Security Conference 2022

Protecting Private Networks and Subscriber Privacy with the 5G SIM

Benoît Collier
TCA Board Member
VP Product Line Mobile Operator BU at IDEMIA

04/09/2022

About Trusted Connectivity Alliance

Trusted Connectivity Alliance (TCA) is a global, non-profit industry association, working to enable trust in a connected future.

VISION: To drive the sustained growth of a connected society through trusted connectivity which protects assets, end user privacy and networks.

- Market Monitoring
- Specifications and Interoperability
- Industry Engagement and Strategy
- Education

Our Membership

TCA TRUSTED CONNECTIVITY ALLIANCE

Founding:

- Giesecke+Devrient Creating Confidence
- IDEMIA
- ST life.augmented
- THALES
- Valid

Executive:

- Kigen
- NXP

Full:

- CARD CENTRIC SOLUTIONS LTD. CARD CENTRIC
- 东信和平 EASTCOMPEACE
- Linxens crafting the future of connections
- OASIS smart sim Embed. Connect. Activate
- Qualcomm
- TIANYU
- WORKZ

Ordinary:

- COMPRION

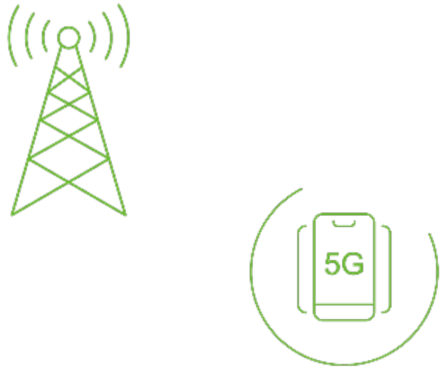
Mobile Networks and The Digital Economy

The advent of 5G is expanding the potential utility for cellular technology.

5G is now deployed in 54 countries with 121 active networks*

According to GSMA, global 5G connections will surpass 2 Billion by 2025.

As 5G SIM deployments continue to gather pace, protecting the most prominent personal data involved in mobile communications must be a critical consideration.



***Ericsson Mobility Report, May 2022**

Promoting Subscriber Privacy

- With global digitalisation advancing there is increasing concern about the **privacy implications**.
- The sensitivity of the information collated means that **any compromise can lead to damaging breaches of user privacy**.
- **Enforcing privacy protection** has emerged as a key focus for multiple regulatory bodies worldwide.
- Ensuring privacy for people as well as machines is also **critical as the IoT continues to expand**.

The Virginia Consumer Data Protection Act (CDPA)

GDPR

enisa THE EU CYBERSECURITY AGENCY

CALIFORNIA CONSUMER PRIVACY ACT

What is an IMSI?

TRUSTED CONNECTIVITY ALLIANCE

The International Mobile Subscriber Identity (IMSI) is a unique subscriber identifier allocated to the SIM by a Mobile Network Operator (MNO)

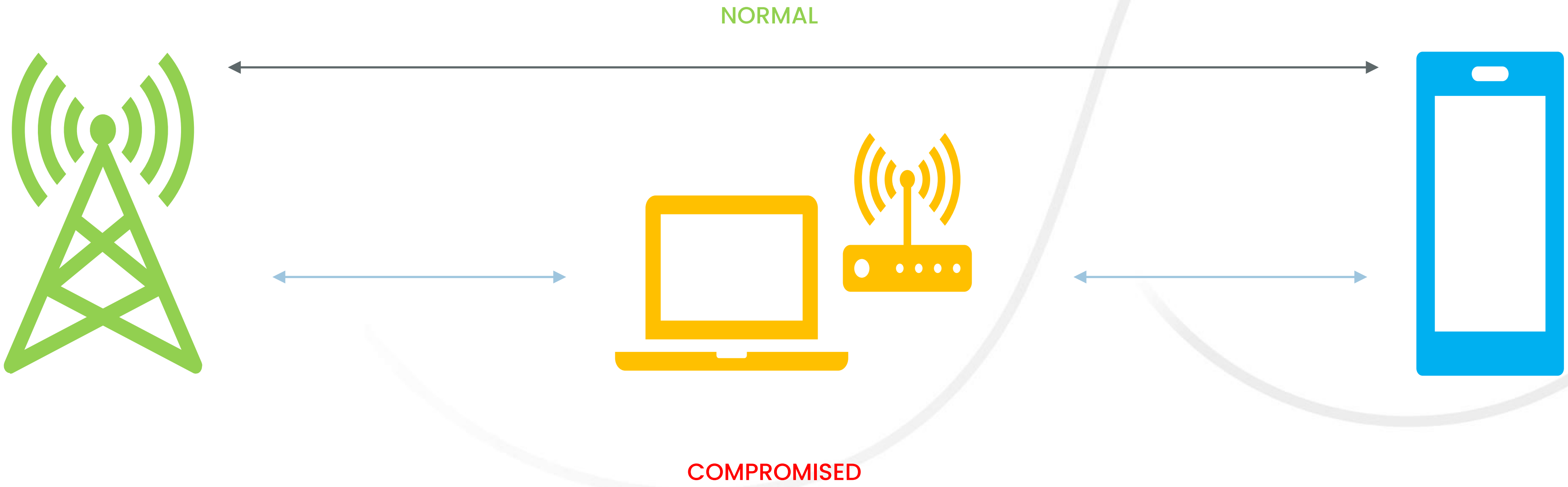
- The IMSI uniquely identifies an MNO subscription.
- It can be used to confirm a subscriber’s identity and monitor their location, calls and SMS messages.
- The IMSI should be considered private information.

IMSI Catchers and Subscriber Privacy

Despite representing highly-personal information, the IMSI is sent in clear over-the-air, ***completely unencrypted*** in the current 2G, 3G and 4G technologies (as defined by 3GPP standards).

This exposes the IMSI to significant security vulnerabilities, most notably IMSI catching attacks.

How an IMSI Catcher Works:



Promoting Subscriber Privacy through Standardisation

TRUSTED CONNECTIVITY ALLIANCE

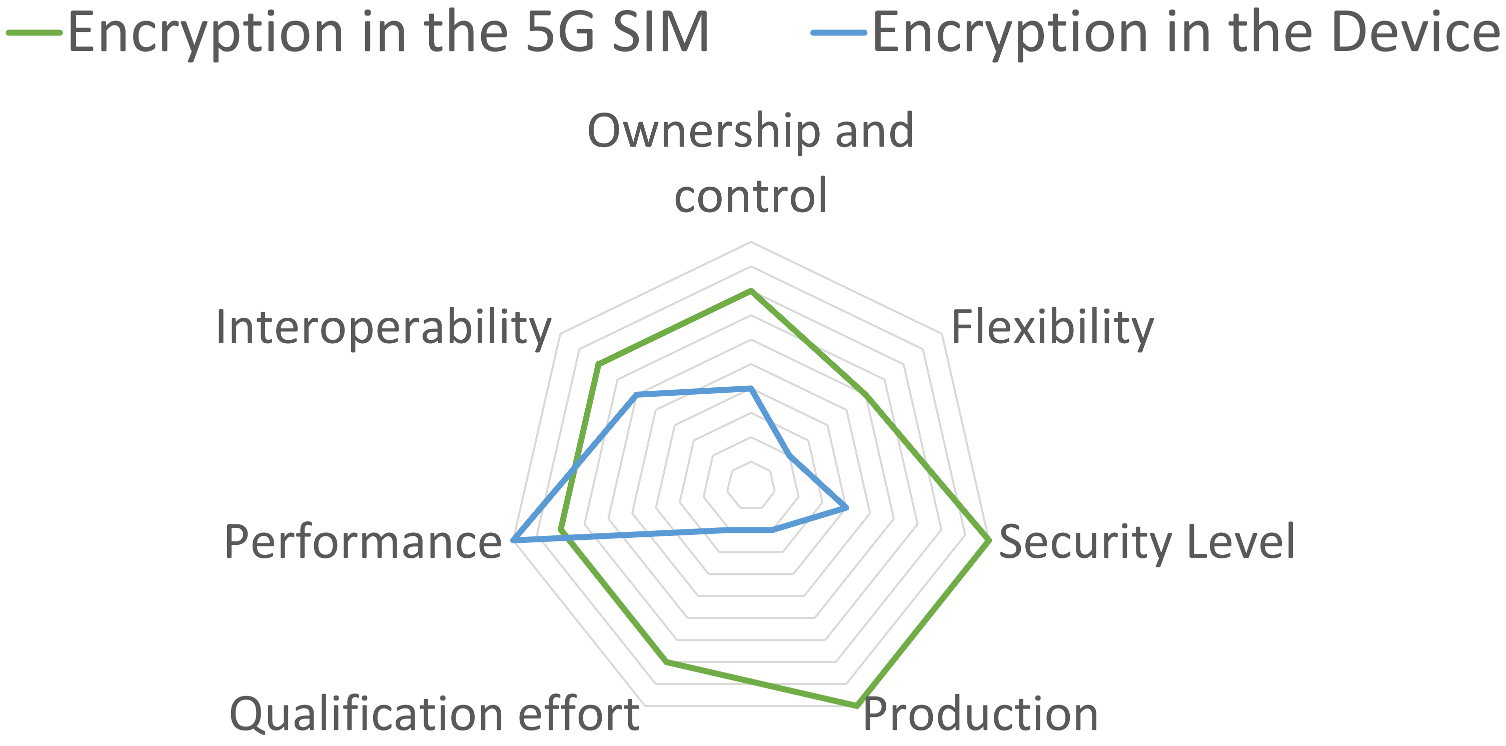
The 5G standards developed by 3GPP introduced the possibility for MNOs to encrypt the IMSI before it is sent over-the-air. However, there is potential for significant variability in terms of implementation

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 which enables IMSI encryption.
- The device executes the cryptographic operations.

Comparing Options for IMSI Encryption

MNOs are recommended to protect privacy by managing IMSI encryption within the 5G SIM, rather than the device



Comparing Options for IMSI Encryption

TRUSTED CONNECTIVITY ALLIANCE

	Encryption in the 5G SIM	Encryption in the Device
Ownership and control	MNO owns and controls IMSI encryption implementation	OEM owns and fully controls implementation
Flexibility	MNO can request the 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

What about Lawful Interception?

There is an important balance to be found between protecting a citizen’s right to privacy, and ensuring that law enforcement agencies can track and monitor criminals when necessary.

- IMSI-encryption prevents unlawful and malicious usage of IMSI catchers.
- Law enforcement agencies will still be able to track and monitor targets with the collaboration of MNOs.

The Case for IMSI Encryption within the 5G SIM

TRUSTED CONNECTIVITY ALLIANCE

- **The privacy implications of sending the IMSI in clear over-the-air are significant** given the vulnerability to well-known attacks from IMSI catchers.

- There is potential for significant variability when implementing IMSI encryption, **creating various scenarios where the IMSI is not protected and consumer privacy is at risk.**

- The recommended way to enforce privacy is to **manage this IMSI encryption within the 5G SIM**, rather than the device.

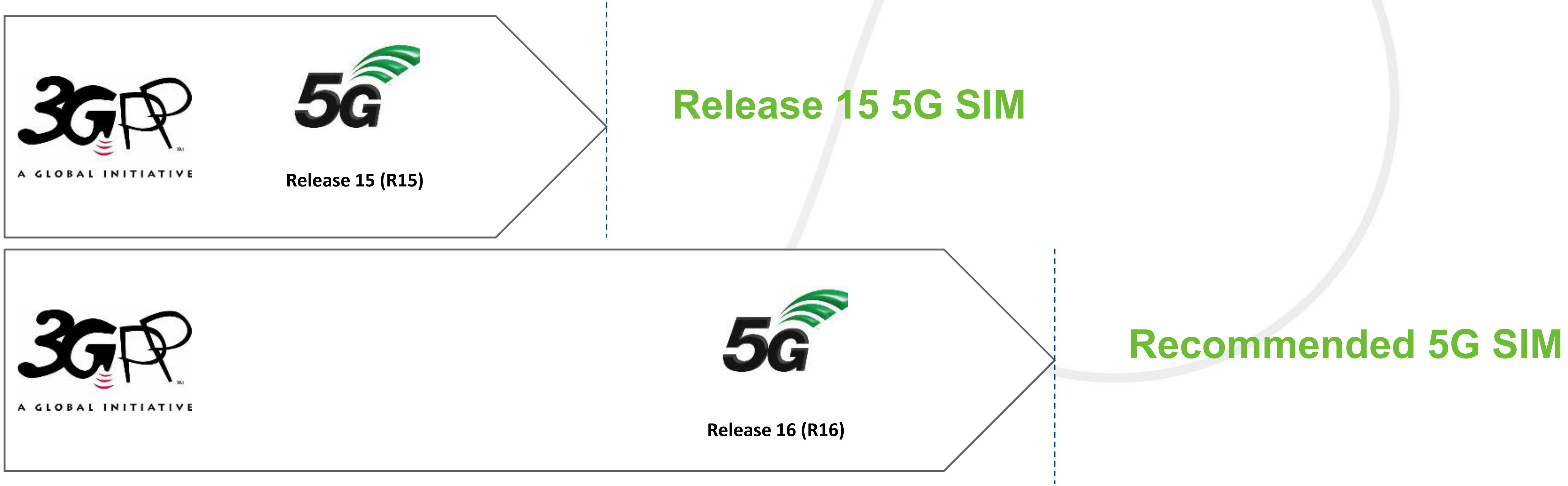
- Governments and other law enforcement agencies will **still be able to utilise lawful interception to track and monitor targets.**

- Beyond mobile handsets, **SIM-based encryption is the only viable way** to establish interoperability across consumer and industrial IoT use-cases.

Enhancing the Recommended 5G SIM

TCA TRUSTED CONNECTIVITY ALLIANCE

- In the same way that network core architecture is evolving, SIM technology is transforming to meet new challenges and opportunities introduced by 5G
- The latest updates respond to powerful new features introduced by 3GPP Release 16 for 5G Phase 2
- The guidance provided in the technical document relates to both 5G Phase 1 (3GPP Release 15) and 5G Phase 2 (3GPP Release 16). The TCA Recommended 5G SIM is fully backwards compatible.



Release 15 (R15)

Release 15 5G SIM

Release 16 (R16)

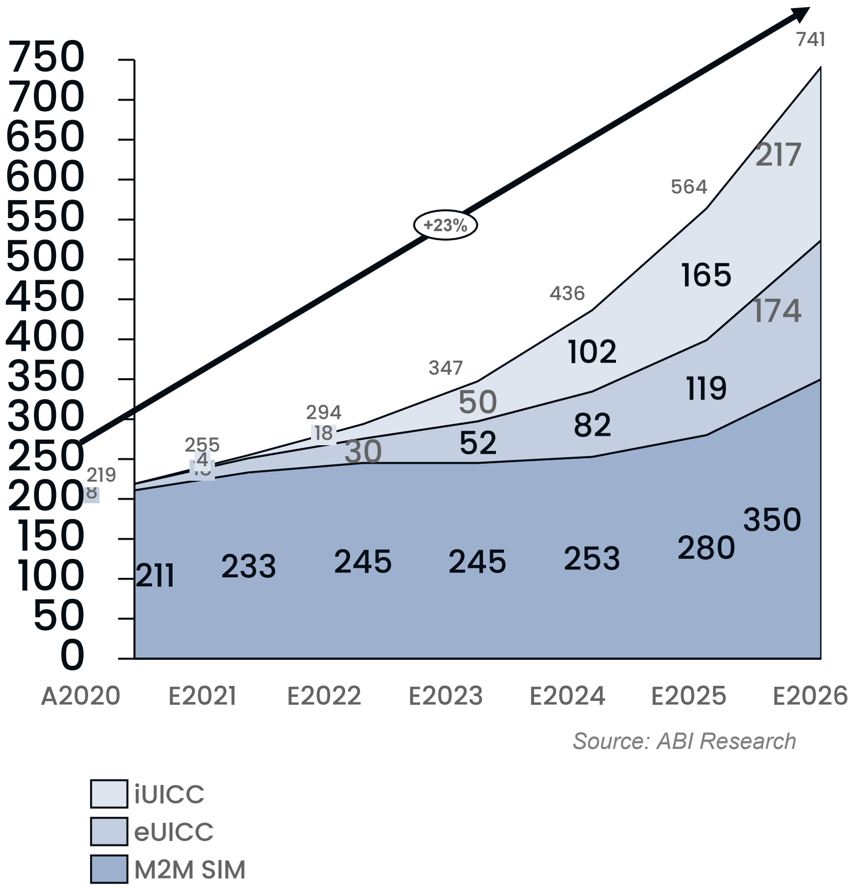
Recommended 5G SIM

Enhanced Recommended 5G SIM – What’s New?

TRUSTED CONNECTIVITY ALLIANCE

1. Enhanced Subscriber Privacy
2. Private Network Access
3. Cellular V2X Communication
4. Improved Mobile Experience

5G SIM – what about the IoT?



Source: ABI Research

There are numerous advantages to leveraging TRE-based SIM products to protect mobile and IoT devices

- An established security platform already present in **billions of devices**
- The ability to protect data at **rest and in transit**
- **Future-proof security** through remote management
- Certification **fast-track**

IoT SAFE – delivering scalability, simplicity and trust

TRUSTED
CONNECTIVITY
ALLIANCE

IoT SAFE

IoT **S**IM **A**pplet **F**or Secure **E**nd-to-End Communication

- IoT SAFE is an **industry partnership** between GSMA and TCA.
- It defines a **standardised way to leverage the SIM and eSIM** to **securely perform** mutual authentication between the IoT device applications and the cloud.
- The result is that IoT device manufacturers can **easily execute security services** and **remotely manage credentials** across billions of devices.

ABI Research Predicts Cellular IoT Devices Will Hit a Global Total of 5.7 Billion by 2026.*

*SOURCE:
https://www.abiresearch.com/press/2026-cellular-iot-devices-will-hit-global-total-57-billion-creating-connectivity-conundrum-carriers/

Unlocking the potential of 5G – what is next?

TCA TRUSTED CONNECTIVITY ALLIANCE

TCA's 5G Working Group is committed to evolving and optimising 5G SIM technology to enhance 5G network services.

✓ The Working Group is now updating the TCA Recommended 5G SIM to respond to the latest updates introduced in 3GPP's Release 17.

TCA will also host a free webinar to provide guidance on the latest updates to TCA's 'Recommended 5G SIM' that will help operators realise benefits and opportunities while unlocking the highest levels of security, privacy and functionality.

Download TCA's technical and educational 5G resources at:
www.trustedconnectivityalliance.org

Learn more and stay up to date

For more information, please contact: **info@trustedconnectivityalliance.org**

Visit our website.

Connect on LinkedIn.

Follow TCA on Twitter.

Sign up to the TCA newsletter.

Learn about becoming a member.