TCA
TRUSTED
CONNECTIVITY
ALLIANCE

Protecting Subscriber Privacy in 5G

Frequently Asked Questions

March 2021

Copyright © 2021 Trusted Connectivity Alliance ltd.

The information contained in this document may be used, disclosed and reproduced without the prior written authorization of Trusted Connectivity Alliance. Readers are advised that Trusted Connectivity Alliance reserves the right to amend and update this document without prior notice. Updated versions will be published on the Trusted Connectivity Alliance website at http://www.trustedconnectivityalliance.org

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.

5G SIM: Promoting Subscriber Privacy

Frequently Asked Questions (FAQs)

1. Does the device need to be trusted as the IMSI could still be read out from the Elementary File (EF) stored in the 5G SIM[1]?

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

In the current 2G, 3G and 4G network technologies, as defined in the 3GPP standards, the IMSI is sent in clear over-the-air without being encrypted. This exposes it to a well-known and significant vulnerability known as IMSI catching attacks.

IMSI catchers are easy to build or obtain and work as follows. As mobile devices usually select the cell with the strongest signal, IMSI catchers simulate a cell with a better signal. The IMSI catcher then launches the basic identification procedure by requesting the mobile phone's IMSI to confirm that the subscriber is in the area. It then relays the traffic between the real cell site and the subscriber's mobile phone, intercepting any data it wants.

The objective of the IMSI encryption is to ensure that IMSI is not circulating in clear on the network. This new encrypted IMSI is also called the Subscription Concealed Identifier (SUCI). This is designed to address the threat posed by IMSI catching attacks.

This means that the IMSI itself is not secret information that needs to be encrypted when accessed by the device, so it is not a matter of trust in the device. Data secrecy is different from data privacy, and data privacy is ensured by encrypting the IMSI when sharing over the network. Even if a mobile device is hacked and the attacker accesses the IMSI, this does not impact network privacy.

In addition, it should be noted that encrypting the IMSI within the SIM provides additional security for the network.

This is because to be able to authenticate to the network, the network needs to receive the encrypted IMSI. To generate the correct encrypted IMSI requires possession of the correct encryption key, as no further authentication exchange will be initiated if the encrypted IMSI received by the network is wrong. So although the IMSI can be read by the device, storing the encryption key and algorithm within the SIM to perform the encryption provides additional security compared to performing this encryption in the device, where the key is revealed in a less secure environment.

2. If a subscriber changes MNO using the eSIM subscription management feature, will it create interoperability issues with the IMSI encryption?

[1] "5G SIM" refers to both the SIM or eSIM as defined as Recommended 5G SIM by TCA.

No. Switching MNO profiles does not present any interoperability issues, even if the MNOs use different encryption methods. This is because all SUCI calculation parameters such as algorithms and encryption keys are stored and personalised inside each individual MNO profile, not in the eUICC operating system. In addition, the SUCI calculation parameters are fully standardised as per GSMA specifications. This standardisation guarantees complete interoperability across the IMSI encryption methods used by different MNOs.

The specifications are also flexible to allow MNOs to select their own proprietary encryption algorithms for their own intent. However, it is important to ensure the algorithms are supported by the UICC hardware and operating system.

3. Is IMSI encryption also relevant for IoT devices?

Yes. Privacy concerns are not limited to mobile handsets. IoT devices like wearables (smart watches, health monitoring devices, fitness trackers), connected cars, and smart home gadgets are increasingly connected to cellular networks and carry extremely sensitive user information. IMSI encryption can therefore play an important role in promoting subscriber privacy concerns.

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

Consequently, an efficient and secure deployment of device-based encryption is challenging.

This means SIM / eSIM based encryption is the best option to decrease fragmentation and ensure interoperability, another consideration that should be taken into account by MNOs wanting to foster their IoT business.

4. Will a 5G SIM card capable of performing IMSI encryption also work on a 2G, 3G or 4G device?

Yes (with the right configuration). The standards defined by 3GPP, the standardisation body for cellular networks, are designed to ensure backward compatibility with previous mobile generations.

This means a 5G SIM card enabled with IMSI encryption capability will also let a 2G/3G/4G device connect to the corresponding network, as long as the network is properly configured. However, IMSI encryption will not be performed, as non-5G cellular networks do not support IMSI encryption.

5. What about lawful interception? Will governments and other law enforcement agencies be able to track criminals when necessary?

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.

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. Other methods and tools also exist to help them continue harnessing data to obtain necessary and actionable intelligence.

For example, governmental agencies can still access the core network of MNOs to track and monitor targeted subscribers. In addition, 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.

6. When should operators launch 5G standalone (SA) SIMs? Should it be before the first deployments of 5G SA devices, or at same time?

5G SA devices are already deployed on the market, with more being introduced. This is a driver for some MNOs to request 5G SIMs that have the capability to perform IMSI encryption to ensure they have the correct SIM deployed in the field when their 5G SA core network is activated. This will prevent the need to perform SIM recalls for 5G SA devices already deployed to users.

TCA therefore recommends introducing 5G SIM cards at an early stage to be ready for 5G SA deployments.

***

For more information on protecting subscriber privacy in 5G:

- Download the white paper.
- View the summary document.
- Watch the webinar.