TRUSTED CONNECTIVITY ALLIANCE

Protecting Subscriber Privacy in 5G

Protecting consumer privacy is a critical consideration in today's connected world.

The advent of 5G presents an opportunity for mobile network operators (MNOs) to address key privacy concerns, and to protect the most prominent personal data involved in mobile communications - the International Mobile Subscriber (IMSI)

What is an IMSI?

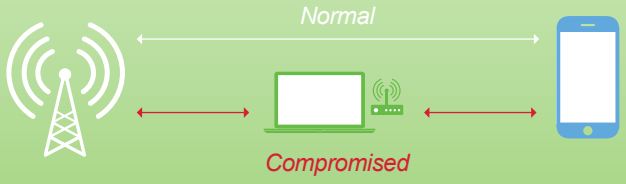
In mobile networks technologies, MNOs allocate a unique subscriber identifier to each SIM card. This is known as an IMSI in 4G and a Subscription Permanent Identifier (SUPI) in 5G.[1]

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.

IMSI Catchers and Subscriber Privacy

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.



1. The mobile phone usually selects the cell with the strongest signal.
2. This malicious device simulates a cell with a better signal strength due to its proximity.
3. The IMSI catcher launches the basic identification procedure by requesting the mobile phone's IMSI and confirm that the subscriber is in the area.
4. The IMSI catcher relays the traffic between the real cell site and the subscriber's mobile phone, intercepting any data it wants.

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 for great expense from the deepest corners of the dark web.

Unfortunately, this is not the case. It is possible to build a basic IMSI-catcher easily for only $7 with some open-source code and a helpful YouTube tutorial, or alternatively to buy one on the open web.

Promoting Subscriber Privacy through Standardisation

Encrypting this information therefore has clear privacy benefits. This is why the Trusted Connectivity Alliance Recommended 5G SIM supports IMSI encryption.

The 5G standards developed by 3GPP introduced the possibility for MNOs to encrypt the IMSI before it is sent over-the-air. However, 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:

- ⊗ *The IMSI encryption feature is not activated in the network.*
- ⊗ *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.*
- ⊗ *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. This increases interoperability risks and can impact the overall protection level.*

[1] *"IMSI" will be used to refer to both the IMSI and the Subscription Permanent Identifier (SUPI) throughout this document.*

[2] *"5G SIM" refers to both the SIM or eSIM as defined as Recommended 5G SIM by TCA.*

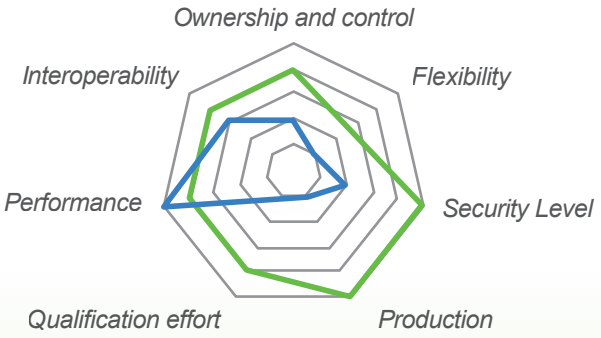
TRUSTED CONNECTIVITY ALLIANCE

Comparing Options for IMSI Encryption

Given these scenarios, the recommended way to enforce privacy is to manage this IMSI encryption within the 5G SIM, rather than the device.

Encryption in the 5G SIM

Encryption in the Device



	Encryption in the 5G SIM	Encryption in the Device
Ownership and control	MNO owns and controls IMSI implementation	OEM owns and fully controls implementation of IMSI security and privacy protection within the device
Flexibility	MNO can request the SIM manufacturer to support MNO-specific security algorithms within the 5G SIM	OEMs determine implementation; MNOs cannot impose a specific algorithm
Security level	Tamper-resistant secure elements, the foundation of the 5G SIM, offer the highest level of security as certified by recognised schemes	Security is neither certified nor dedicated to the device
Production	SIM produced and provisioned in secure, regulated facilities	Devices may be built in unregulated facilities
Qualification effort	Streamlined and simplified qualification process	Complex qualification process due to diversity of brands, models and operating systems
Performance	Relatively slower processing, but still a seamless user experience	Potentially fast computation within the device
Interoperability	Well-established interoperability between different 5G SIM implementations	Increased risk of interoperability issues

The Case for IMSI Encryption within the 5G SIM

- Sending the IMSI in clear over-the-air can create privacy issues, given the vulnerability to well-known attacks from IMSI catchers which can expose a subscriber's identity, location, calls and messages.
- While the 5G standards allow for IMSI encryption, different implementation options create various scenarios where the IMSI is not protected and consumer privacy is at risk.
- The recommended way to most effectively protect privacy is to manage this IMSI encryption within the 5G SIM, rather than the device. A comparison of key criteria clearly supports this recommendation.
- Governments and other law enforcement agencies will still be able to utilise lawful interception to track and monitor targets with the collaboration of MNOs.
- Beyond mobile handsets, SIM-based encryption is the only viable way to establish interoperability across the vast array of consumer and industrial IoT use-cases.