management process. ENISA has published several tools to support such activities ([34]) ([35]).

The basic source of confidence in eSIMs lies with the GSMA Security Accreditation Scheme (SAS) ([36]), which offers the SAS certificate. This enables MNOs to evaluate the security of their eSIM suppliers via the SAS for UICC production (SAS-UP) and the security of the SM-DP(+) platforms via the SAS for subscription management (SAS-SM). In addition, MNOs should be encouraged to review certificates at contractual phases and also regularly, as the validity of certificates is usually renewed on an annual basis.

The following two key factors have been identified in the context of eSIM security.

a. The MNO is not directly connected to the eSIM manufacturer, which is a strong shift from the SIM manufacturer – MNO direct relationship. The absence of that relationship is compensated for by the introduction of certification and the role of parties such as the GSMA in ensuring the validity of certification.

([32]) ENISA, *Guideline on Security Measures under the EECC* (https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc).
([33]) Council of the European Union, *Strengthening EU-wide Cybersecurity and Resilience – provisional agreement by the Council and the European Parliament*, 2022 (https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/).
([34]) https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools
([35]) https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox
([36]) GSMA, *Security Accreditation Scheme* (https://www.gsma.com/security/security-accreditation-scheme/).

b. The provisioning process has been essentially dematerialised, creating vast opportunities for variations of seamless provisioning processes. MNOs should embed security in those processes to effectively protect the part of the end-to-end process that is directly under their responsibility. The ENISA *Countering SIM-Swapping* report [37] points out that eSIM swapping attacks can be attributed to immature swap and provisioning processes.

Due to the plethora of entities involved in the eSIM certification process, MNOs are encouraged to establish a monitoring process to follow up periodically on the changes introduced to the eSIM certification and subsequently evaluate their cybersecurity posture.

MNOs should especially be encouraged to assess the impact of the COVID-19 interruption in the global logistics processes and proper on-site auditing, which was hindered by the absence of key personnel. Compensating mechanisms evolve to manage the COVID-19 impact and any eSIM security threats may be contained in the COVID-19-era production lots. However, it should be taken into account that the lifetime of eSIMs is significantly longer than another form of SIM ([38]).

As the eSIM is integrated within the device, a malfunction may affect not only the device itself but also any directly connected element. The eSIM's role becomes more important, as it becomes the de-facto root of trust (RoT) for the IoT.

As defining all stakeholders' limits of responsibility is practically impossible, a model of cooperation is being followed by MNOs. For example, Orange ([39]) proposed that the 'eSIM ecosystem stakeholders are co-actors and co-responsible of the ecosystem's global security'. The proposed model for achieving the same level of trust for eSIMs as for regular SIMs is based on i) certifying the different parts of the eSIM ecosystem and ii) permitting access by all stakeholders to security exposure and risk evaluations so that they can feed their own risk management and decision-making processes.

MNOs are encouraged to participate in such schemes and to frequently revise them.

SM2 Security of third-party dependencies

For most MNOs, a key issue remains their dependence on third-party eSIM platform providers, as they are unable to take on the costs of a self-built or acquired solution. Although these providers are well-respected ecosystem players that include rigid security requirements in their solutions, MNOs should include specific security clauses in the contracts and establish a security review mechanism.

Among other obligations, suppliers should be contractually obliged to report and address any security incident that may affect the MNO.

SM3 Security awareness (subscribers)

Attackers usually carry out phishing and/or social engineering techniques against unaware subscribers.

([37]) See footnote 1
([38]) Senior Officials Group Information Systems Security, *JIL Temporary Covid19 pandemic operational SOGIS evaluation and certification policy and rules*, 2021 (https://www.sogis.eu/documents/mra/JIL-TempCertCoronaPolicy-v1.1.pdf).
([39]) Orange, *How increasing the confidence in the eSIM ecosystem is essential for its adoption*, 2022 (https://hellofuture.orange.com/en/how-increasing-the-confidence-in-the-esim-ecosystem-is-essential-for-its-adoption/).

Therefore, conducting public awareness campaigns to inform subscribers about the potential threats, while advising them on good practices could contribute greatly to reducing the number of attacks and minimising their impact. According to the ENISA *Countering SIM-Swapping* report ([40]), the following precautions can be followed by subscribers to avoid phishing attacks.

- Be cautious with the information shared on social media networks.
- Do not open any suspicious internet hyperlinks or attachments received through email or messages.
- Avoid providing any personal information by email or by phone when called by someone claiming to be the MNO's representative. A real customer representative will never request personal details such as credit card details or two-factor-authentication SMS content. In some cases, MNOs can send a one-time password (OTP) SMS for finalising a SIM swap. This OTP must never be communicated to anyone, even to people who call customers and claim to be MNO employees.
- Update account passwords on a regular basis.

5.2 OPERATIONS MANAGEMENT

SM4 Securing the eSIM provisioning process

The provisioning process has been identified as a key process for the security of eSIMs.

As the downloading of a profile is equivalent to the one-to-one connection of the eSIM to a physical person or a specific device, a thorough review of the process should be performed regularly.

Established provisioning scenarios include:

- the use of an MNO-related application for confirming the request;
- the use of a QR activation method;
- the use of a connection between the device and the platform that is customer initiated via submission of their electronic identification (eID) and international mobile equipment identity).

Any introduction of changes in the process should be preceded by a security and privacy evaluation to safeguard process integrity.

5.3 HUMAN RESOURCES SECURITY

SM5 Continuous training and security awareness (personnel)

The MNOs should train their personnel properly and at regular intervals on relevant security risks relating to eSIMs, while keeping the relevant training records.

([40]) see Footnote (1)

5.4 SECURITY OF SYSTEMS AND FACILITIES

SM6 ISD-P management

On-card mechanisms can be applied to manage the ISD-P creation in order to avoid attacks focusing on depleting the memory resources of the card. Once an ISD-P is created, the mechanism should automatically delete the ISD-P if the awaited process of the 'DownloadProfile' (see the GSMA's remote provisioning procedure 'Download & Install') isn't received in the proper time frame. This action should also send a notification to the SM-SR.

SM7 eUICC's characteristics authentication

An undersizing memory attack by the SM-SR prevents MNOs and SM-DPs from installing profiles on an eUICC. This attack is only feasible due to the mutable fields of the EIS file that are not signed by the eUICC manufacturer nor by the eUICC.

This type of attack can be prevented, through the protection of the eUICC's mutable characteristics (e.g. 'remainingMemory'). This can be done by signing the values sent by the eUICC to the SM-SR during an 'AuditEIS', using the eUICC's private key which should also contain the specific timestamp. Thus, the SM-DP can be assured of the value's integrity while the card is protected from replay attacks by the SM-SR.

SM8 Profile size definition

The definition of a profile upper bound size will minimise inflated profile attacks. Through the introduction of an upper bound, when making a 'DownloadProfile' request, the SM-DP and the SM-SR would check the size of the profile to be safely created with this maximum size, thus mitigating malicious actions of profiles that exhaust the remaining memory.

SM9 Profile locking definition

Through the definition of an upper bound regarding the locking period (e.g. 12 months), a mechanism could be able to automatically unlock the eUICC once the specified time frame expires, thus preventing profile abuse by opportunistic MNOs. Additionally, the introduction of a counter set (to a specific value, e.g. >1), could permit profile locking only for a specific number of times during the lifetime of the eUICC (e.g. never, etc.).

SM10 Identity and access management

Multi-factor authentication should be used as a way of verifying identity prior to actions relating to the eSIM, in order to reduce the likelihood of a successful cyberattack.

For example, one of the most common multi-factor-authentication method used is the One Time Passwords (OTPs). Another example, currently used by multiple organisations for eSIMs, is the process of scanning a QR code. When a subscriber requests a SIM change online, they can log into a secure environment using their credentials in order to scan a specific QR code found there and realize the SIM change.

In order to prevent malicious attacks, the QR code should never be provided via alternative means (i.e. email, etc.). The identity of customers requesting a SIM change offline (e.g. in a shop) can also be verified on the basis of ID, in which case they will be provided with a physical voucher.

Other measures, analysed in the ENISA *Countering SIM-Swapping* report[41] could be also applied as and when appropriate.

5.5 MAPPING TO THE ENISA GUIDELINE

Table 2 maps the security measures analysed above to the risks and the security objectives of the ENISA guideline[42].

Table 2: eSIM security risks and measures mapping

Risk	Security measure	Security principle	ENISA security objectives
R1 sim swapping	SM1 risk management and certification SM3 security awareness (subscribers) SM4 securing the eSIM provisioning process SM5 continuous training and security awareness (personnel) SM10 identity and access management	Confidentiality	SO2, SO3, SO6, SO8, SO17, SO29
R2 memory exhaustion	SM1 risk management and certification SM6 ISD-P management	Availability	SO2, SO12, SO14, SO21, SO28
R3 undersizing memory	SM1 risk management and certification SM7 eUICC's characteristics authentication	Availability	SO2, SO12, SO14, SO21, SO28
R4 inflated profile	SM1 risk management and certification SM8 profile size definition	Availability	SO2, SO12, SO14, SO21, SO28
R5 locking profile	SM1 risk management and certification SM9 profile locking definitionSM9	Availability	SO2, SO12, SO14, SO21, SO28
R6 protocol attacks	SM1 risk management and certification SM3 security awareness (subscribers) SM5 continuous training and security awareness (personnel)	Confidentiality, Integrity	SO2, SO6, SO29
R7 attacks on the MNOs and other entities in the eSIM supply chain	SM1 risk management and certification SM2 security of third party dependencies SM4 securing the eSIM provisioning process SM5 continuous training and security awareness (personnel)	Confidentiality, integrity	SO1, SO2, SO4, SO9, SO10, SO12, SO14, SO15, SO28

[41] See Footnote 1
[42] See Footnote 32

6.CONCLUSIONS

eSIMs have been fully and successfully introduced into the mass market and are now supported by all major network operators across Europe and by a variety of devices.

With the help of all major device manufacturers, eSIMs are expected to become a standard feature in all major smartphone releases over the next few years.

eSIMs are also becoming the key Root of Trust (RoT) ([43]) solution for IoT devices.

They have proven to be a secure evolution of SIM technology, supported by standardisation and advances in relevant enabling technologies.

Although several security issues have been identified, current standards and evolving standardisation efforts seem to have adequately addressed these issues.

The role of authorities is twofold: enabling the adoption and introduction of a more secure technology that supports consumer interests, while safeguarding and reviewing the integrity of supporting processes.

eSIM is a secure evolution of SIM technology. eSIM is present in international roaming, 5G devices and connected vehicles but is not a consumer mass-market leader.

([43]) For any IoT device, a security foundation based on a secure hardware element can be used as a RoT. The purpose of a RoT is to contain security functions, information and data from device applications, secret keys and information about the IoT device.

ANNEX – INDUSTRY GOOD PRACTICES ON ESIM SECURITY

The following paragraphs introduce initiatives from industry, trade and standardisation bodies designed to mitigate eSIM-related vulnerabilities.

A. The role of GSMA in eSIM security

The GSMA is in charge of establishing standards for eSIMs to ensure that they are secure, reliable and interoperable with other devices.

The association has been a key player in defining how to comply with this new technology through relevant projects. GSMA documents lay out a specific set of rules that must be followed for an eSIM product to be considered compliant. These documents cover various aspects of eSIMs, including how the profile data, ID document, certificate and provisioning messages are structured and how these elements need to be generated for an eSIM.

The GSMA has also published security guidelines ([44]) to assist with the security and integrity of eSIM provisioning. These guidelines recommend that entities generating provisioning messages should use a secure network and a certificate issued by a legitimate authority, follow strong cryptographic practices and support eSIM data integrity checks, including signing the provisioning message and encrypting the message body.

The association is also responsible for overseeing the submission of eSIMs to the appropriate bodies for homologation or approval, as required by relevant standards. Once approved, GSMA maintains a public database of all approved eSIMs and their attributes to help users easily identify which devices support which features and services.

The GSMA also provides an authorisation tool that allows organisations to verify if an eSIM has been approved by the appropriate body or not ([45]).

Table 3: Overview of the GSMA's eSIM security compliance documents

Consumer	M2M
SGP.24 declaration	SGP.16 declaration
PKI digital certificate	PKI digital certificate

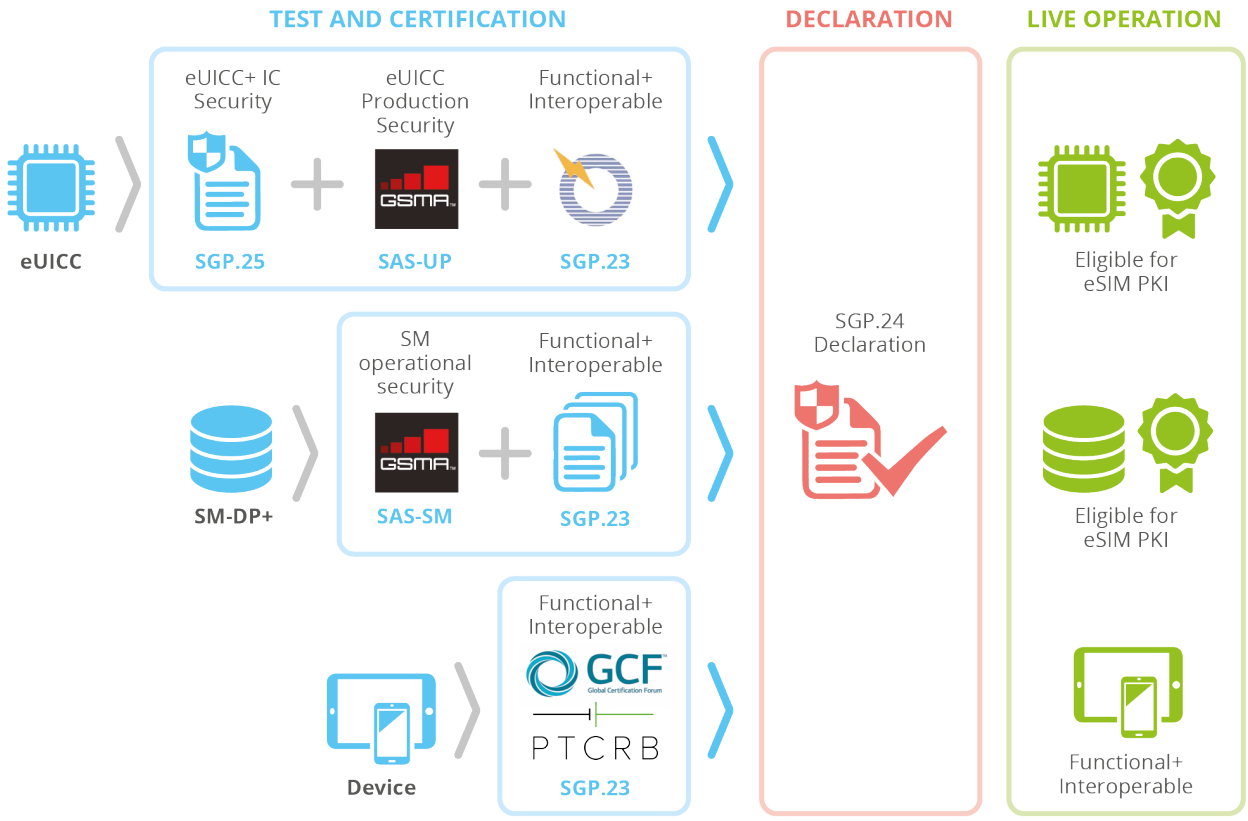
With the Security Accreditation Scheme, GSMA enables MNOs to assess the security of both their eUICC suppliers and their eUICC subscription management service providers.

([44]) GSMA, *eSIM Consumer Compliance* (https://www.gsma.com/esim/compliance/).
([45]) Kigen, *An Essential Guide to GSMA eSIM Certification*, 2020 (https://kigen.com/wp-content/uploads/2020/11/Kigen-An-essential-guide-to-GSMA-eSIM-certification.pdf).

Two schemes operate under the SAS.

- SAS-UP: eUICC manufacturers undergo a production site and processes security audit. Following successful results, manufacturing sites are awarded security accreditation valid for 1 year.
- SAS-SM: addresses the security of remote provisioning for eUICCs based on a security auditing and accreditation scheme for the providers of eUICC subscription management services.

Figure 9: Overview of the eSIM compliance process



GSMA is the key point of cooperation between involved parties and is driving the technical security work on eSIM. MNOs are encouraged to keep track of the GSMA's work on eSIMs and address the adherence of their supply-side partners to this work.

Regarding the use of eSIMs in 5G, the GSMA Fraud and Security Group advises that preventing eSIMs from accessing network slices does not limit the attack scenarios and that network security policies that prevent the attacks at a technical level need to be implemented.

GSMA has issued the IoT SIM applet for secure end-to-end communication ([46]) to enable IoT device manufacturers and IoT service providers to leverage the eSIM as a robust, scalable and standardised hardware RoT to protect IoT data communications. This can be used as a basis to manage eSIM-related risks.

Table 4 provides the latest GSMA core eSIM (consumer and IoT) specifications and the corresponding relevant test and requirement specifications.

([46]) GSMA, *IoT SAFE*, 2021 (https://www.gsma.com/iot/iot-safe/).

Table 4: Overview of GSMA eSIM specifications

Architecture specifications (includes eSIM Discovery)	SGP.21 eSIM architecture specification SGP.31 eSIM IoT architecture and requirements specification SGP.22 V3.0 (not published yet) SGP.32 v1.0 (not published yet)	
Technical specifications	SGP.22 eSIM technical specifications SGP.23 V1.12	
Test specifications	SGP.23 eSIM test specifications SGP.26 eSIM test certificates	
GSMA eID definition and assignment	GSMA eID definition and assignment	
Compliance specifications	SGP.24 eSIM compliance process	Provides a description of obligatory process and procedures to be followed to declare a product, platform or service, compliant with the GSMA requirements and technical specifications defined in SGP.21 and SGP.22.
Security evaluation of integrated eUICC	SGP.08 GSMA security evaluation of integrated eUICC	
GSMA eUICC SAS	GSMA eUICC security assurance specifications	
eUICC for consumer device protection profile	SGP.25 eUICC for consumer device protection profile V1.0	
eUICC PKI certificate policy	SGP.14 eUICC PKI certificate policy V2.0	CIs must operate GSMA-recognised certificate roots for certificate issuance, in line with the GSMA eUICC PKI certificate policy, GSMA permanent reference document (PRD) SGP.14.
GSMA CI registration criteria	GSMA PRD SGP.28 eSIM CI registration criteria	CIs must comply with GSMA PRD SGP.28.

B. Other initiatives and key organisations

The GSMA Mobile Connectivity Group aims to deliver a secure, scalable and interoperable framework for deploying eSIMs for use in multiple connected devices.

The group is a key contributor to the global eSIM initiative, a collaborative effort between GSMA and the Global Smart Card Alliance to establish an industry-wide initiative that defines an open interface standard for global eSIM deployments in both consumer and M2M markets. The initiative contributes to the GSMA mobile identity initiative by defining global eSIM standards for authentication, security, privacy and data protection, along with application management capabilities.

The European Telecommunications Standards Institute (ETSI) plays also a vital role in eSIM security (e.g. work on Technical Specification 103.645).

Finally, the International Telecommunication Union's Telecommunication Standardization Sector Study Group 2 is currently working on a technical report on the carrier switching of SIMs and e-SIMs for businesses in M2M/IoT ([47]).

Overall, there is widespread cooperation on standardisation of eSIM security. This is partially driven by the idea that eSIM, due to its forecasted wide distribution and its inherent security characteristics, may become the de facto security element needed for a plethora of domains and applications.

([47]) International Telecommunication Union Telecommunication Standardization Sector, *Technical report on the carrier switching of SIM and e-SIMs for enterprises in M2M/IoT* (https://www.itu.int/ITU-T/workprog/wp_search.aspx?isn_sp=8265&isn_status=-1,1,3,7&title=SIM&details=0&field=acdefghijo).

TP-05-22-387-EN-N

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-598-2
doi:10.2824/161297