RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PRV-W01**

Catch Me If You Can: Protecting Mobile Subscriber Privacy in 5G

Jean-Louis Carrara

Trusted Connectivity Alliance / Kigen
Twitter: @_TCAlliance

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

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.
- **MISSION:** To collectively define requirements and provide deliverables of a strategic, technical and marketing nature that enable all stakeholders in our connected society to benefit from the most stringent secure connectivity solutions that leverage our members' expertise in tamper proof end-to-end security.

Specifications and Interoperability	Market Monitoring	Industry Engagement and Strategy	Education

Our Membership

Founding:

Giesecke+Devrient Creating Confidence · IDEMIA · life.augmented · THALES · Valid

Executive:

Kigen · NXP

Full:

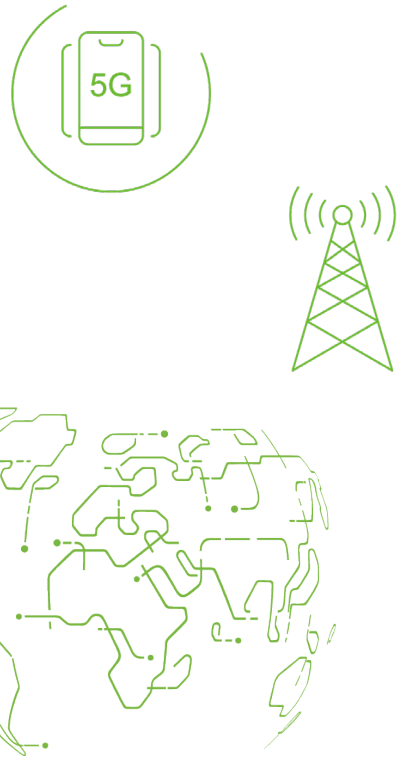
CARD CENTRIC SOLUTIONS LTD. CARD CENTRIC · 东信和平 EASTCOMPEACE · Linxens crafting the future of connections · OASIS smart sim Embed. Connect. Activate · Qualcomm · TIANYU · WORKZ

Ordinary:

COMPRION

Mobile Networks and the Digital Economy

- Mobile networks play an integral role in the digital life of subscribers, and have evolved far beyond enabling voice calling and SMS.
- The advent of 5G will further expand the potential utility for cellular technology.
- **According to GSMA, global 5G connections will reach 2 Billion by 2025.***
- Protecting the most prominent personal data involved in mobile communications must be a critical consideration.



*https://www.gsma.com/newsroom/press-release/mobile-momentum-5g-connections-to-surpass-1-billion-in-2022-says-gsma

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.

CALIFORNIA CONSUMER PRIVACY ACT

GDPR

The Virginia Consumer Data Protection Act (CDPA)

What is an IMSI?

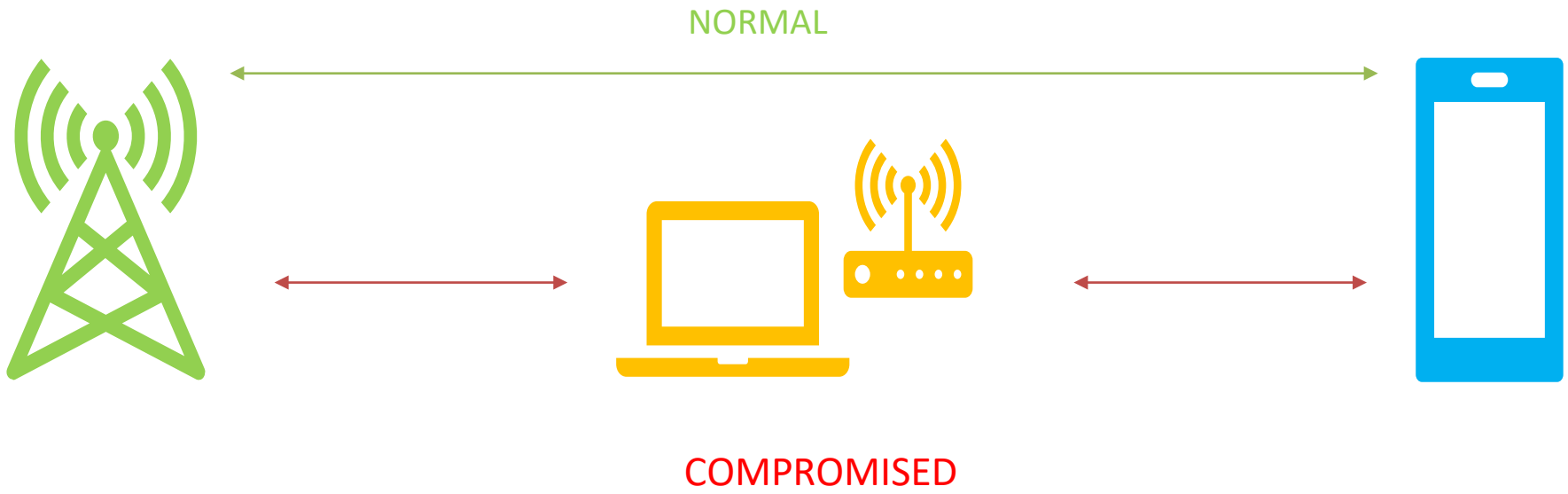
The International Mobile Subscriber Identity (IMSI) is a unique subscriber identifier allocated to the SIM by a Mobile Network Operator (MNO)

- The IMSI 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

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:

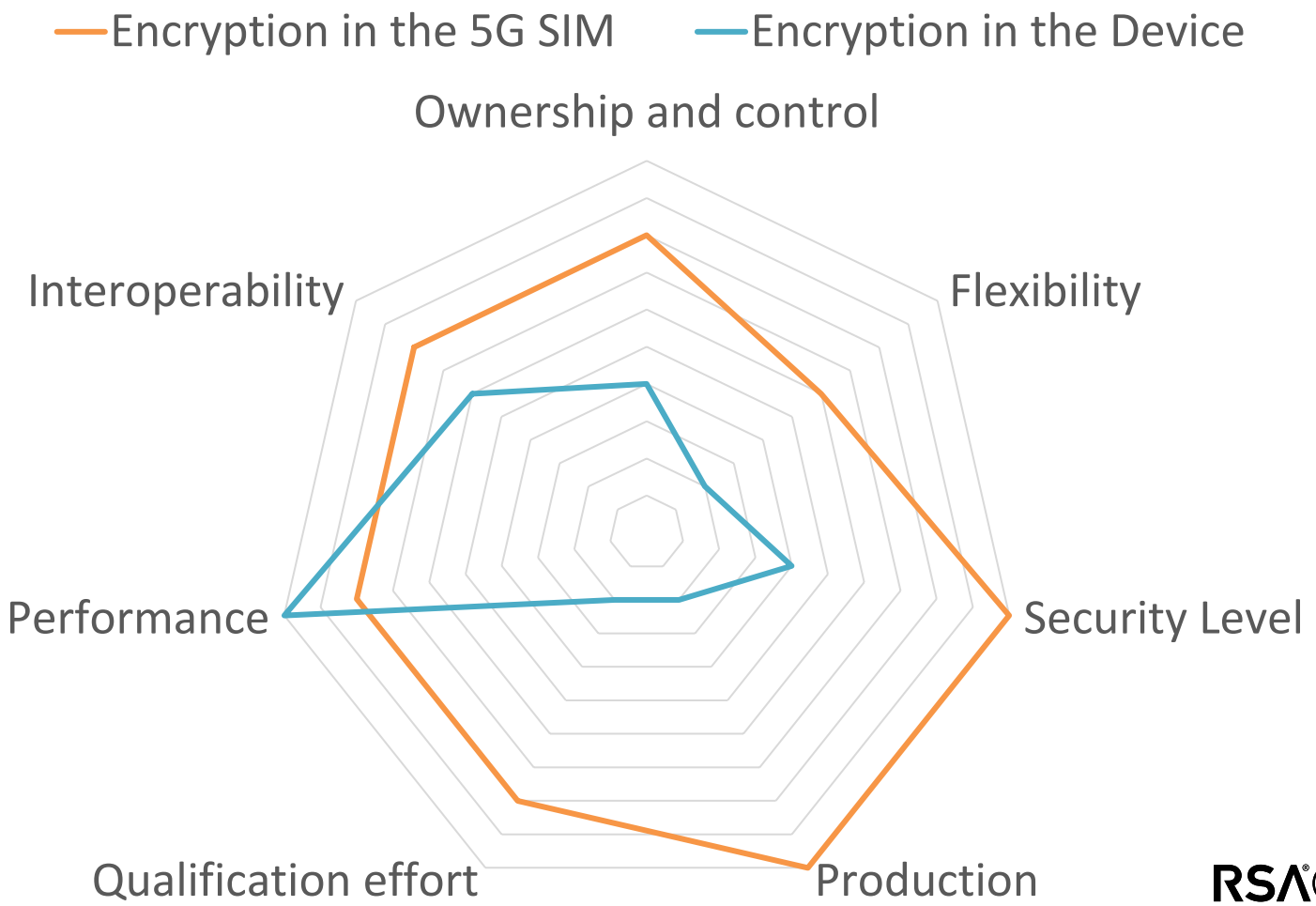
- The IMSI encryption feature is not activated in the network.
- The IMSI encryption feature is activated in the network but end-users with a 5G device do not use a 5G SIM which enables IMSI encryption.
- The device executes the cryptographic operations.

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

- **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.

What is the TCA Recommended 5G SIM?

- The SIM / eSIM is the only platform which can be used to secure 5G network access according to 3GPP – the 5G standardisation body.

- TCA first defined the Recommended 5G SIM in December 2018 to outline which technical features of SIM technology address the challenges MNOs face, beyond network access, when migrating to 5G.

- The technical definition has now been enhanced to align with new use cases introduced by 3GPP's Release 16 Specifications for 5G Phase 2.

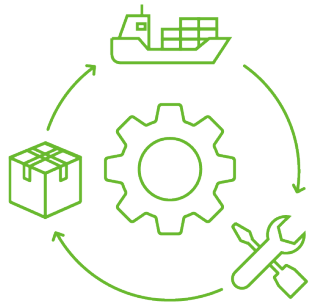
Enhancing the Recommended 5G SIM

- 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.

Enhanced Recommended 5G SIM – What's New?

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

5G SIM Deployments Gather Pace



TCA member data showed substantial increases in 5G SIM shipments in 2021.

This builds on advances made in 2020, which marked the first year of widespread 5G SIM deployments.

The ‘Recommended 5G SIM’ as defined by TCA promotes the highest levels of security, privacy and functionality in 5G networks to maximise operator investments and support 5G use-cases.

Unlocking the potential of 5G

TCA has established a Working Group committed to evolving and optimizing 5G SIM technology to enhance 5G network services.

TCA Recommended 5G SIM: A Definition

TCA's Recommended 5G SIM helps MNOs maximise investments in core 5G network infrastructure by selecting the right choice of SIM technology at 5G launch. This enhanced definition supports new use cases introduced by 3GPP's Release 16 Specifications for 5G Phase 2.

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

TRUSTED CONNECTIVITY ALLIANCE

Learn More and Get Involved

For more information, **all technical and educational resources are available for free download** from the TCA website: www.trustedconnectivityalliance.org

TCA also encourages organisations to actively participate to **help develop, define and influence the future technologies, standards and services that will impact our industries and sectors**. To find out more about joining TCA, contact: info@trusteconnectivityalliance.org

Stay up to date by following TCA:

@_TCAlliance

Trusted Connectivity Alliance

Trusted Connectivity Alliance

TRUSTED CONNECTIVITY ALLIANCE