3GPP Non-Public Network Security

Anja Jerichow*, Betsy Covell, Devaki Chandramouli, Ali Rezaki, Atte Lansisalmi and Juergen Merkel

Nokia Bell Labs, Munich, Germany
E-mail: anja.jerichow@nokia.com
**Corresponding Author*

Received 13 November 2019; Accepted 28 November 2019;
Publication 04 January 2020

Abstract

The 3GPP Rel-16 5G System focuses on enabling support for Industrial Internet of Things (IIoT) for Industry 4.0. Building blocks of 5G supporting use cases and requirements from the manufacturing sector are extreme mobile broadband, massive machine-type communication, ultra-reliable critical machine communication, non-public networks, time sensitive communication, 5G LAN communication, precise positioning. While for all of them, security plays an important role, the focus of this paper is on the 3GPP Rel-16 architecture and security concept of 5GS Non-Public Networks. We conclude with insights on the challenges for using 5G in the Operational Technology Industry.

Keywords: Security, verticals, non-public network (NPN), standalone non-public network (SNPN), public network integrated non-public network (PNI-NPN), private networks.

1 Introduction

In support of high-performance and highly efficient systems that can meet customized market needs, the 3GPP 5G System (5GS) has been designed to enable extreme mobile broadband. It also allows millions of machine-type

Journal of ICT, Vol. 8_1, 57–76. *River Publishers*
doi: 10.13052/jicts2245-800X.815

devices to communicate with each other or send information to the network. Finally, critical machine communication is enabled in an ultra-reliable way and with negligible delay.

The 5GS requirements were driven by input from vertical industries and have motivated 3GPP in providing 5GS enhancements to support industrial use cases. The aim is to enable the use of 3GPP 5G technology in Non-Public Networks, also referred to as private networks, for dedicated use cases in industrial automation enabled by Industrial IoT. With these enhancements, 5GS paves the way to "Industry 4.0", as the next era in industrial production with significant improvements to flexibility, versatility, usability and efficiency of future smart factories [7].

In the following, the concept of Non-Public Networks (NPN) is introduced and security specific authentication related features are explained.

2 5GS Non-Public Network Specification References

Note to the reader: The authors assume a general understanding of the 5GS requirements in 3GPP TS 22.261 [3], architecture in 3GPP TS 23.501 [10] and security in 3GPP TS 33.501 [11].

Service requirements for industrial automation use cases are described as part of the general 5GS requirements specification 3GPP TS 22.261 [3] and the cyber-physical control applications in the vertical domains' requirements specification 3GPP TS 22.104 [4]. These stage-1 service requirements in vertical domains have been the foundation of non-public network related stage-2 architecture work.

The key objective of the 3GPP feasibility study on Vertical LAN study 3GPP TR 23.734 [5] was to study architecture enhancements to 5G System which enable the support of new deployment scenarios in order to address the diverse market segments in support for NPNs. The conclusions of this study were then transformed into normative specification text describing architectural enhancements (3GPP TS 23.501 [10]), procedural enhancements (3GPP TS 23.502 [16]) and enhancements to the policy and charging framework (3GPP TS 23.503 [17]) for non-public networks.

Based on these architectural specifications, a security study 3GPP TR 33.819 [6] was conducted on security requirements and solutions for three vertical industry related features: Non-Public Networks, Time Sensitive Communication (TSC) services, and 5G LAN. The outcome of the security study is being specified in three new normative annexes of TS 33.501 [11], with NPN being the focus of this article.

3 Non-Public Network Architecture

Non-Public Networks (NPNs) are intended for the use by a private service provider such as an enterprise. These networks are not open for use by the general public. As specified in [3], NPNs may be deployed in a variety of configurations, utilising both virtual and physical elements. Standard enablers are specified for two main deployment options: Standalone Non-Public Network (SNPN) and Public Network Integrated Non-Public Network (PNI-NPN).

3.1 Standalone Non-Public Network Architecture

A Standalone Non-Public Network (SNPN) is assumed to be operated by an SNPN operator without relying on network functions offered by the PLMN. This applies for licensed New Radio (NR), lightly licensed NR (e.g. NR deployed on top of shared spectrum such as CBRS band), unlicensed NR (NR-U). NG-RAN can be shared by multiple SNPNs. NG-RAN can be shared by one or multiple SNPNs and one or multiple PLMNs.

SNPN is identified by combination of PLMN ID and NID (Network Identifier). The ITU assigned PLMN ID with MCC value 999 can be used by SNPN operator. 3GPP introduced NID on top of PLMN ID to identify SNPN as the PLMN ID value that is used to identify SNPN is not assumed to be globally unique e.g. PLMN ID can also be regionally shared (i.e. country regulator can assign an MNC value which is shared by multiple networks in a single country).

Two assignment models are envisioned for Network identifier (NID):

- Coordinated assignment: NIDs are assigned using one of the following options:
  - The NID is assigned such that it is globally unique independent of the PLMN ID used; or
  - The NID is assigned such that the combination of the NID and the PLMN ID is globally unique.
- Self-assignment: NIDs are chosen individually by SNPNs at deployment time (and may therefore not be unique) but use a different numbering space than the coordinated assignment NIDs.

UE(s) accessing SNPNs can support either IMSI or NSI (Network specific identifier) as Subscription Permanent Identifier (SUPI).

In order to enable UE(s) camp in SNPN, SNPN RAN broadcasts one or more PLMN IDs, and a List of NIDs per PLMN ID to identify the SNPN

(up to a max of 12 NIDs). SNPN RAN can also optionally broadcast human readable network name per NID. Furthermore, SNPN RAN broadcasts indicators to block RACH access to unauthorized UE(s) (i.e. UE(s) with no subscription and no access rights for accessing SNPN). In case of network congestion and overload, SNPN RAN can leverage unified access control and broadcast barring control information associated with access categories and access identities to prevent access to SNPNs for authorized UE(s).

An SNPN enabled UE supports reading broadcast information and it supports SNPN access mode. It is configured with the necessary credential for SNPN. When the SNPN enabled UE is set to SNPN access mode, it does not perform normal PLMN selection using PLMN ID. Rather it performs network selection using PLMN ID and NID. There are two modes of network selection – automatic network selection and manual network selection – as illustrated in Figure 1.

When a UE performs Initial Registration to an SNPN, the UE indicates the selected NID and the corresponding PLMN ID to NG-RAN. NG-RAN

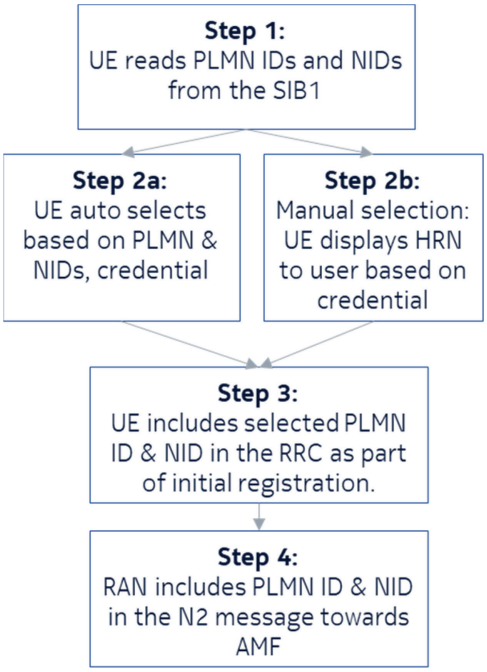

Figure 1 Illustration of automatic and manual SNPN selection by UE.

informs the AMF of the selected PLMN ID and NID and the AMF accepts the initial registration if the UE is authorized and can be authenticated.

3.2 Public Network Integrated Non-Public Network

A Public Network integrated Non-Public Network (PNI-NPN) is deployed with the support of a PLMN. It is supported using network slices or Closed Access Group (CAG) cells or a combination of both. The PLMN ID identifies the network and the CAG ID identifies the CAG cells. Network selection and reselection is performed based on PLMN ID. Cell selection and reselection, and access control are done based on the CAG ID.

In more detail, a CAG identifies a group of subscribers who are permitted to access one or more CAG cells associated to the CAG. The CAG concept is used for PNI-NPNs to prevent UE(s), which are not allowed to access an NPN, from automatically selecting and accessing the associated cell(s). I.e. it is used for authorization at network/cell selection independent from network slice selection, where a CAG cell broadcasts one or multiple CAG Identifiers per PLMN. The CAG cell broadcasts information such that only UEs supporting CAG are accessing the cell. This is not possible with network slicing unless an operator specific barring is used.

Network slices are network instances for individual customers using the same infrastructure to be dynamically shared by different tenants. They are composed of capabilities from multiple network segments from the access to the core, as well as applications.

3.3 Security View on Deployment Scenarios

The NPN deployment options aligning with the capabilities provided by the 3GPP standard are visualized by 5G Alliance of Connected Industries and Automation (5G-ACIA) in Figure 2. They are based on work in 3GPP studies, e.g., TR 22.804 [1], TR 22.830 [2], where these use cases elaborated relevant scenarios, provided rationales for the deployment options, and explored new requirements for the 5GS. Security, both in terms of enterprise data and access to NPNs, was a key concern identified in these studies.

The term Isolated NPN is synonym for SNPN as used by 3GPP. For PNI-NPNs, i.e., where NPN is deployed in conjunction with a public network, three different non-standalone deployment scenarios are mentioned in the 5G-ACIA White Paper [9]. The scenarios vary depending on the degree of interaction and infrastructure sharing with the public network as showing

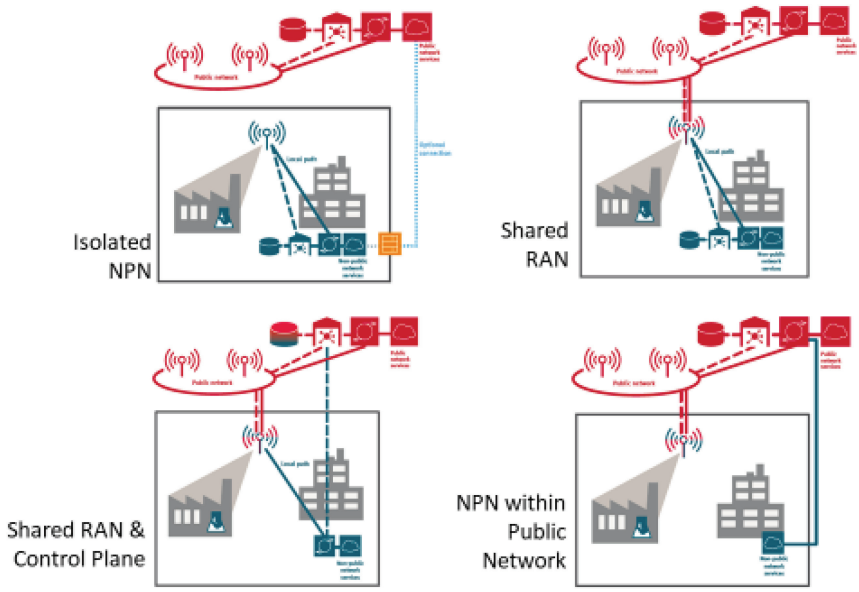

Figure 2 Isolated and non-standalone NPN deployment options [9].

the different usage of the NPN architecture concepts with either only shared RAN, shared RAN and control plane, or the NPN fully integrated in a PLMN.

Due to the situation that in industrial scenarios the users are accustomed to working in a closed domain, with physical as well as cyber security, security measures need to be in place for NPNs to protect procedures, equipment, and data in factory scenarios. Introducing 5GS, with its potential for access beyond the factory walls, creates a need for additional privacy and integrity protection measures to ensure that no unauthorized access to the enterprise system is allowed.

The completely standalone NPN is one mechanism to provide this security, but there are many use cases when some access to a PLMN is needed or even desired as addressed by the various PNI-NPN configurations. Thus, new rules for network selection are needed to provide security from unauthorized access as well as new requirements for third parties (i.e., the enterprises in the vertical domain), which demand alternative authentication methods, end to end encryption, and integrity protection. Further, it must be possible to restrict UEs to accessing only the NPN even though PLMN coverage is available in the same geographic area while other enterprise UEs may be enabled to access both the NPN and PLMN. Only this way, it is ensured that

unauthorized UEs and even the PLMN operator will not have access to the enterprise data.

These requirements are rather challenging since they change prior 3GPP system behaviour, which allowed a UE to attempt network access and then be rejected based on, for example, failing authentication, or to access an otherwise unauthorized network for emergency services, albeit in a limited service state. However, 3GPP addresses these challenges by the usage of slice specific access (NSSAI) identifier, network specific identifier (NSI) and the CAG concept as well as the authentication methods as described in the following.

4 5GS Authentication Methods in Rel-15

The purpose of the authentication and key agreement procedure as specified in [11] is to enable mutual authentication between the UE and the network. Keying material is provided to the serving network (the so-cold serving network anchor function (SEAF) key) and is used between the UE and the serving network to create dedicated keys for the subsequent security procedures.

There are several 5GS improvements over LTE related to authentication, which are summarized below for the convenience of the reader and independent of the usage for NPNs.

- Access security is managed in a unified manner, for which the network function AUSF (Authentication Server Function) is introduced in the home network.
- There is no access type limitation over 3GPP access or non-3GPP access. Unlike LTE, operators do not need to deploy specific authentication infrastructures.
- Authentication methods mandatory to support by a PLMN in Rel-15 are 5G-AKA and EAP AKA′. EAP-TLS is optionally defined. Any method can be used to authenticate the UE over both access types.
- The home network gets confirmation if the UE was successfully authenticated in the serving network.
- There is a binding of the serving network ID into the authentication request in order to prevent fraud, e.g. a serving network attempting to register a UE that is not present in the visited network.
- Privacy of the UE identity is preserved by registering to the serving network with a subscription concealed identifier (SUCI), a one-time useable identifier created from the subscription identifier (SUPI).

The authentication methods 5G AKA and EAP-AKA′ are based on authentication vector generation by the home network in an ad-hoc fashion, i.e., only when requested from a serving network to authenticate a UE that wishes to access the serving network. After UE and serving network finalized the authentication process, the home network receives an authentication confirmation and, in case of successful authentication, provides to the serving network the security anchor key for generating further key material between the UE and the serving network. During the authentication process the serving network sends a challenge to the UE, which the UE needs to respond to. If the response by the UE is equal to an expected response provided earlier by the home network to the serving network, the serving network will allow the UE to access its network.

Based on the serving network anchor key (SEAF key) provided by the home network to the serving network and equally generated by the UE after successful authentication, the UE and the serving network will generate dedicated keys for the confidentiality protection and encryption of NAS and AS communication between UE and MME as well as UE and gNB respectively.

5 Security Requirements for NPNs in Rel-16

A high level of 5G security and privacy is essential for critical communication as described in 3GPP TS 22.261 [3]. 5G security addresses these need while continuing to provide security consistent with 3GPP systems based on earlier releases. This has resulted in a set of requirements:

- The 5G system shall support operator controlled alternative authentication methods with different types of credentials for network access for IoT devices in isolated deployment scenarios (e.g., for industrial automation).
- 5GS shall also support, in non-public networks, operator-controlled alternative authentication methods with non-3GPP identities and credentials for UE network access authentication.
- The 5G system shall support a suitable framework (e.g., EAP) allowing alternative authentication methods with non-3GPP identities and credentials to be used for UE network access authentication in standalone non-public networks.

Thus, in simple words, 5GS is opening up to allow access to devices that might not have a USIM application, where the pre-agreed shared secret between UE and home operator would usually be stored in the UE.

6 NPN Authentication

6.1 EAP Authentication Framework

3GPP TS 33.501 [11] Rel-15 utilizes the EAP authentication framework (see [11], clause 6) as specified in RFC 5247 [12]. This is generalised in Rel-16 for SNPN usage in the newly introduced normative Annex I [11]. The framework has become the baseline for SNPN scenarios for SNPN operators that may want to support alternatives to the 5G AKA method.

In the EAP authentication framework there are 3 roles: the EAP server, the peer, and the authenticator. The EAP server is the entity that terminates the EAP authentication method with the peer. The peer is the end of the link that responds to the authenticator. The authenticator is the end of the link initiating the EAP authentication.

Mapping this to the 5GS architecture, the back-end authentication server AUSF in the home operator network acts as the EAP server, the UE takes the role of the peer, and the SEAF, being a functionality of the AMF in the serving network, takes the role of a pass-through authenticator.

6.2 Supported Authentication Methods in PNI-NPNs and SNPNs

When 5G AKA is not the preferred authentication method, the EAP authentication framework is used instead, which supports in general a variety of authentication methods. 5GS has restricted the usage to key-generating EAP authentication methods.

5GS Rel-16 distinguishes NPN authentication in SNPN and PNI-NPN authentication as follows:

- For PNI-NPNs, the authentication methods 5G AKA and EAP-AKA′ are mandatory to support and other EAP key-generating authentication methods can optionally be used.
- For SNPNs 5G AKA or EAP key-generating authentication methods are optional to support.

Main difference between PNI-NPN and SNPN deployments is that for a PLMN deployment the support for AKA methods is mandatory in the UE and network. However, for an SNPN, it is optional to support 5G AKA or EAP-AKA′. In general, there is no mandatory authentication method for UE(s) in SNPNs.

Thus, if supported, SNPNs may use 3GPP authentication methods, identities and USIM credentials for a UE to access the network, but the widening

of the requirements to allow alternative authentication methods enables an SNPN operator to utilize other EAP authentication methods than EAP-AKA′, e.g., when NPN operators want to use their own devices (not having a USIM application) while having the same high level of security due to utilising the EAP authentication framework. An example for this is the usage of EAP-TLS, which 3GPP Rel-15 already introduced as an alternative authentication method by an informative clause (TS 33.501 [11, Annex B]). With Rel-16 study on Vertical LAN [6] this concept was generalized such that different types of credentials for network access could be used, e.g., for IoT devices in isolated deployment scenarios.

6.3 Authentication Framework and Key Hierarchy

SNPNs support using the EAP authentication framework. It is worth noting that even though the support of key-generating EAP authentication methods is specified, the choice and implementation has been kept out of scope in 3GPP Rel-16. It also needs to be mentioned, that 3GPP TS 33.501 [11] only details the selection procedure for 5G AKA and EAP-AKA′, other NPN operator deployment-specific authentication methods are not detailed.

When an EAP authentication method other than EAP-AKA′ is selected, the chosen method determines the credentials needed in the UE and network. These credentials, called the EAP-method credentials, are used for authentication. 3GPP Rel-16 does also not specify how the credentials for EAP methods other than EAP-AKA′ are stored and processed within the UE, thereby removing the requirement for SIM-based storage and processing and allowing other implementation options.

For any key-generating EAP-method other than EAP-AKA′, the Rel-15 key hierarchy [11, clause 6] needs to be adapted, starting with EAP method-specific credentials from which an Extended Master Session Key (EMSK) is calculated, as illustrated in Figure 3. EMSK is shared between peer and server, i.e. UE and AUSF, and shall not be exposed to any other entity. It is used for the mutual authentication between both.

Important from 3GPP point of view is that the EAP authentication method selected must result in an EMSK. K_{AUSF} is then derived from this specific EMSK, respectively. The rest of the 5GS key hierarchy below K_{AUSF} (see clause 6.2.1 and 6.2.2 in 3GPP TS 33.501 [11]) applies as specified for the AKA-based methods 5G AKA or EAP-AKA′.

The serving network identifier (SN Id) is used within the key derivation process as an input parameter to allow verification by the home network

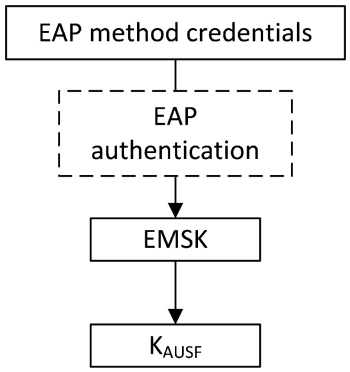

Figure 3 K_{AUSF} derivation for key-generating EAP authentication methods other than EAP-AKA′ (see clause I.2.3-1 of [11]).

operator of the serving network which is requesting authentication of a UE. While in PLMNs, the SN Id contains the PLMN Id only, SNPNs use in addition the Network Identifier (NID) for the identification of their private network. Thus, for SNPNs, the SN Id needs to include NID and PLMN ID into the key derivation, i.e. when deriving the anchor key K_{SEAF}.

7 NPN Privacy

7.1 General

5GS provides enhanced user privacy by also protecting the SUbscription Permanent Identifier (SUPI) over the air using a privacy preserving identifier that contains the concealed SUPI, called SUCI (SUbscription Concealed Identifier). The SUCI is a one-time identifier. It is required that SUCI does not allow correlation with a temporary identity assigned to a UE after successful authentication.

In comparison with LTE, where the SUPI equivalent identifier, the International Mobile Subscription Identifier (IMSI), was still sent in the clear in EPS [12] during initial registration of the UE with the serving network and used paging, in 5GS SUPI is never exposed in clear over the air.

The SUCI is generated by the UE using a protection scheme with a raw public key, i.e. the Home Network Public Key, that was securely provisioned to its subscribers in control of the home network operator. The protection schemes are specified in Annex C of [11], but also proprietary schemes by a mobile operator are possible. The operator holds a Home Network

Public/Private Key pair, the private key never leaving the home operator's secured environment.

Subscription identifier privacy over the air also applies to NPNs: the UE conceals the SUPI with the Home Network Public Key of the operator, to whom the subscription belongs to, and then sends the SUCI in the initial registration message. During the registration procedure, SUCI is converted to SUPI by the home network Subscription Identifier De-concealing Function (SIDF) using the private key. With SUPI the user's subscription is then located, the authentication method selected, and the UE can be authenticated. Upon successful authentication, a 5G-Globally Unique Temporary Identifier (5G-GUTI) is allocated for the UE. To preserve the privacy of the user, the 5G-GUTI is frequently reallocated. It is also essential for the network to reallocate 5G-GUTI whenever parts of the 5G-GUTI (i.e. S-TMSI) are exposed in the clear over the air. Furthermore, in 5GS the SUPI cannot be used to page the UE and this is also to protect the privacy of the UE.

When using 5G AKA or EAP-AKA′, 5GS currently mandates that the USIM holds the Home Public Network Key and the indication of which encryption scheme to apply for SUPI concealment. Due to regulatory requirements or operator configuration the privacy feature may be disabled, in which case the creation of the SUCI format will be done with the so-called null-scheme, a format-preserving scheme, which however includes the SUPI in clear.

7.2 SNPN Privacy Consideration

As explained in the clause above, Rel-15 mandates that the privacy feature involves the USIM. If the Home Network Public Key is not available in the USIM, in Rel-15 the ME (mobile equipment) can only do the calculation of the SUCI using the so-called null-scheme, which means no privacy protection.

However, the usage of EAP TLS does not imply the need of a USIM, since no long-term key needs to be shared in advance and certificates may also be stored outside the USIM. Instead, the extended master session key to build up the communication tunnel between UE and network is generated on the fly. Privacy can therefore be provided if SUPI is using the NAI (Network Access Identifier) for UE identification. (A SUPI is either an IMSI or a NAI).

The NAI is a network-specific identifier that takes the form as specified in RFC 7542 [18] and follows the format rules defined in TS 23.003 [19]. To provide privacy in NPNs, only the realm (i.e. the part identifying the

network, but not the subscriber) part from NAI is included in SUCI analogous to using the anonymous identifier in EAP (see RFC 4282 [14] for details). 3GPP TS 33.501 [11] provides, in an informative manner, privacy considerations for EAP TLS. Similarly, those should be taken into account for any other EAP authentication method used for SNPNs or potentially in releases beyond Rel-16 for PNI-NPNs.

8 Accessing PLMN Services Via SNPN RAN and Vice Versa

When the user has credentials and subscription to access both PLMN and SNPN independently, there may be situations when the UE needs to access PLMN services while camping in SNPN RAN and vice versa. Some example situations why a user might want to access PLMN services via SNPN RAN include the following: lack of certain PLMN services support in the SNPN, lack of indoor coverage, remote location without coverage.

In order for the UE to obtain PLMN services while camping in SNPN RAN, UE can leverage the IP connectivity offered by the SNPN to establish an IPsec tunnel to public network. Then the UE registers with the PLMN using the credentials to access the PLMN and obtain access to corresponding PLMN services. If the UE moves from SNPN RAN to PLMN RAN, the IP address is preserved thus service continuity is enabled for UE mobility from SNPN to PLMN with no need for any service level agreement between PLMN and SNPN.

Similarly, while camping in PLMN RAN, UE can leverage the IP connectivity offered by PLMN to establish an IPsec tunnel to SNPN. Then the UE registers with the SNPN using the credentials to access SNPN and obtain access to corresponding SNPN services. Also, if the UE moves from PLMN RAN to SNPN RAN, service continuity is enabled as the IP address is preserved with no need for any service level agreement between PLMN and SNPN.

It is assumed that there is no service level agreement between PLMN and SNPN. The SNPN is considered as untrusted network by the PLMN and the PLMN is considered as untrusted network by the SNPN. Thus, there is no support for seamless mobility between PLMN and SNPN. In other words, when the UE moves from PLMN RAN to SNPN RAN, handover at the radio network is not supported (as there is no Xn interface assumed between RAN nodes), context transfer is not performed (i.e. no N14 interface between AMFs) thus full authentication is necessary in the target network.

From a security point of view the procedures for authentication for untrusted non-3GPP access (Rel-15) are used as specified in clause 7.2.1 of [11].

9 Summary with Remarks on Security for OT Industries

This paper provided an overview on Public-Network Integrated NPNs and Standalone NPNs. The main focus was set on summarizing requirements, architecture and authentication considering the opening up for alternative authentication methods, potentially without the need of USIM in the UE.

While 3GPP is focusing at the technical solutions, we would like to elaborate in the following clauses on the security need for the OT industries and challenges faced as well as to mention related standards-relevant activities.

9.1 Security Risks in OT Industry

Security measures need to be commensurate with security risks faced. Public mobile networks have a relatively well-understood threat model and established security measures and trust relationships to counter these threats. 5G carries forward and improves on these security mechanisms. However, many of the 5G security concepts are relatively new to Operational Technology (OT) i.e. Industrial Automation companies, and their adoption in OT environments may require careful consideration of the diverse requirements of OT deployments and use cases, as presented in [15].

PLMN deployment characteristics can generally be considered relatively uniform as compared to possible NPN variants in different vertical deployments. This uniformity served as one of the success factors in the effective development and wide adoption of 3GPP specifications. Industry verticals do not have such uniform characteristics. OT use cases may have varying risk profiles and operational constraints in deploying 5G security measures and they may also have additional specific needs of their own.

A general expectation is that OT industries expect usability, flexibility and configurability from 5G security. When adopting 5G technologies by OT it might not be realistic to expect the OT industry to change their operation models and processes quickly due to their existing deployments and the long-life cycles associated with those. OT are “brown field” meaning that when introducing 5GS into an existing industrial or enterprise deployment it must be able to interwork effectively with the existing infrastructure and technology.

9.2 Trust and Threat Models

In comparison to telecom operators, each operator of a private OT network has a different background and is likely to have very different trust assumptions and threat models with varying degrees of isolation and a multitude of end point types and owners.

A public network under the control of an operator has uniform subscriber management functions with a hardware root-of-trust such as a USIM or eSIM being a fundamental component of a PLMN. However, USIM or eSIM is rarely used in an industrial network with perimeter protection. Its introduction to the NPNs would need to match the risk profile of organizations and their operational processes and capabilities. Some OT operators might want to opt for alternate roots-of-trust or completely different authentication and credential storage methods, according to their risk profiles and operational constraints. Imagine thousands of IIoT devices being managed by the often-limited team and other resources of a private OT operator.

9.3 Further Challenges for OT Industry

Apart from the different risks and associated trust and threat models, challenges in NPNs can be seen in the definition and management of the relationship with PLMNs.

OT deployments are often isolated and include a single, perimeter-fenced trust domain. Allowing a telecom operator into this trust domain might require some getting used to, along with some additional technology measures. While it is an option to use higher level encryption functions, its impact on performance, productivity and in-line operations need to be considered. Network slicing could be used in numerous isolation scenarios to improve trust. Effective slice security mechanisms that would meet the needs of OT industry, such as autonomous management of keys, and co-existence with flexible hardware roots of trust could provide the much-needed enhancements.

9.4 5G-ACIA Versus 3GPP

The 5G Alliance for Connected Industries and Automation (5G-ACIA, [7]) was established in 2018 to serve as the central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain [8]. Discussions on OT security requirements from 5G are ongoing, looking at different use cases and different NPN options and taking a risk-based approach to security.

Discussions at 5G-ACIA reveal a very fundamental truth that telecommunications have been the core business of the standards developers at 3GPP. The telco industry knows the PLMN requirements first hand and 3GPP develops solutions accordingly. Industrial vertical topics have not been the core business of telco operators so far and telecommunications is not the core business of the OT industry vendors and operators. Therefore, there was a gap observed in the representation of OT requirements in 3GPP, not just in security but also generally, which is currently tackled by joint effort.

9.5 Outlook

The non-uniform characteristics of Industry verticals needs to be taken into account when further developing solutions by 3GPP since OT use cases have varying risk profiles and operational constraints in deploying 5G security measures. Both 3GPP and 5G-ACIA are working to bring these two worlds together by collecting requirements from verticals and providing 5G solutions that are feasible and scalable for use in the OT domain.

Abbreviations

3GPP	3rd Generation Partnership Project
5G	5^{th} Generation
5G-ACIA	5G Alliance of Connected Industries and Automation
5G-GUTI	5G-Globally Unique Temporary Identifier
5GAA	5G Automotive Alliance
5GS	5G System
5G LAN	5G Local Area Network
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
AS	Access Stratum
CAG	Closed Access Group
CBRS	Citizens Broadband Radio Service
EAP	Extensible Authentication Protocol
HRN	Home Routing Number
ID	Identifier
IMSI	International Mobile Subscriber Identity
ITU	International Telecommunication Union
MCC	Mobile Country Code

ME	Mobile Equipment
MNC	Mobile Network Code
NAS	Non-Access Stratum
NG-RAN	Next Generation RAN
NID	Network Identifier
NPN	Non-Public Network
NR	New Radio
NR-U	NR unlicensed
NSI	Network specific identifier
NSSAI	Network Slice Selection Assistance Information
OT	Operational Technology
PLMN	Public Land Mobile Network
PNI-NPN	Public Network integrated NPN
RAN	Radio Access Network
RACH	Random Access Channel
RRC	Radio Resource Control
SEAF	Security Anchor Function
SIDF	Subscription Identifier De-concealing Function
SNPN	Standalone NPN
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TSC	Time Sensitive Communication
UE	User Equipment

References

[1] 3GPP TR 22.804: “Study on Communication for Automation in Vertical domains (CAV)”.
[2] 3GPP TR 22.830: “Study on Business Role Models for Network Slicing”.
[3] 3GPP TS 22.261: “Service requirements for the 5G system; Stage 1”.
[4] 3GPP TS 22.104: “Service requirements for cyber-physical control applications in vertical domains”.
[5] 3GPP TR 23.734: “Study on enhancement of 5G System (5GS) for vertical and Local Area Network (LAN) services”.
[6] 3GPP TR 33.819: “Study on security enhancements of 5GS for vertical and Local Area Network (LAN) services”.
[7] 5G-ACIA, The 5G Alliance for Connected Industries and Automation, https://www.5g-acia.org/.

[8] 5G-ACIA Whitepaper "5G for Connected Industries and Automation", https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/Whitepaper_5G_for_Connected_Industries_and_Automation/WP_5G_for_Connected_Industries_and_Automation_Download_19.03.19.pdf, March 2019.
[9] 5G-ACIA Whitepaper "5G Non-Public Networks for Industrial Scenarios", https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/WP_5G_NPN_2019_01.pdf, July 2019.
[10] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".
[11] 3GPP TS 33.501: "Security architecture and procedures for 5G system".
[12] RFC 5247: "Extensible Authentication Protocol (EAP) Key Management Framework" in https://tools.ietf.org/html/rfc5247
[13] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
[14] RFC 4282: "The Network Access Identifier" in https://tools.ietf.org/html/rfc4282.
[15] ETSI security week 17–21 June 2019: "5G Security Challenges for Verticals – a Standards View"; A. Rezaki & A. Jerichow.
[16] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".
[17] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".
[18] RFC 7542: "The Network Access Identifier", in https://tools.ietf.org/html/rfc7542.
[19] 3GPP TS 23.003: "Numbering, addressing and identification".

Biographies

Anja Jerichow leads the Converged 5G Security project within Nokia and drives the vertical security work item in 3GPP SA3 among her other responsibilities as security expert in 3GPP and GSMA. **Betsy Covell** leads the Converged 5G System Architecture and New Core project and has been driving the vertical work item in 3GPP SA1 together with **Juergen Merkel**, who is also highly involved in related vertical standardization activities such as 5G-ACIA and 5GAA. **Atte Lansisalmi** is deputy chair of WG3 "Architecture and Technology" in 5G-ACIA and formed the Industrial IIoT Standardization Strategy within Nokia. **Ali Rezaki** is Head of Security Standardization Nokia team and drives the work item "Security Aspects of 5G for Connected Industries and Automation" in 5G-ACIA. **Devaki Chandramouli** is Head

of the North American Standardization Nokia team and leading 5G System Architecture specification in 3GPP SA2.

All of the authors are senior experts and part of the Nokia Bell Labs CTO Industry Standardization Group. They represent Nokia as delegates in 3GPP as well as 5G-ACIA and drive in both groups the Industry 4.0 related work in their respective domains of expertise. Further biographic details are available at https://www.linkedin.com.