T-ISAC
Telecommunication
Information Sharing and Analysis Center

T-ISAC 5G Security Evolves Webinar
Questions and Answers
27th May 2021

As I understand in 5G the Network Profile/eSIM no-longer needs to be in a dedicated Secure Element but can be in the SOC or a TEE like environment. How does 5G Network handle this from a security perspective as a dedicated SE is no longer required.

- The principle of the UICC (Universal Integrated Circuit Card) remains valid in the 5G, with its file structure, that is, USIM contents, but the form of the UICC can be also embedded or integrated. In the latter cases, there is a need for remote SIM provisioning method that can be based on GSMA definitions of the Subscription Management (SM-DP+) and accompanying elements to transfer operator SIM profile securely to the embedded or integrated UICC over the air (OTA).
- The GSMA manages the secure accreditation scheme (SAS) for the production of the "traditional" form of the SIM card (UICC), as well as the ones requiring OTA.
- More information on the SAS at: https://www.gsma.com/security/sas-accredited-sites/

How are improvements to minimum supported data rates for UP integrity protection (on radio interface), considering it can (could in rel15) be set so low as to be practically non-effective? There was a liaison statement to SA3 on this, I believe.

- The topic is a rather detailed and would require subject matter expert opinions, e.g., from the 3GPP SA3.
- In general, it is understood that the integrity protection requires resources that not all devices will be able to support at the full data rate. This is why 5G allows means to negotiate lower rates. One of the implications is, as stated as an example, that "...*if the device indicates e.g. 64 kbps as its maximum data rate for integrity protected traffic, then the network only turns on integrity protection for UP connections where the data rates are not expected to exceed the 64-kbps limit*." (Ref. https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview)

Does the terminal need to support extra features for eSIM (i.e. the LDSs etc)?

- The terminal's support for eSIM, as per GSMA, is the same for 5G and previous generations in terms of the functionality. The eSIM-related features, when embedded UICC is utilized and Remote SIM Provisioning (RSP) / Subscription Management (SM) system is deployed, include, e.g., Local Profile Assistant (LPA) which can reside in the device or UICC. There are various scenarios and versions of the SM, the latest Permanent Reference Documents (PRD) describing the options for the consumer as well as M2M environments.

- More information on the eSIM specifications of the GSMA can be found at:
- Overall description and whitepaper: https://www.gsma.com/esim/
- technical and architectural specifications for consumer and M2M devices: https://www.gsma.com/esim/esim-specification/

How will an eSIM / 5G SIM be involved in case a UE authenticates to several network slices at the same time?

- The 3GPP specifications define device's support for up to eight simultaneous network slices. These slices can be isolated as for the security, and network security can be applied creating security policy rules based on network Slice/Service Type (SST).
- The authentication and authorization of each slice is managed by the NSSAAF (Network Slice Specific Authentication and Authorization Function).

Is there best practice or reference documents regarding NFs certificate management in the 5GC HPLMN? (Revocation procedure? How many certificate per NFs? One per API? For example)

- As per the 3GPP TS 33.501, and ETSI TS 133 501, the following is defined: "Subscriber certificates that are used with EAP-TLS typically include static validity times. A certificate revocation list (CRL) as specified in RFC 5280 and online certificate status protocol (OCSP) as specified in RFC 6960 are means for the issuing certificate authority (CA) to revoke the certificates before their scheduled expiration date. In 5G security architecture, the UDM/ARPF is responsible for such subscriber status information. EAP-TLS peers and servers may also support Certificate Status Requests (OCSP stapling) as specified in RFC6066 which allows peers to request the server's copy of the current status of certificates."

How do you see the NWDAF role in the threat detection and mitigation?

- The primary role of the NWDAF (Network Data Analytics Function), as described in the 3GPP TS 29.520, to collect data using standard service-based architecture interfaces. The collection can happen by subscription or request of other network functions. The NWDAF provides analytics functions and reporting in common format.
- The 3GPP TR 23.791 presents various analytics use cases of the NWDAF, based on also AI/ML, including service experience and load performance computation and prediction, devices expected prediction and abnormal behaviour detection including communication pattern prediction, and QoS prediction. Even if the specifications might not mention specifically threat detection, these capabilities of the NWDAF could, in fact, be utilized as an input for detection mechanisms such as a separate Fraud Monitoring System (FMS).

How will roaming and roaming vasbe impacted?

- GSMA Fraud and Security team is considering the roaming security and protection scenarios at the 5GMRR (5G Mobile Roaming Revisited) at present. The scenarios include best practices involving roaming partners such as VAS (Value Added Service) providers and IPX (IP Exchange) providers when 5G SEPP (Secure Edge Protection Proxy) is present. The resulting guidelines will complement the SEPP specifications of the 3GPP by offering practical ways to implement the interconnected environment.

Edge and Slice security? How it should be design and implemented?

- The implementation of the 5G Edge and Network Slice security is a vast topic. The 5G as such has security-by-design model for the 5G infrastructure, including interconnected 5G networks, but there can be also new potential threats that 3GPP has not been able to take into account in designing the 5G security architecture. Thus, it is a good practice to follow up the security vulnerability reports to, e.g., GSMA Coordinated Vulnerability Disclosure (CVD) Programme, Telecommunication Information Sharing and Analysis Center (T-ISAC), and Fraud and Security Group (FASG) activities.
- More information at https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/
- https://www.gsma.com/security/t-isac/
- https://www.gsma.com/aboutus/workinggroups/fraud-security-group

How will 5G accommodate PSD2 SCA requirements for payments transactions?

- More information on this topic, including 'RCS and Payments' whitepaper, can be found at: https://www.gsma.com/futurenetworks/latest-news/is-rcs-set-to-transform-mobile-payments-and-psd2-sca/

With respect to massive MTC, what additional cybersecurity functions have been introduced on the device side, gNB, and SA core?

- The overall 5G security architecture introduces the new model (e.g., enhanced key derivation, extended mutual authentication also for roaming cases, keys for also integrated non-3GPP access, etc.) equally for all the use cases, although the security level of different network slices (e.g., those dedicated for massive MTC) can be varied (level of the isolation).
- The new security architecture and the security features for the network components and device are detailed in the latest version of the 3GPP TS 33.501.

What are the security best practices in 5G?

- GSMA coordinates 5G security-related discussions with the members, e.g., on roaming environment (SEPP), at the Fraud and Security work groups.

- In addition, there are GSMA guidelines for 5G-related topics including security, e.g., at the following resources:

https://www.gsma.com/security/securing-the-5g-era/

https://www.gsma.com/security/5g-cybersecurity-knowledge-base/