TRUSTED
CONNECTIVITY
ALLIANCE

Protecting Subscriber Privacy in 5G

July 2020

About Trusted Connectivity Alliance

TRUSTED
CONNECTIVITY
ALLIANCE

Enabling a secure, connected future.

- Our members are participants within the SIM ecosystem.
- Our vision is to facilitate the sustained growth of connected objects through trusted connectivity.
- Our members represent over 80% of the global SIM market.
- Our members work collaboratively to identify and deliver collective work requirements, of a technical, strategic and marketing nature.

Our Membership

TRUSTED CONNECTIVITY ALLIANCE

Founding:

THALES

G+D Mobile Security

IDEMIA augmented identity

ST life.augmented

VALID

Executive:

arm

NXP

Full:

CARD CENTRIC SOLUTIONS LTD. CARD CENTRIC

kona i KONA international

Linxens crafting the future of connections

Qualcomm

Watchdata

TIANYU

WORKZ

Ordinary:

COMPRION

Why Trusted Connectivity Alliance?

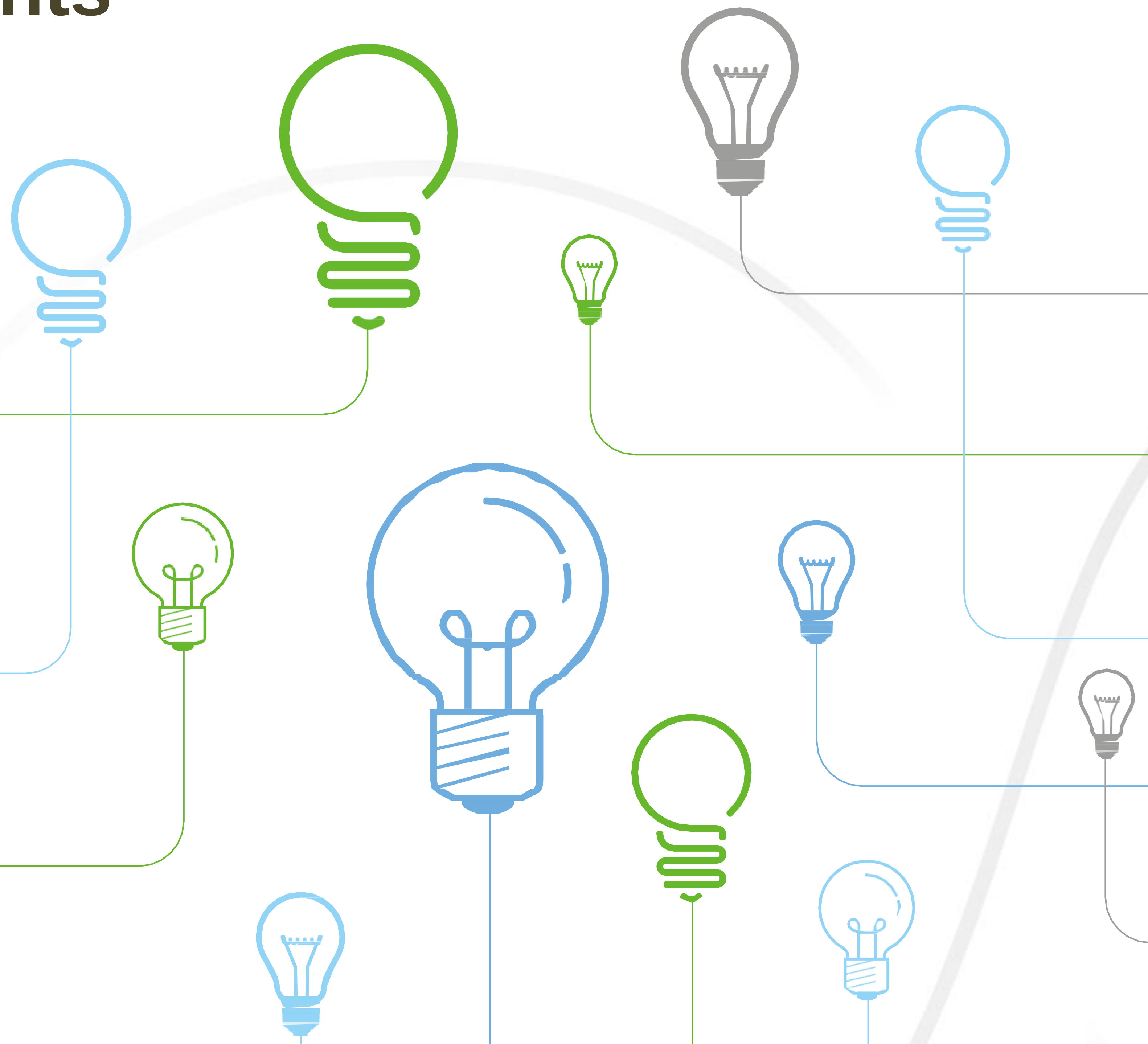
TRUSTED CONNECTIVITY ALLIANCE

SIM technology use cases are expanding rapidly in line with ubiquitous global connectivity.

The number of devices, applications and stakeholders engaging within the SIM ecosystem has broadened in recent years

- Worldwide SIM shipments remain significant.
- New connectivity needs are fuelling demand for additional eSIM solutions.
- The prospect of integrated technologies is now on the horizon.

Key Recent Achievements



IoT SAFE (GSMA collaboration)
Specifies a common API and defines a standardised way for the SIM to be leveraged to securely perform mutual authentication between IoT devices applications and the cloud

eUICC Interoperable Profile Package Technical and Test Specification (GSMA collaboration)
Enables mobile network operators to load standardised, interoperable connectivity profiles in an eSIM, regardless of the SIM vendor.

5G Security
Played a significant role in supporting the maintenance of the hardware SIM in 5G

Open Mobile API (GlobalPlatform collaboration)
Established the first API for Android apps to communicate with the SIM or Secure Element and execute security services

Standardisation support
Including 5G for 3GPP, SSP for ETSI

Annual Shipments Monitoring
The definitive source for global shipments

Helping developers use SIM products
(CAT Loader)

Best practices for developing apps on a Secure Element
(Interoperability Stepping Stones)

Recommended connectivity profiles for each new network release (e.g. LTE)

Dynamic SIM Service: facilitated deployment of MNO services (SAT)

Establishing interop tests and device recommendations for NFC services

Marketplace education

What is an IMSI?

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

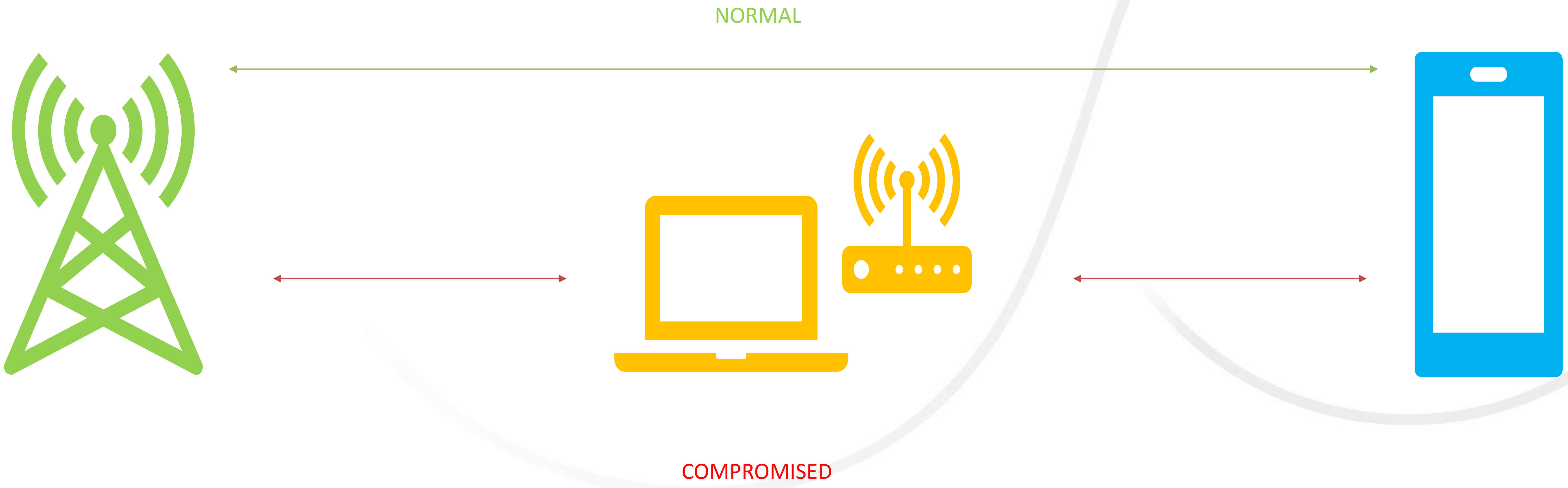
- The IMSI represents the relationship between subscribers and the MNO that issued the SIM card.
- It can be used to confirm a subscriber’s identity and monitor their location, calls and SMS messages.
- The IMSI should be considered ***deeply private information.***

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:

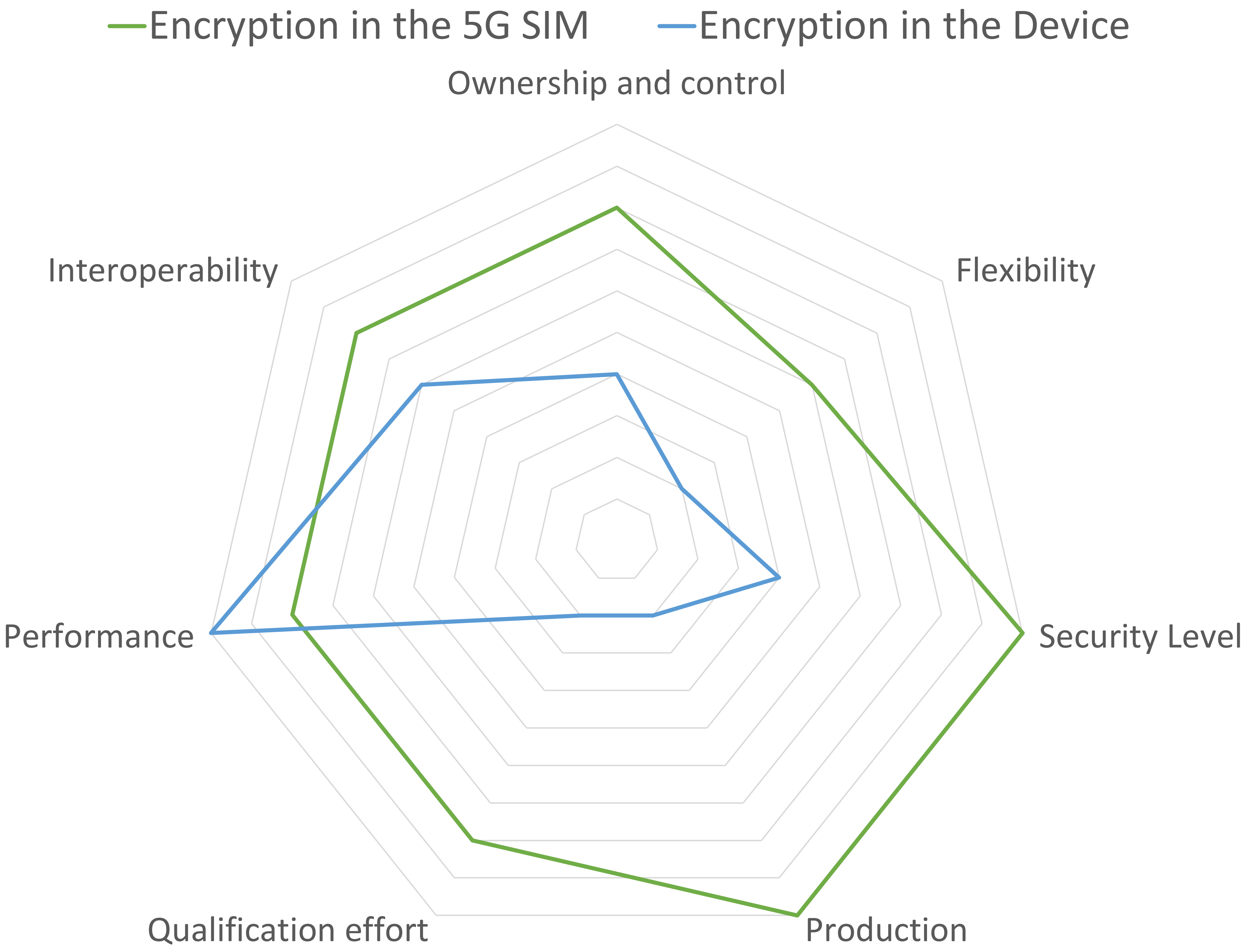
- **The IMSI encryption feature is not activated in the network.**
- **The IMSI encryption feature is activated in the network but end-users with a 5G device do not use a 5G SIM which enables IMSI encryption.**
- **The device executes the cryptographic operations.**

Comparing Options for IMSI Encryption

	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

Comparing Options for IMSI Encryption

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



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.