

5G

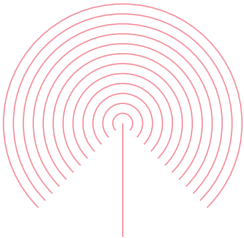
Protect subscriber privacy in 5G

Privacy protection is a key concern for consumers and authorities. With the 5G SIM, a tamper-resistant secure element, Mobile Network Operators (MNO) will be able to address this matter and more.

Contents

1. Protecting citizens & customer privacy: what's at stake for MNOs and their brand reputation?	6
2. Privacy issues to address:	6
2.1 How does an IMSI catcher work?	8
2.2 How easy is it to buy/build IMSI catchers?	9
2.3 Concerns are already public from U.S. Homeland Security	9
3. 3GPP introduced IMSI encryption to protect subscriber privacy	10
4. Is the 5G Network too secure?	11
5. Conclusion	11

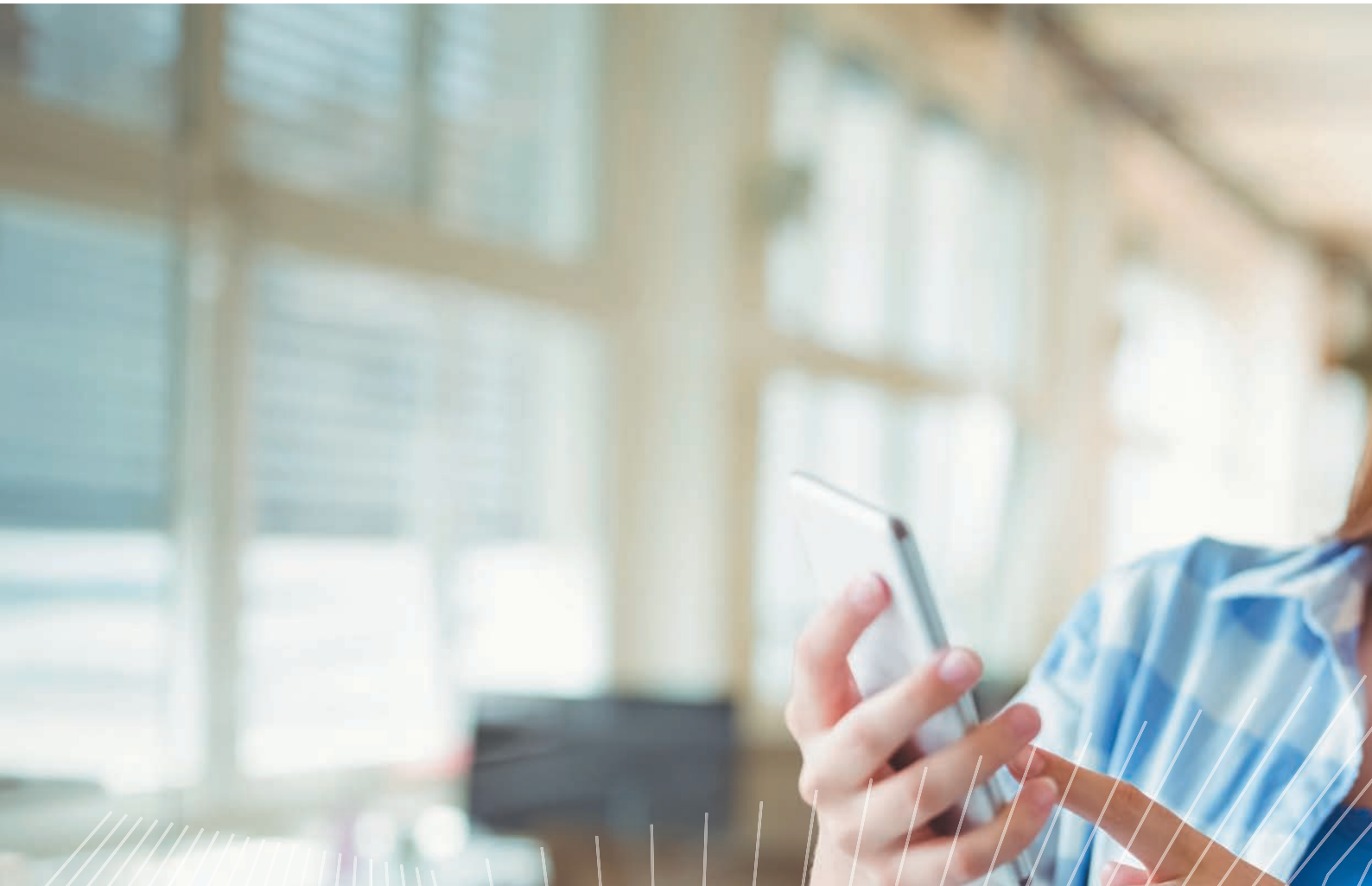
Executive Summary



As the world keeps advancing into a more digital-centric environment and as users tend to be “always connected”, they become more and more concerned about the fact that they can be identified and that their geolocation can be tracked by third parties, whether willingly or unbeknownst to them. This could lead to undesirable breaches of user privacy, opening the door to potential consequences, such as harassment, employee monitoring, commercial profiling, fraud, etc.

For these reasons, privacy concerns became a focus within different bodies of regulators to promote user privacy protection. We've already seen actions taken, for example, in the U.S. where companies have to demonstrate what measures they have taken to protect user privacy and data, after major security breaches and complaints.

In Europe, the EU set up the General Data Privacy Regulation (GDPR), which took effect in the spring of 2018 after a 3-year preparation period. This regulation reinforces user privacy protection, from a national level to a global one. Companies, not in compliance with this new regulation, run the risk of being fined up to ten million Euros or 2% of their total worldwide annual turnover of the preceding financial year.



With 5G telecommunication, the 3GPP standard has introduced a new feature for subscriber identity protection on the SIM, meant to address privacy problems known as IMSI catching attacks. This IMSI encryption feature is called the SUCI. In this white paper, we explain in more details:

- » Why this new feature has been introduced in 3GPP 5G standard
- » Why IMSI catchers present a growing threat to subscriber privacy and how they work
- » The different options for MNOs to implement IMSI encryption and why SUCI encryption in the 5G SIM enables MNOs to offer their subscribers best-in-class privacy and protects their brand reputation
- » The necessary balance between subscriber privacy and law enforcement investigation



1.

Protecting citizens & customer privacy:

What's at stake for MNOs and their brand reputation?

In the digital world, consumers and citizens are leaving traces everywhere, sharing some personal data without being aware of it and without their consent. The time where one could purchase, travel, and simply live without leaving a trace seems long past. This is becoming a concern for citizens, for MNO subscribers and for public authorities as well.

According to a 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”. “Because of privacy concerns, more than a third of respondents (38 percent) reported cutting back their use of social media*.”

In this context, it is important that MNOs begin taking measures to answer their subscribers' privacy concerns. Potential exposure to breaches would not only affect their subscribers but would also be detrimental to their brand reputation. While it is well known that subscribers trust their MNO, damaging that trust relationship because of privacy breaches could be traumatic.



2.

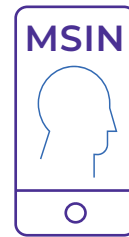
Privacy issues to address:

Why sending the IMSI in clear over-the-air can expose subscribers.

In mobile networks technologies, MNOs allocate a unique subscriber identifier to each SIM card known as an International Mobile Subscriber Identity (IMSI) in 4G and a Subscription Permanent Identifier (SUPI) in 5G. The IMSI/SUPI represents the relationship between subscribers and their issuing Mobile Operator. It is used by MNOs as a basis for secure mutual authentication and user identification. 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.

* <https://www.webopedia.com/Blog/we-cant-give-up-on-privacy.html>

The IMSI is composed of three fields



Mobile Country Code

indicates from which country the subscription comes

Mobile Network Code

indicates from which MNO the subscription depends

Mobile Subscription Identification Number

identifies the individual user of a particular MNO

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 and, passes through the phone at first connection to the network or, when the network is specifically requesting it (rarely). Once the subscriber is authenticated and identified by the network, a temporary IMSI is allocated to that subscriber's mobile phone for further communication.



Sending the IMSI/SUPI in clear allows well-known attacks from IMSI catchers*, exposing subscriber's identification, location, and calls.

* In this white paper, we are going to use the term IMSI catchers to encompass the whole Cell Site Simulator family.

2.1 How does an IMSI catcher work?

The mobile phone usually selects the cell that has 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. Some of them can even track the location, divert calls or collect users' data.



Techniques also exist that can redirect the subscriber from a secure cell, e.g. 3G or 4G, to a less secure cell, i.e. 2G, deactivating some security services to be able to locate the user and crack conversation or SMS for a targeted IMSI.

2.2 How easy is it to buy/build IMSI catchers?

Using or buying an IMSI catcher is illegal, but unfortunately, one can easily find tutorials to build a basic IMSI catcher for \$20 with some open-source codes. There are also some sophisticated IMSI catchers for sale on the internet public market place.

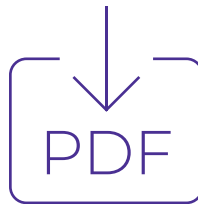
For \$1,800, one can buy an IMSI catcher that enables the user to redirect a 3G mobile phone to a specific GSM frequency in order to monitor the conversations with active or passive cellular monitoring systems. Some models, for example, allow the suppression of specifically selected conversations of targeted persons. This is not science fiction, nor expensive equipment only reserved for criminal organizations. IMSI catchers are now easily accessible and available on the web, not just the dark web.

Thanks to this type of equipment, one can capture the IMSI, which can be considered as private data, and track the location of a targeted subscriber, which in turn could be a violation of a subscriber's privacy.

2.3 Concerns are already public from U.S. Homeland Security



In a letter to senator Wyden, the U.S. Homeland Security department expresses concerns regarding an IMSI catcher:



<https://www.wyden.senate.gov/imo/media/doc/Krebs%20letter%20to%20Wyden%20after%20May%20meeting.pdf>



3.

3GPP introduced IMSI encryption to protect subscriber privacy

Along with 5G, 3GPP (the standardization body of cellular networks) has introduced, in 3GPP Release 15, the possibility for MNOs to **encrypt the IMSI before it is sent over-the-air**. The 3GPP standard is referring to the SUPI (Subscriber Unique Primary Identity) and the SUCI (Subscriber Unique Concealed Identity). Once the SUPI is encrypted, 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 through the ECC with the MNO public key. Only the MNO can decrypt the IMSI thanks to its private key. For best in class protection, the public key should be kept secret as well.

A different encrypted IMSI is sent each time the IMSI is requested by the network, preventing the tracking of a given subscriber, therefore **protecting their privacy**.

With 5G, there are now two possibilities for encrypting the IMSI for MNOs.

The standards state that it can be performed within the phone or within the SIM card. For optimum security, and to ensure MNO end-to-end control of IMSI encryption and decryption, it is recommended that they perform this encryption with the secure element the MNO is trusting and owns, i.e. the SIM card.

Preferring the SIM for the IMSI encryption prevents any

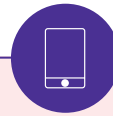
security breaches that could appear in the mobile phone device, which the MNO is not controlling. This also helps avoid technical interoperability issues with devices not implementing the IMSI encryption processing capability within the phone, or having to manage the different device OS that may have different implementations of IMSI encryption.

¹ The SUPI can be the IMSI, as we understand it in this white paper, but there is generalization in the standard where the subscriber identification can also be an email address for example.



Encrypting the IMSI within the SIM

- High level of security as it is done in a secure element
- Mastering security end-to-end
- No dependency on external entity such as phones



Encrypting the IMSI within the phone

- MNOs keep the SIM they have (with the same OS but a new profile)
- Fast computation leveraging high processing power of the phone



- Processing is slower than on phone, but it will be fast enough not to affect the user experience.

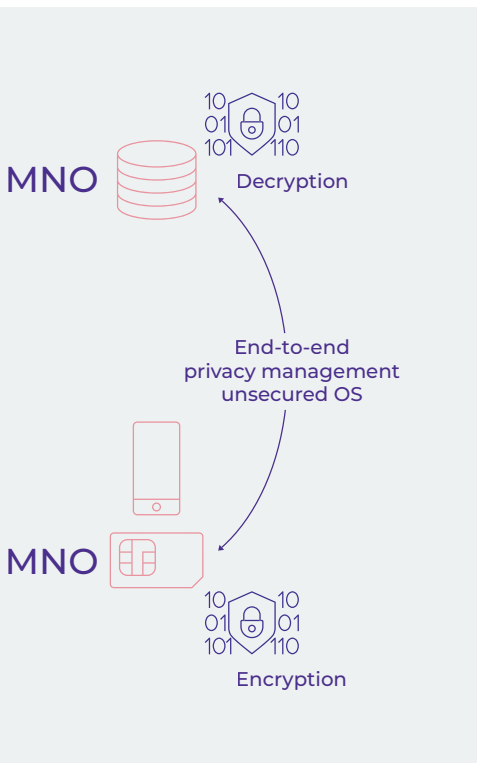


- Tests to be done for each phone/OS version at least at the beginning
- Security not enforced as running on non-secured OS
- Phone may be built with untrusted hardware
- Some devices are not going to implement SUCI in the phone

The recommended way for MNOs to ensure privacy protection is to manage this IMSI encryption end-to-end from the SIM card they own to the core network they control.

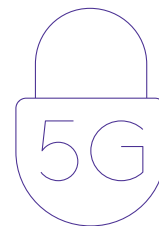
4.

Is the 5G network too secure?



Some concerns are circulating in the press regarding the 5G SIMs highly secure standardization requirements and how they will affect the usage of law enforcement IMSI catchers. While encrypting the IMSI does prevent the usage of IMSI catchers, governments and other law enforcement will still be able to track people of interest with the collaboration of MNOs. Other methods and tools also exist to help them continue harnessing data to power actionable intelligence.

There is always a balance to find between protecting citizen privacy and enabling law enforcement agencies to track criminals and fraudsters. Regulators in each country now have to decide on how telecom operators and law enforcement agencies will bridge that gap.



5.

Conclusion

Trust is everything. The 5G SIM ensures that the MNO remains a trusted brand by offering their subscribers best-in-class privacy protection. Moving forward, protecting citizens and consumer privacy is something MNOs have to take into serious account to avoid endangering their brand reputation and diminishing their subscribers' trust. Changing over to a 5G SIM now eliminates those two issues thanks to the IMSI encryption (or SUCI) key feature. Providing subscribers with the latest advanced standards in the SIM, MNOs are ensuring subscriber privacy with an end-to-end solution right from the 5G SIM card to their core network.

Protect **suscriber** **privacy** in 5G

idemia.com/5g-sim



All rights reserved. Specifications and information subject to change without notice.
The products described in this document are subject to continuous development and improvement.
All trademarks and service marks referred to herein, whether registered or not in specific countries, are the property of their respective owners.

Join us on     

www.idemia.com