TRUSTED CONNECTIVITY ALLIANCE

Protecting Subscriber Privacy in 5G

July 2020

Intellectual Property Rights (IPR) Disclaimer

Attention is drawn to the possibility that some of the elements of any material available for download from the specification pages on Trusted Connectivity Alliance's website may be the subject of Intellectual Property Rights (IPR) of third parties, some, but not all, of which are identified below. Trusted Connectivity Alliance shall not be held responsible for identifying any or all such IPR, and has made no inquiry into the possible existence of any such IPR. TRUSTED CONNECTIVITY ALLIANCE SPECIFICATIONS ARE OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER TRUSTED CONNECTIVITY ALLIANCE, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION.

Table of Contents

1. Executive Summary

Protecting consumer privacy is a critical consideration in today's connected world. The advent of 5G presents an opportunity to address key privacy concerns for mobile networks. But while industry standardisation efforts have undoubtedly made progress, the significant variability in terms of implementation means there are many scenarios in which private subscriber information is still vulnerable.

This paper outlines the threats, challenges and why they must be addressed. It also describes the clear benefits of leveraging the 5G SIM, a tamper-resistant secure element (SE), to deliver best-in-class security, and why mobile network operators (MNOs) should strongly consider ensuring the consistent protection of subscriber privacy across the globe using the 5G SIM.

2. Abbreviations

5G SIM	In this document, "5G SIM" refers to the SIM or eSIM as defined as Recommended 5G SIM by TCA. A key feature of the 5G SIM is to protect end user privacy through encryption of the subscriber identifier.
AMF	Access and Mobility Function
EUM	eUICC Manufacturer
IMSI	International Mobile Subscriber Identity
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
OEM	Original Equipment Manufacturer
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier

3. Introduction

3.1 Mobile Networks and the Digital Economy

Mobile networks play an integral role in the digital life of subscribers, and have evolved far beyond enabling voice calling and SMS. For example, Facebook statistics show that in January 2020, 98 percent of active user accounts worldwide accessed the social network via any kind of mobile phone.[1]

And of course, other devices besides the mobile phone can connect to cellular networks and be associated with a subscriber. This includes wearables such as smartwatches or fitness trackers, tablets and PCs, connected cars, and even smart home appliances.

The advent of 5G technology, which by 2025 will cover up to 65 percent of the world population and generate 45 percent of the world's total mobile traffic, will further expand the potential utility for cellular technology.[2]

3.2 Consumer Privacy Concerns

With global digitalisation advancing and with users tending to be "always connected", however, there is increasing concern about the privacy implications.

The time where we could purchase, travel or simply live without leaving digital footprints seems to have passed. The sensitivity of the information collated by mobile phones and other connected devices, which includes communications, location and even medical data, means that any compromise can lead to damaging breaches of user privacy. Potential consequences include, but are not limited to, blackmail, harassment, employee monitoring, commercial profiling and fraud. [3]

Given these profound potential consequences, coupled with high-profile incidents and breaches, privacy is an increasingly pressing concern for consumers. According to research conducted by the Boston Consulting Group, "privacy of personal data is a top issue for 76 percent of global consumers and 83 percent of U.S. consumers". This has a direct impact on consumer behaviour, with the same report noting that "[…] because of privacy concerns, more than a third of respondents (38 percent) reported cutting back their use of social media."[4]

3.3 Privacy Regulation Around the World

For these reasons, enforcing privacy protection has emerged as a key focus for multiple regulatory bodies worldwide.

The strictest and most comprehensive regulation is that introduced in the European Union (EU) with the establishment the General Data Protection Regulation (GDPR), which took effect in spring 2018 after a three-year preparation period. GDPR reinforces user privacy protection on a national and global level, and imposes strict controls on the collection, storage and use of consumer data. Companies not in compliance face fines of up to a maximum €20 million or 4 percent of the total worldwide annual turnover of the preceding financial year. By the end of 2019, authorities had issued €400 million in fines.[5]

---

[1] Statista, *Device usage of Facebook users worldwide as of January 2020*, January 2020
[2] Ericsson, '*Ericsson Mobility Report*', November 2019
[3] For more insight into the potential privacy implications across key use-cases, see www.trustedconnectivityalliance.org
[4] Boston Consulting Group, Data Privacy by the Numbers, February 2014
[5] Alpin, *Major GDPR Fine Tracker*, April 2020

GDPR has transformed the privacy landscape. We have already seen similar regulation introduced in the U.S., for example, where companies must now demonstrate what measures they have taken to protect user privacy and data following major security breaches and complaints.

3.4 MNOs and Privacy

Mobile subscribers are consistently reported to place a high degree of trust in mobile network operators (MNOs), and the industry is known for its cautious approach to data processing when compared to other sectors.

However, significant privacy vulnerabilities are emerging and, given the sensitive nature of the data processed by MNOs, the reputational and commercial consequences of a breach are considerable.

The potential level of risk in this area demands robust support for subscriber privacy.

3.5 Industry Initiatives to Promote Subscriber Privacy

5G technology has presented an opportunity for industry standardisation efforts to address potential vulnerabilities and boost consumer trust.

Within the standards for 5G, the 3GPP[6] introduced a new feature in order to protect the most prominent personal data involved in mobile communications, the International Mobile Subscriber Identity (IMSI). This new encrypted IMSI is also called the Subscription Concealed Identifier (SUCI). This is designed to address a significant privacy vulnerability known as IMSI catching attacks.

In this white paper, we explain in more detail:

- Why this new feature has been introduced in 3GPP 5G standards, and the challenges created by variable implementations;
- How IMSI catchers work and why they present a significant and growing threat to subscriber privacy;
- The different options for MNOs to implement IMSI encryption;
- Why implementing IMSI encryption within the 5G SIM delivers significant benefits;
- The necessary balance between subscriber privacy and law enforcement investigation;
- How IMSI encryption can complement broader privacy and security frameworks; and,
- How IMSI encryption can support privacy across consumer and industrial IoT use-cases.

4. Problem Statement

In mobile network technologies, MNOs allocate a unique subscriber identifier to each SIM card. This is known as an IMSI in 4G and a Subscription Permanent Identifier (SUPI) in 5G.[7] The IMSI represents the relationship between subscribers and the MNO that issued the SIM card, so can be used to confirm the subscribers identity and monitor their location, calls and SMS messages.

[6] 3GPP is the technical body that develops standards for mobile networks.
[7] Note this identifier must not be confused with the subscriber's mobile phone number (MSISDN). It is the IMSI that properly identifies each unique subscriber on the network. In addition and for the purposes of this document, the term "IMSI" will be used when referring to both the IMSI and SUPI unless explicitly stated.

Encrypting this information therefore has clear privacy benefits. However, this feature may be implemented in several ways according to the 3GPP specifications. It may or may not be activated in the network, and if activated, it may or may not be supported in a device and in a SIM, be it in the form of a removable card or embedded into the device (eSIM).

This variability results in several potential situations where the protection of end-user privacy is not guaranteed:

- The IMSI encryption feature is not activated, i.e. the network operator uses the NULL encryption scheme in the network. This exposes the IMSI and means end-user privacy is not protected.
- The IMSI encryption feature is activated in the network but end-users with a 5G device do not use a 5G SIM, and instead use an older version of the SIM that does not support IMSI encryption. Again, the IMSI remains exposed and end-user privacy is not protected.
- The IMSI encryption feature is activated in the network and 5G end-users have a 5G SIM that does not support IMSI encryption. In this case, the device executes the cryptographic operations defined to protect the IMSI as per the 3GPP standards. But because such devices come from a high diversity of original equipment manufacturers (OEMs), the risk of inconsistency between device in terms of implementation, interoperability and security assurance level, and ultimately on IMSI privacy protection increases.

In order to remove this uncertainty and ensure best practice in protecting end-user privacy, MNOs should consider additional measures to limit the available options and steer other stakeholders to rely on proven and certified solutions.

The following chapters offer a more detailed analysis of these vulnerabilities and considerations, and provides recommendations on how to address them.

5. IMSI Catchers and Subscriber Privacy

In the current 2G, 3G and 4G network technologies, as defined in the 3GPP standards, the IMSI is sent unencrypted over-the-air and passes through the phone at first connection to the network or, more rarely, when the network specifically requests it. Once the subscriber is authenticated and identified by the network, a temporary IMSI is allocated to that subscriber's mobile phone for further communication.

The privacy implications of sending the IMSI in clear over-the-air are significant, given vulnerability to well-known attacks from IMSI catchers exposing subscriber's identification, location, and calls.[8]

5.1 How Does an IMSI Catcher Work?

The mobile phone usually selects the cell with the strongest signal, which is where an IMSI catcher comes into play. This malicious device simulates a cell with a better signal strength due to its proximity. Then, it can launch the basic identification procedure by requesting the mobile phone's IMSI and confirm that the subscriber is in the area. After that, the IMSI catcher relays the traffic between the real cell site and the subscriber's mobile phone, conveniently intercepting any data it wants. This can be used to track location, divert calls or collect users' data.

Techniques also exist that redirect the subscriber from a secure network access technology, such as 3G or 4G, to a less secure network access technology, i.e. 2G, that does not require the

[8] Note that in this white paper, the term 'IMSI catchers' is used to encompass the whole Cell Site Simulator family.

network to authenticate the SIM. By deactivating some security services, the attacker is able to locate the user and the SIM to snoop on the conversation of the targeted IMSI.

5.2 How Easy is it to Obtain IMSI Catchers?

Given the sensitivity and value of the data that can be obtained by intercepting the IMSI, it is not unreasonable to think that IMSI catchers would require a high level of technical sophistication to build, or could only be bought at great expense from the deepest corners of the dark web. Unfortunately, this is not the case.

Even though using or buying an IMSI catcher is strictly regulated, there may be fraudulent usage as it is possible to build a basic IMSI catcher easily for *only $7* with some open-source code. Incredibly, step-by-step tutorials detailing how to build IMSI-catchers already exist on YouTube, including a helpful signpost to the required equipment on eBay.

For those with larger budgets, there are also sophisticated IMSI catchers for sale on the public web, such as Alibaba. For $1,800, it is possible to buy an IMSI catcher that enables the user to redirect a 3G mobile phone to a specific GSM frequency, in order to monitor the conversations with active or passive cellular monitoring systems. Other models, for example, allow the suppression of specifically selected conversations of targeted persons.

5.3 IMSI Catchers in Practice

In the end, it is unsurprising that IMSI catchers may already be maliciously deployed. The Department of Homeland Security has reported the use of IMSI catchers by an unidentified entity 'operating near the White House and other sensitive locations in Washington.'[9]

6. IMSI Encryption to Protect Subscriber Privacy

The publication of 3GPP Release 15 introduced the possibility for MNOs to encrypt the IMSI before it is sent over-the-air. The 3GPP standard refers to the SUPI and the SUCI (Subscriber Unique Concealed Identity). Note that once the selected encryption scheme is applied to SUPI, it is called the SUCI.

The IMSI is encrypted using a classical private and public key scheme that uses new cryptography in cellular called Elliptic Curve Cryptography (ECC). The ECC enables fast and secure calculations. The IMSI is encrypted, every time there is an enquiry, through the Elliptic Curve Integrated Encryption Scheme (ECIES) with an MNO public key that is stored in the SIM. Only the MNO can decrypt the IMSI thanks to its private key, which is known only by the MNO.

For additional protection, the public key shall also be kept secret. Storing this public key in the 5G SIM and performing the encryption within the 5G SIM ensures this key is not shared to untrusted entities.

A new, freshly encrypted IMSI is sent each time it is requested by the network, preventing the tracking of a given subscriber, and therefore protecting their privacy.

[9] Washington Post, 'Signs of sophisticated cellphone spying found near White House, U.S. officials say', June 2018. An explanatory video is also available here.

7. Comparing Options for IMSI Encryption

Within 5G, there are now two ways of encrypting the IMSI for MNOs. The standards state that it can be performed either by the SIM or by the device.

For optimum security, and to ensure MNO end-to-end control of the IMSI encryption and decryption process, it is recommended that it is performed within the secure element (SE) that the MNO trusts and controls, i.e. the 5G SIM.

The following table supports this recommendation by comparing both options based on the following key criteria:

- Ownership of the IMSI privacy protection
- Control over the actual technical implementation and exchange of sensitive data
- Flexibility to realise non-standardised algorithms or features / extensions
- Security level and available security certification
- Production and provisioning of relevant parameter
- Performance and interoperability

7.1 Comparison Between 5G SIM and Device Encryption

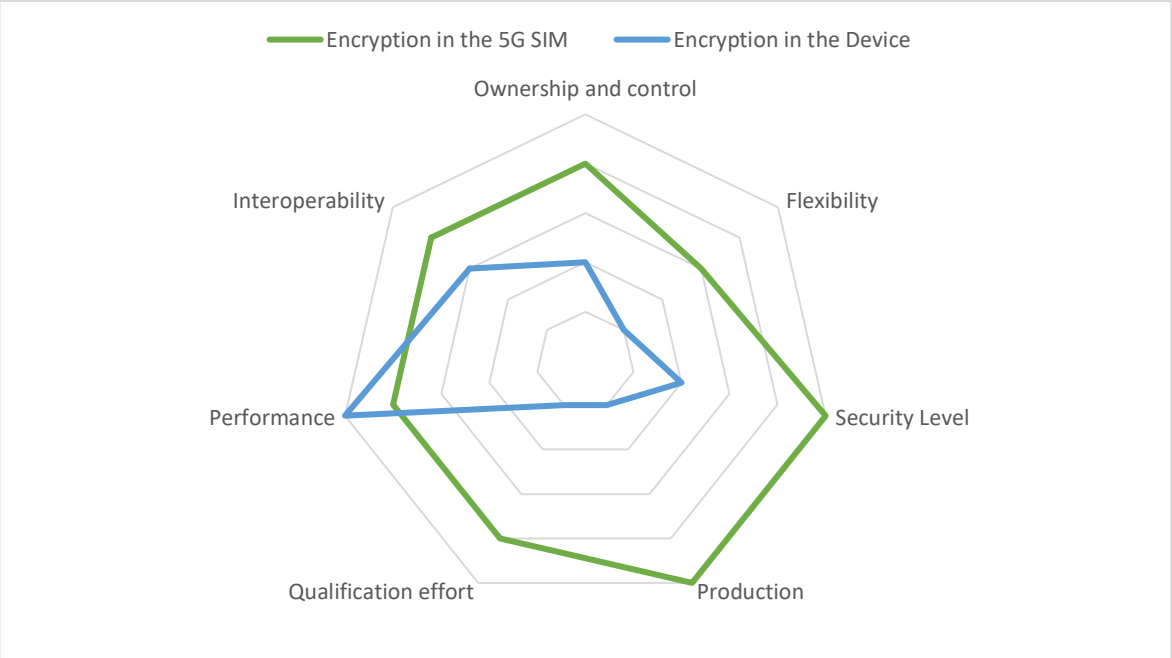

Figure 1: Comparison between 5G SIM and device encryption

	Encryption in the 5G SIM	Encryption in the Device
Ownership and control	The MNO owns the 5G SIM configuration and thus controls the security and privacy of the IMSI end-to-end from the SIM to the network, so the MNO is directly enforcing subscriber privacy.	The OEM is the owner of the device and owns the implementation of the IMSI security and privacy protection within the device. MNOs are unsure of implementation quality due to lack of business levers to control OEMs.
Flexibility	The MNO can request the EUM to support MNO specific security algorithms used for SUCI calculation within the 5G SIM in the future.	OEM may limit their implementations to standardised options only. Consequently, for off the shelf devices, MNOs have no control and cannot impose a specific algorithm on the OEM.
Security Level	Tamper-resistant SEs, the foundation of the 5G SIM, offer the highest level of security. In addition, eSIMs are certified according to recognised schemes. This allows the protection of the MNO public key as well as the Subscriber Permanent Identifier (SUPI) when encryption is performed by the 5G SIM.	Implementation of SUPI-concealing within the device does not provide any dedicated and certified security. It could therefore be susceptible to malware attacks.
Production	The SIM is produced and provisioned in secure production facilities. The eSIM configuration is controlled by the MNO. Secure and well proven interfaces and processes to exchange sensitive information are established between the MNO and the SIM manufacturer / EUM.	Devices may be built in uncontrolled facilities.
Qualification effort	Less qualification to be performed because there are less suppliers and test suites available. Implementation within the 5G SIM ensures consistent behaviour of the SUCI calculation across all devices and throughout the network.	The combination of brands, models and operating systems versions is leading to a high number of qualification activities, especially for IoT devices.
Performance	Processing may be slower compared to a device, but still delivers a seamless user experience.	Fast computation within the device depending on the implementation.
Interoperability	Well-established processes to ensure interoperability between different 5G SIM implementations.	Multiple different device types and operating system versions may increase the risk of interoperability issues.

***

As the above table demonstrates, encryption within the 5G SIM is clearly preferable across a range of key factors. Processing speed ('performance') may be slightly slower when encryption is executed within the 5G SIM, but it should be emphasised that this is only minimally so and only seldomly executed. Overall, encryption within the 5G SIM is markedly superior in terms of ownership and control; the security of the SIM and its production process; and certification and interoperability.

8. What about Lawful Interception?

There is an important balance to be found between protecting a citizen's right to privacy, and ensuring that governments and law enforcement agencies can track and monitor criminals when necessary. Some concerns have been raised regarding the 5G SIMs highly secure standardisation requirements, and how they could potentially compromise the implementation of lawful interception.

While encrypting the IMSI does prevent the unlawful and malicious usage of IMSI catchers, governments and other law enforcement agencies will still be able to track and monitor targets with the collaboration of MNOs. In addition, other methods and tools also exist to help them continue harnessing data to obtain necessary and actionable intelligence:

- Governmental agencies can still access the core network of MNOs to track and monitor targeted subscribers.
- If a roamer from a foreign country is targeted by a governmental agency, then 3GPP specifies in 3GPP TS 33.501 that the Visited Core Network shall be able to get the IMSI from the Home Network or reject the subscriber".[10]

9. Privacy Regulation Around the World

It should also be considered how IMSI encryption within the 5G SIM supports compliance with broader privacy and security frameworks worldwide.

In Europe, for example, IMSI encryption supports compliance with GDPR and the e-Privacy Directive (which concerns the processing of personal data and the protection of privacy in the electronic communications sector). In addition to supporting GDPR-compliance, it also addresses points identified by the NIS Cooperation Group within 'Cybersecurity of 5G Networks – EU Toolbox of Risk Mitigating Measures.'[11]

Beyond Europe, the broader regulatory trend of granting data subjects increasing rights and data processors increasing obligations, particularly as regards data privacy and security, is echoed in legislation such as the Australian Privacy Principles (APPs)[12], Japan's newly-strengthened Act on the Protection of Personal Information (APPI)[13], and the more recent California Consumer Privacy Act.[14]

[10] 3GPP, 3GPP TS 33.501, March 2017
[11] NIS Cooperation Group, Cybersecurity of 5G Networks – EU Toolbox of Risk Mitigating Measures, January 2020
[12] Office of the Australian Information Commissioner, Australian Privacy Principles, February 2018
[13] Japan and the Personal Information Protection Commission, Act on the Protection of Personal Information, May 2017
[14] State of California, California Consumer Privacy Act, June 2018

10. Privacy for IoT

Consumer privacy should not be limited to mobile handsets, IoT devices must also be addressed. This paper has already identified that IoT devices like wearables (smart watches, health monitoring devices, fitness trackers), connected cars, and smart home gadgets collate extremely sensitive information.

10.1 Industrial IoT Use-Cases

Industrial devices deserve attention, too. Industrial Internet of Things (IIoT) promises to revolutionise the manufacturing, energy, agriculture and transportation sectors.

Some 'machine type' IoT devices (like smart meters or robots) are expected to be key components in critical infrastructures. In this context, security and privacy can really be a matter of life and death. For example, in the threat model from the *ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,* the sensitive data leakage is classified as having a Crucial Impact, the highest rating among Crucial, High, and Medium.[15]

10.1 Addressing Market Fragmentation

The IoT space adds a new dimension to the encryption debate. In comparison to the consumer handset industry, the IoT market is extremely fragmented. Many companies have little experience or institutional knowledge of security and privacy.

Consequently, an efficient and secure deployment of device-based encryption seems out of reach. This means SIM / eSIM based encryption is the only realistic option to decrease fragmentation and ensure interoperability, another consideration that should be taken into account by MNOs wanting to foster their IoT business.

***

[15] ENISA, ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017

11. Conclusions

- Subscriber privacy is a critical consideration for MNOs and requires strong protection mechanisms, as the reputational, commercial and regulatory consequences of a privacy breach are significant.

- IMSI catchers are a known concern for subscriber privacy. The easy accessibility means this equipment is not just the preserve of sophisticated criminal organisations or nation-states. Nor is this merely a theoretical vulnerability with little prospect of real-world exploitation. Any individual could conceivably capture the IMSI and track the activity and location of a targeted subscriber. If we consider the potential implications, it is clear that this is a significant violation of a subscriber privacy that must be addressed.

- While the 5G standards introduced by 3GPP allow for IMSI encryption, there is potential for significant variability in terms of implementation. This creates various scenarios where the IMSI is not protected and consumer privacy is still at risk. MNOs should therefore consider additional measures to limit the available options and steer stakeholders to rely on proven and certified solutions.

- The recommended way to promote privacy is to manage this IMSI encryption within the 5G SIM, rather than the device. A comparison of key criteria clearly supports this recommendation.

- IMSI-encryption is capable of supporting privacy and security standards mandated by regulatory bodies worldwide. Given this broad utility, all MNOs should strongly consider IMSI encryption within the 5G SIM to support broader regulatory compliance.

- While encrypting the IMSI does prevent the unlawful and malicious usage of IMSI catchers, governments and other law enforcement agencies will still be able to track and monitor targets with the collaboration of MNOs.

- SIM-based encryption is the only viable way to establish interoperability across the vast array of consumer and industrial IoT use-cases.

12. About Trusted Connectivity Alliance

Trusted Connectivity Alliance is a global, non-profit industry association which is working to enable a secure connected future. Its members are participants within the SIM ecosystem, which is the most widely distributed, secure application delivery platform in the world. The organisation's vision is to facilitate the sustained growth of connected objects through trusted connectivity which offers protection for service provider assets, application and device data and end user privacy. Members have an interest in SIM, embedded SIM (eSIM), embedded SE (eSE), integrated SE and SIM (iSIM, iSE), hardware and software IP provisioning or related personalisation services. They work collaboratively to identify and deliver collective work requirements, of a technical, strategic and marketing nature, which will support the ability of mobile network operators, OEMs, device manufacturers and service providers to choose connectivity solutions which benefit from end-to-end security.

Trusted Connectivity Alliance members represent over 80% of the global SIM market and include: Arm, Card Centric, COMPRION,, Giesecke+Devrient Mobile Security, IDEMIA, KONA I, Linxens, NXP, Qualcomm, Thales, ST, Valid, Watchdata, Workz and Wuhan Tianyu.

www.trustedconnectivityalliance.org