5G Security – Use Cases and Best Practices Webinar - November 2021

Q&A with Jyrki Penttinen, Senior Technology Manager, North America, GSMA

#	Questions	Answers
1	Which instance takes care of Security Analytics for 5G?	NWDAF (Network Data Analytics Function) provides slice-specific network data analytics to the Network Functions which are subscribed to it.
2	Source of the certificate management reference architecture for 5GC SBA?	The 3GPP TS 33.310 (Network Domain Security; Authentication Framework, Release 17) presents the certificate concept in 5G. There is also an 3GPP-internal Technical Report TR 33.876 that presents a study on automated certificate management in Service-Based Architecture.
3	How Non-Standalone and Standalone 5G roaming differ from each other?	5G roaming in SA mode refers to the inter-network communications via SEPP elements (for control plane as of Release 15) and IPUPS (user plane as of Release 16). In Non-Standalone mode, the roaming connections depend on whether the core network is of 4G EPC or 5G Core. In case of 4G EPC, the roaming takes place as it is done in 4G environment today, that is, e.g., via IPX or direct connections.
4	Certificate Management ref. architecture.	As stated in [https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture], "The usage of both TLS and OAuth 2.0 in the SBA relies on the use of a Public-Key Infrastructure (PKI) in place in the network. In a PKI, a Certificate Authority (CA) issues certificates to each of the communication endpoints guided by proper (identity) management functions and policies. The public/private key pairs associated with the certificate can then be used for the asymmetric cryptography used in mutual authentication and signing/verifying of tokens that is required for using TLS and OAuth 2.0 as specified in the SBA." Furthermore, "Realizing SBA will be mainly done using a microservice architecture supporting continuous deployment and updates at a fast pace. Combined with the overall use of TLS for connections between the NFs, there is a need for a highly automated process to issue and manage certificates that the NFs must hold securely. There will be little room for manual procedures for certificate issuing that have been used in the past for physically nodes." More information on CA can be found in 3GPP TS 33.310 V17.0.0 (2021-09).

5	Does NSSAA work as kind of 2nd authentication factor?	NSSAA works on top of the 5G authentication procedure; the NSSAA (Nnssaaf_NSSAA) service provides slice-specific authentication and authorization for their respective UE. The role of NSSAAF is to be an NF Service Producer whereas the AMF is the NF Service Consumer. More information on the slice-specific authentication: https://itectec.com/spec/5-services-offered-by-the-nssaaf/.
6	API authentication and authorization will be a key factor in 5G SA Core. Do you recommend implementing a dedicated NF to manage API security?	5G Release 15 introduces Network Exposure Function (NEF). It can provide a platform for creating new services by consolidating APIs and presenting unified access to the API framework for both internal and 3rd party developers. [https://www.nokia.com/networks/products/network-exposure-function/] Furthermore, NEF can provide secure exposure of network services such as voice, data connectivity, and charging, towards 3rd party application over APIs, as well as developer environment and SDK for operator and community. Also, NEF enables end-to-end service creation by combining network assets into application, and an integration layer that connects the application to operator's network. The related API framework can be done via a plug-in concept supporting API-based services and additional APIs as per need. For multi-vendor core networks, NEF can be deployed in such a way that it exposes APIs from other vendors' network functions, by enabling the use of 3rd party plugins. [https://www.nokia.com/networks/products/network-exposure-function/]
7	What is the job of the IPUPS, is it offering GTP-U tunnel validation only?	As stated in GSMA PRD NG.113, "The N9 interface makes use of the GPRS Tunnelling Protocol, GTP version 1 for the User Plane. The UPF's inside the PLMNs making use of the Home-Routed solution architecture is compliant to 3GPP TS 29.281 Release 16 together with the Inter-PLMN User Plane Security (IPUPS) functionality for 5G Roaming User Plane Security." Furthermore: "Operators can deploy either UPFs supporting the IPUPS functionality or the IPUPS as a separate Network Function from the UPF, at the border of their network to protect their network from invalid inter PLMN N9 traffic in home routed roaming scenarios."
8	NWDAF = Network Data Analytics Function	NWDAF (Network Data Analytics Function) provides slice-specific network data analytics to the Network Functions which are subscribed to it.
9	Is the communication between two NF's encrypted, even though this communication is completely internal; does not leave operators 5GC?	Yes. More information at: https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture

10	I wonder if it validates the TEID only or if it has any functions for integrity of the e2e payload as well. Since I think it is quite easy to inject traffic into an ongoing GTP-U tunnel and make UE/devices respond to it. So that was what I wondered when asking.	Release 15 defines mutual authentication and transport security directly between network functions. TLS 1.2 and 1.3, and token-based OAuth 2.0 authorization are used for NF service consumers to access the services offered by NF service producers. The Release 16 introduces security for indirect communication, too. In this model, instead of an NF producer and consumer interacting directly, Service Communication Proxy (SCP) is located in between them. In indirect model, consumers and producers use SCP for service requests and forwarded responses, SCP needing to modify the service requests. In this new model, TSL is still used for the mutual authentication and transport security per hop, but the end-to-end transport security between consumer and producer is no longer possible.