5G OPERA

5G-OPERA Deliverable 3.4

Definition of Requirements for Open Core Solutions

Document Properties	
Nom du projet :	5G-OPERA
Titre du document :	Definition of Requirements for Open Core Solutions
Donneur d'ordre :	Ministère de l'économie, des finances, et de la relance, Bundesministerium für Wirtschaft und Energie
Référence officielle :	5G-OPERA D3.4
Relecteur :	Florian Kaltenberger, Thomas Höschele
Résumé :	
Date de publication :	10/02/2023
Version :	1.0
Accès :	Public
Mots clés :	Open RAN, 5G Private Networks, Requirements

Executive Summary

Within the 5G-OPERA project, German and French partners cooperate to develop a technological ecosystem for open Radio Access Networks (RAN) for private networks. This report explains the technical requirements for open core network. The report starts with a short introduction in Section 1.

Section 2 explains the minimum required core network function for private networks as well as additional functions for innovations targeted by 5G-OPERA, i.e., time sensitive network, positioning and network slicing.

Section 3 defines the security requirement of core network. Since virtualization is key in the core network, a list of security requirements of virtualized environment is given. Afterwards, the main security requirements of service based architecture are defined for each function. Section continues with the security requirements of open-source software, management and information.

Section 4 explains what kind of changes or additional features are required in core network in order to integrate time sensitive networking (TSN). General architecture of integration of TSN in 5G network is illustrated. Afterwards, required extensions in core side, i.e., new application function, new TSN translator and extension for policy charging function (PCF-AF), etc. have been explained. Information flows and synchronization requirements have been defined. The section finalized by explaining interactions between TSN-AF and PCF, Centralized Network Controller (CNC), Session Management function (SMF), User Plane Function (UPF) and TSN Translators (TTs).

Section 5 describes the requirements for positioning for 5G private network. The characteristic of Location Management Function (LMF) are introduced and then positioning procedures and algorithm are visualized. Finally, the localization accuracy is introduced in a table as function of bandwidth.

Section 6 shows the requirements of network slicing, while Section 7, 8, 9, 10 are briefly explain the automation, interoperability, scalability, and flexibility, respectively. And report gives a summary and conclusions in Section 11.

Table of Contents

Abbreviations

TSN	Time Sensitive Networking
5GS	5G System
NFs	Network Functions
AF	Application Function
CP	Control Plane
CNC	Centralized Network Plane
PCF	Policy Charging Function
TTs	TSN Translators
DP	Data Plane
NW-TT	Network-Side TSN Translator
SMF	Session Management Function
GM	Grand Master
TSCAI	Time Sensitive Communication Assistance Information
UPF	User Plane Function
UE	User Equipment
gPTP	generalized Precision Time Protocol
TSi	ingress Timestamping
PTP	Precision Time Protocol
TSe	egress Timestamp
PSFP	Per-Stream Filtering and Policing
QoS	Quality of Services
VLAN	Virtual Local Area Network
PFCP	Packet Forwarding Control Protocol
LMF	Location Management Function
AMF	Access and Mobility Management Function
UL-TDoA	Uplink-Time Difference of Arrival
SRS	Sounding Reference Signal
NRPPa	NR Positioning Protocol A

PDU	Protocol Data Unit
NGAP	NG Application Protocol
MIoT	Massive Internet of Things
eMBB	evolved Mobile Broad Band
URLLC	Ultra-Low Latency
SBA	Service Based Architecture
CUC	Centralized User Configuration
CI	Continues Integration
CD	Continues Development
SCAS	5G Security Assurance Specification
UPF	User Plane Function

Table of Figures

Table of Tables

1 Introduction

The 5G-OPERA project aims to build a Franco-German ecosystem for private 5G networks under the joint leadership of TU Dresden and EURECOM (Sophia Antipolis). The focus of the project is the idea of open hardware and software with open interfaces in the area of mobile communication networks to allow multi-vendor options for technical equipment. The goal of the project is to ensure that the hardware and software of all project partners can work together. In addition to setting up reference test environments and demonstrators in Industry 4.0 environments of both countries, 5G-OPERA is supporting the trials in the three demonstration projects and will advise all additional projects joining the program.

This deliverable is the third of the 5G-OPERA project and defines the requirements of the open core networks (CNs) for private 5G networks. In this document, openness means that interfaces between CN and Radio Access Networks (RAN) are open which allow interoperability for multivendor option. If interfaces become open, then secure communication should be ensured. Furthermore, there are some innovations such as Time Sensitive Network (TSN) and positioning, which are in the scope of the 5G-OPERA. Integration of these innovations requires implementation of new feature sets which are defined in this document. In addition to these, requirements of network slicing are also listed, following by other requirements, i.e., interoperability, flexibility, scalability, etc.

Most content of this document is based on the specifications defined by 3GPP standards. Interested readers are referred to the relevant cited documents for further investigation, since covering all requirements from the standards will yield unnecessary extension of the document.

2 Network Function Requirements

This section describes briefly the required NFs for 5G private networks which are different from 5G public networks. At first, the NFs for a minimalist version of the CN are presented. Second, additionally required NFs for localization, TSN and network slicing are presented. These functions and interfaces must follow specifications in the Rel. 16 and later versions.

Based on the use cases, a reduction of the functionality can be applied to theCN for private networks, such as roaming, UPF-UPF communication or billing and charging since CN for private networks is different than the CN for public networks. The required NFs for a minimalist version are listed in Table 1 while additional network functions are listed in Table 2.

Table 1: Minimalist version of core network

Network function	Description of Requirements
AUSF	Specified in TS 29.509
AMF	Should support N1, N2 interfaces in TS 23.502

	Should support Namf service interfaces as specified in TS 29.518 Should support multiple gNBs at the same time. Limit is provided by performance of hardware running the CN / AMF and deployment of the NF
UDM	Specified in TS 29.503
SMF	Should implement N4 interface
UPF	Should expose N4 (PFCP) interface as specified in TS 29.244 Should implement N3 (GTP-U) interface as specified in TS 29.281 Should implement N6 Should support IPv4 PDU types Should support Ethernet PDU types (optional, required for TSN – Qbv)
UDR	Specified in TS 29.504
PCF	Should expose N5 interface to a TSN application function
NRF	Specified in TS 29.510

Table 2: Additional NFs required for localization, TSN and network slicing.

Network function	Description of Requirements
NSSF	Specified in 29.531
LMF	See Section 'Positioning Requirement for Core Network'
TSN AF	Would require CNC/CUC; if not available NETCONF message to TSN-AF could be enough
I-UPF	Should support data flow via N3 to the NG-RAN Specifications in TS 29.244
I-AMF	Should support message flow via N2 to the NG-RAN Specifications in TS 29.518

3 Security Requirements for Core Network

5G was designed by taking the security into account. This secure-by-design philosophy led to many technical changes to security mechanisms in comparison to its predecessors like 3G and 4G. These mechanisms aim to protect the network and the user alike.
The different use cases, like massive Machine Type Communication (mMTC), evolved Mobile Broad Band (eMBB) and Ultra-Reliable Low Latency Communication (URLLC) have unique security requirements. They must be evaluated in a use case specific threat and risk analysis. With its modular architecture, 5G is able to support many security requirements out of the box.

3.1 Virtualization

The CN is often rolled out in a virtualized environment like Docker or Kubernetes. The virtualization itself comes with their own threats and risks. All virtualization solutions come with their own set of security mechanisms. Often, they are not enabled by default. Therefore, the following recommendations apply to all virtualization solutions:

- Using virtualization needs a well-planned approach. This approach needs to be documented.

- If several different applications are planned to run on the same bare metal, but in different virtualized environments, it has to be ensured that the resource and security requirements of all applications can still be met.
- Only services necessary to run the virtualization should run on the machine hosting the virtualized environments.
- The hardware on which the virtualization runs needs to be planned with enough resources and performance to support all applications that are planned to run on it.
- The system administrator needs to be familiar with the specific security mechanisms of the used solution.
- Necessary and useful security mechanisms need to be enabled.
- The handling of snapshots must be regulated. The regulation needs to be documented.
- Necessary management interfaces need to be protected. A good way to do so is to only make them accessible from a trusted network (e. g. via VPN).
- When using virtualization, sometimes problems with inconsistent system times occur. It needs to be taken care of that the system time on the virtualized instances is always correct [1].
- Additional to these general recommendations it is suggested to observe the recommendations for virtualization provided by NIST.
    - Guide to Security for Full Virtualization Technologies - Special Publication 800-125 [2].
    - Application Container Security Guide - NIST Special Publication 800-190 [3].
    - Security Recommendations for Server-based Hypervisor Platforms - NIST Special Publication 800-125A Revision 1
- Administrators need to make themselves familiar with the security recommendations for the platform used.
- It is always recommended to prepare a threat analysis as well as a risk analysis for every installation. This measure helps in deciding for the needed security mechanisms in the specific environment.

3.2 Service Based Architecture

The 5G Service Based Architecture (SBA) is a key component of the CN that enables the creation of flexible, programmable, and scalable 5G networks. Among other things, the CN is responsible for resource management, such as compute, storage and network bandwidth. It ensures that they are granted in a dynamic and efficient manner.
The SBA may consist of several network functions. It's important to note that the specific security functions used in a CN can vary depending on the network configuration and the specific use case.
The main functions of the 5G SBA include:

- User Plane Function (UPF)
- Session Management Function (SMF)
- Access & Mobility Management Function (AMF)
- Unified Data Management (UDM)
- Authentication Server Function (AUSF)
- Application Function (AF)
- Policy Control Function (PCF)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- Network Exposure Function (NEF)

- Service Exposure Function (SEF)
- (User Data Repository (UDR))
- And the interfaces N1, N2, N3, N4, N6 and N9

There are several security functions that are used by default in the CN to protect the network and user data from unauthorized access, data breaches, and other types of cyber threats. Requirements on CN security, such as requirement on SBA, and on E2E CN interconnection security is specified in TS 33.501 [4].

- Following entities are introduced in 5G CN for security TS 33.501 [4]:
- Security assurance specifications for AMF, UPF, UDM, SMF, AUSF, SEPP, NRF, and NEF are described in TS 33.512 (AMF), TS 33.513 (UPF), TS 33.514 (UDM), TS 33.515 (SMF), TS 33.516 (AUSF), TS 33.517 (SEPP), TS 33.518 (NRF), TS 33.519 (NEF), respectively.
- If referencing the SCAS documents, please check, if newer versions are available.

3.2.1 UPF

Security requirements specific to the UPF are the following:

- Confidentiality protection of user data transported over N3 interface
- Integrity protection of user data transported over N3 interface
- Replay protection of user data transported over N3 interface
- Signalling Data Protection
- TEID uniqueness

The complete description, relevant references and SCAS (5G Security Assurance Specification) test cases can be found in the ETSI document “ETSI TS 133 117 V16.6.0 (2021-01)” [5].

3.2.2 SMF

The ETSI derived specific security requirements from the 3GPP documentation. They are published in TS 133 515 [6]. The relevant requirements are:

- Priority of UP security policy
- Security functional requirements on the SMF checking UP security policy
- Charging ID Uniqueness

The complete description, relevant references and SCAS test cases can be found in the ETSI document “ETSI TS 133 515 V16.2.0 (2020-08)” [6].

3.2.3 AMF

Derived from the 3GPP documentation, the ETSI defined the following security requirements for the AMF [7]. The relevant requirements are:

- Synchronization failure handling
- RES* verification failure handling
- Replay protection of NAS signalling messages
- NAS NULL integrity protection
- NAS integrity algorithm selection and use
- Bidding down prevention in Xn-handover
- NAS protection algorithm selection in AMF change
- 5G-GUTI allocation
- Invalid or unacceptable UE security capabilities handling

The complete description, relevant references and SCAS test cases can be found in the ETSI document “ETSI TS 133 512 V16.3.0 (2020-08)” [7].

3.2.4 UDM

The ETSI derived specific security requirements from the 3GPP documentation. They are published in TS 133 514 [8]. The relevant requirements are:

- De-concealment of SUPI from the SUCI based on the protection scheme used to generate the SUCI
- Synchronization failure handling
- Storing of authentication status of UE by UDM

The complete description, relevant references and SCAS test cases can be found in the ETSI document "ETSI TS 133 514" [8].

3.2.5 AUSF

5G NR uses strong authentication mechanisms, such as mutual authentication between the user equipment (UE) and the network, to ensure that only authorized devices and users can access the network. The AUSF shall provide SUPI to the VPLMN only after authentication confirmation if authentication request with SUCI was sent by VPLMN.
Authentication in general is a very security critical process. The implementation should be tested intensively, especially for any implementation mistakes. ETSI did not define any specific security requirements for the AUSF. General requirements are published in ETSI TS 133 516 [9].

3.2.6 AF

The ETSI did not publish any specific security requirements for the AF. Nevertheless, the AF is designed to provide application services (e. G. video streaming) to the subscriber. Trusted AFs can interact directly with the CN. Therefore, it is essential, that only well tested application functions are trusted. One way to prove the trustworthiness of an AF would be if it was successfully pretested and all found vulnerabilities got patched.

3.2.7 PCF

The CN the creation and enforcement of policies to control access to network resources and to ensure that network services meet specific quality of service (QoS) requirements. Policies need to be created carefully to protect all the resources that need to be. Policies should always be created with security and privacy in mind. After setting up the network with its particular Policies, it is good practice to test the efficiency of the policies.
Currently, there is no ETSI Special publication available on specific security requirements and test cases for the PCF.

3.2.8 NRF

All the NFs in the network are fundamentally housed in the NRF, which is also protected by mutual authentication. The ETSI derived specific security requirements from the 3GPP documentation. They are published in T TS 133 518 [10]. The relevant requirement is "NF discovery authorization for specific slice".
The complete description, relevant references and SCAS test cases can be found in the ETSI document "ETSI TS 133 518" [10].

3.2.9 NSSF

The 5G SBA enables the creation of multiple isolated virtual networks on a shared physical infrastructure, which can be used to create customized network services for different use cases and industries.

The usage of network slices protects the QoS of every slice. It is also an additional hurdle for an attacker who has access to the network, but not to the network slice in question. Therefore, it can be seen as a measure to reduce the risk of information disclosure.
The ETSI did not publish any specific security requirements for the NSSF. A general statement by ETSI is, that interfaces between the NSSF and all providers should be protected [11].

3.2.10 UDR

The User Data Repository (UDR) is a component of the CN that is responsible for storing and managing subscriber information, such as user profiles and policies. The UDR is typically part of the application function and is used by other network elements, such as the PCRF (Policy and Charging Rules Function), to determine how to handle different types of traffic. This includes things like allocating resources, enforcing security policies, and applying QoS settings. The UDR also stores subscriber's information such as subscription-related data, service-related data and user-related data. It also enables the sharing of this data with other network functions, such as the PCRF, for example, in order to make policy decisions.
Due to the handling of user data, the UDR is a sensitive function. The UDR itself is not seen as a critical function by ETSI. Nevertheless, interfaces should always be protected. All implementations should be tested for potential security risks. If any risks are found, the implementation should be patched immediately.

3.3 Security of Open-Source Software

Although open-source software is useful to contemporary development teams, it also presents a security concern due to the prevalence of vulnerabilities. In fact, according to 65% of telecom experts, this poses the biggest security threat to 5G networks. Any open-source software used on the network needs to undergo a comprehensive audit in order to identify and patch any potential vulnerabilities [5].

3.4 Security Management Policies/Information Security Management System

It is highly recommended to run a so-called Information Security Management System (ISMS) to regulate and control security measures when running an CN. Such ISMS provides rules on how to use, operate and administer systems. It ensures that the entity running the CN asked themselves some of the relevant questions when running a sensitive system. Several ISMS systems are available. The most well-known may be the ISO 27001 System.

Such management systems are designed to monitor and manage security-related events and to respond to security incidents adequately.

ISO 27001 provides security best practices in a written form. They can be implemented and documented in the organization running the CN. The organization can apply for a certificate, proofing them to stick to these standards. The certificate will only be granted after a successful audit of the organization by an accredited auditor. To maintain the certificate yearly maintenance audits are necessary and every three years a successful re-certification audit must take place.
Even if running such a management system also introduces at least some overhead, it can as well help to streamline processes in the organization and make the whole management leaner. Practice has also shown, that companies using an ISMS are less likely to be affected by a successful computer attack. And even if they are affected, they often can ensure business continuity and/or go back to normal operations in a shorter timeframe compared to companies not using an ISMS.

3.5 Use cases

- Secure communication with other 5G networks
- Secure edge-to-core communication
- Secure UE authentication and converged edge

4 Core Network Requirements for 5G-TSN

This section describes the requirements of integration of Time Sensitive Networking (TSN) in 5G System (5GS). At first, general architecture has been illustrated. Then, required extensions in 5GS is described. Afterwards, requirements for information flow in TSN integrated 5GS has been listed. Afterwards, the synchronization and interaction between Network Functions (NFs) and TSN units has been explained.

4.1 Architecture in General

Figure 1: Integration of TSN in 5G Figure 1 illustrates the TSN control plane which is responsible to receive stream information from TSN End Station. TSN control plane also communicates with TSN bridge via TSN AF. The integration of TSN with 5G Control and User Plane (C-Plane and U-Plane) is depicted in Figure 2 showing the relationship between TSN AF and NFs in the C-Plane.

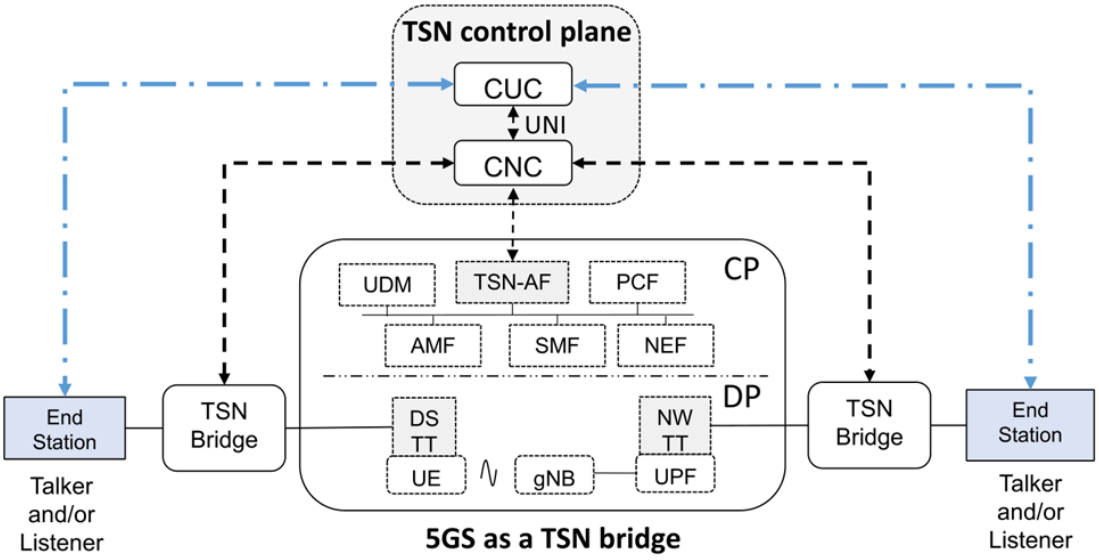

Figure 1: Integration of TSN in 5G [12]

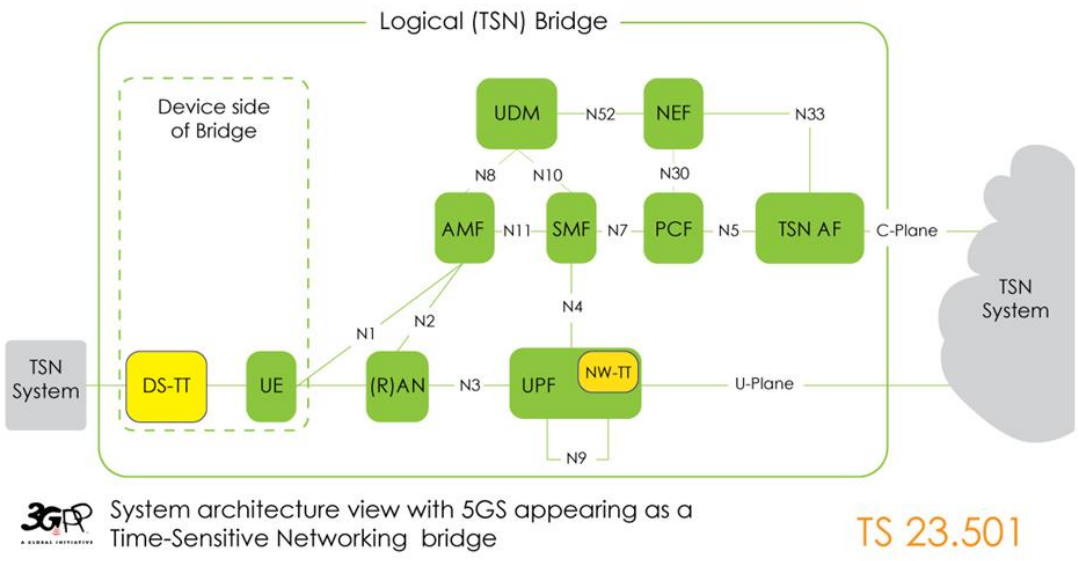

Figure 2: 5G system as a bridge [13]

4.2 5GS Extensions to Support TSN

- New Application Function (AF) to translate Control Plane (CP) communication from/to Centralized Network Controller (CNC)
- Extensions for Policy Charging Function (PCF)-AF communication
- New TSN Translators (TTs) to support User/Data Plane (DP) communication, e.g., translate Ethernet header, preserve priority information

4.3 Information Flows for 5GS integration with TSN

- According to the specification 3GPP TS 23.502, Appendix F [14], 5GS needs to implement two procedures to enable 5GS as a TSN bridge.
- The procedures are 5GS Bridge information reporting and 5GS Bridge configuration.
- As part of the first procedure, UPF needs to pre-configure the Network-Side TSN Translator (NW-TT) ports, and Session Management Function (SMF) needs to send measurement requests to NW-TT to determine the clock drift between the 5G GM clock and the TSN Grand Master (GM) clock.
- In the second procedure, SMF must be able to adjust the Burst Arrival Time, Periodicity, and Survival Time (clock drift) to RAN via Time Sensitive Communication Assistance Information (TSCAI). SMF can also forward if needed the additional information from CNC e.g., Port Management information to the User Plane Function (UPF)/NW-TT or the UE/DS-TT.

4.4 Synchronization

- Section 5.27.1 in 3GPP TS 23.501 [15] describes how 5GS can support time synchronization service.
- According to 3GPP TS 23.501 [15] - section 5.27.1.1, 5G can operate in one or multiple PTP instances in one of the following modes:
    - As a time Aware system in gPTP
    - As a boundary Clock

    - As a Peer to Peer or End to end Transparent clock
- According to 3GPP TS 23.501 [10] section 5.27.1.1, Translators support a PTP profile according to the configuration. DS-TT, NW-TT, User equipment, gNB, and UPF are synchronized with the 5G internal clock. The grandmaster clock selection can be done either with the best master clock algorithm (BMCA) or can be configured locally.
- In the port management capability message, translators indicate the time synchronization parameters they support. This message is transmitted to TSN AF in a UMIC or PMIC, and AF then sends this data to CNC. This information contains things such as:
    - Supported PTP instance types;
    - Supported transport types;
    - Supported PTP delay mechanisms;
    - Grandmaster capability;
    - Supported PTP profiles;
    - Number of supported PTP instances.
- The Configuration of PTP (including Sync and announce reception timeouts, port states, sync and announce messages intervals) are discussed in 3GPP TS 23.501 [15] - Annex K.2.2.
- According to 3GPP TS 23.501 [15], section 5.27.1.2.2.1, when NW-TT receives the downlink gPTP message, it adds an ingress timestamping (TSi) for each gPTP event (Sync) message. Moreover, NW-TT has to implement a PTP instance to forward the gPTP message to the corresponding port in DS-TT.
- After DS-TT receives the gPTP message, it needs to add an egress port timestamp (TSe). For this gPTP message, the difference between TSi and TSe represents the residence time in the 5G system.
- The DS-TT has to do the following operations: Adds the calculated residence time expressed in TSN GM time to the correction field, replaces the cumulative rateRatio received from the downstream TSN node with the new cumulative rateRatio, and Removes the suffix field that contains TSi.

4.5 Interaction between CNC and TSN-AF

- According to 3GPP TS 23.501 [15], section 4.4.8.2, TSN AF acts as the control plane translator in 5G system to interact with CNC, and TSN-AF is responsible to register or update bridge information to CNC.
- In Annex I, TSN usage guidelines , if 5G system support Per-Stream Filtering and Policing (PSFP) the PSFP information should be provided by CNC.
- In section 5.28.2, the QoS Flows are setup based on the PSFP information provided by CNC. If the PSFP is not available, the pre-configured QoS is used during the PDU session establishment. More specific, in section 5.28.4, the 5GS can support TSN stream using pre-configured mapping from PCP to QoS Flows.
- In section 5.28.4, TSN AF is responsible to updates the QoS information to CNC. The minimum set of TSN QoS-related parameters used by TSN AF are: traffic classes and their priorities per port, TSC Burst Size of TSN streams, 5GS bridge delays per port pair and traffic class (independentDelayMax, independentDelayMin, dependentDelayMax, dependentDelayMin), propagation delay per port (txPropagationDelay) and UE-DS-TT residence time.

- Section 5.28.3.3 states that the VLAN configuration are pre-configured at the TSN AF and NW-TT and reported to CNC. The VLAN information cannot be exchanged between TSN AF and NW-TT.
- NetConf is the controlling interface between TSN AF and CNC as well as CNC and other TSN bridges ("the 5GS should appear as a regular TSN bridge").
- The architecture of CUC and CNC in the TSN domain can be seen in [16]. CUC may be required as well for testing; however, there is no direct connection between 5GS and CUC.

4.6 Interaction between TSN-AF and PCF

- The interface between TSN-AF and PCF is N5 interface and the corresponding specification is 3GPP TS 29.514 [17] and 3GPP TS 23.502 [14] (section 4.16.5.1)
- There are mainly two cases of PCF that require notifying TSN AF.
    - According to 4.2.5.16, PCF must send an Npcf_PolicyAuthorization_Notify message to TSN AF to notify the TSN bridge, NW-TT port, and DS-TT port information corresponding to a PDU session.
    - Or if PCF receives the TSN bridge management containers and TSN port management containers from SMF, it needs to update the TSN bridge configuration and TSN port configuration to TSN AF using the same message according to 4.2.5.13.

4.7 Interaction between SMF and PCF

- The interaction between SMF and PCF related to TSN is defined in Section 4.16.5.1 in 3GPP TS 23.502 [14] and Section 5.2.2.3 in 3GPP TS 29.513 [18].
- SMF may use SMF initiated SM Policy Association Modification (Npcf_SMPolicyControl_Update) service to report to PCF that a manageable DS-TT port has been detected and no AF session exists for this PDU session yet. PCF then will notify the AF as described in the previous section (3.6). SMF also may include UE-DS-TT Residence Time or PMIC with port number or BMIC in the report message.

4.8 Interaction between SMF and UPF

- The interface between SMF and UPF is N4 interface and the corresponding specification is 3GPP TS 29.244 [19].
- According to Section 5.26.2, SMF should send a Packet Forwarding Control Protocol (PFCP) Session Establishment Request to the UPF to establish the corresponding PFCP session for ethernet traffic. This is for the TSN bridge management, where the port numbers, bridge ID, and info are set.
- According to Section 5.26.3, SMF transparently relays the information of the 5GS bridge and port management Container between NW-TT and TSN AF through the PFCP Session Modification Request and Response message.
- Last, based on Section 5.26.4, the UPF reports the clock drift between the TSN and 5GS times if the time offset reporting threshold or cumulative rate ratio measurement threshold is fulfilled.

4.9 Interaction between TSN –AF and TTs

- The interactions between TSN AF and TTs are specified in 3GPP TS 24.539 [20].
- We can separate Procedures into two categories:
    - Interaction of TSN AF with Device Side Translator (DS-TT)
    - Interaction of TSN AF with Network side Translator (NW-TT)

- **TSN AF with DS-TT procedures:** Port management requests (5.2.1, 5.2.2), Port management capability
    - According to Sections 5.2.1, 5.2.2, port management can be requested by the **network** and DS-TT. They are used for getting the capabilities, setting and monitoring parameters
    - According to Section 5.2.3, DS-TT port management capability is also sent by DS-TT to TSN AF via SMF and PCF, for notifying of DS-TT capabilities to TSN AF.
- **TSN AF with NW-TT procedures**: Includes Port Management (Sections 6.2.1, 6.2.2), User plane node management (Section 6.3)
    - Similarly, each of these procedures is either initiated by TSN-AF for obtaining/setting/modifying/subscribing to parameters, or initiated by NW-TT to notify TSN-AF of the current values of parameters requested by TSN-AF.

5 Positioning Requirement for Core Network

5.1 LMF

The 5G-OPERA shall develop a localization management function (LMF) with the following characteristics

- LMF shall support service-based architecture and interfaces based on 3GPP specifications
- LMF shall provide NL1 interface to AMF
- LMF shall support LPP PDU Transfer and NRPPa PDU transfer
- LMF shall support interfaces with external localization algorithms
- LMF shall support UL-TDoA localization based on SRS measurements as defined in Section 8.13 of 3GPP TS 38.305 [21].
- LMF shall support external interface to query position of a given UE.

5.2 Positioning procedures and algorithms

LMF shall support Uplink-Time Difference of Arrival (UL-TDoA) localization based on SRS measurements as defined in Section 8.13 of 3GPP TS 38.305 [21] and shown in Figure 3.

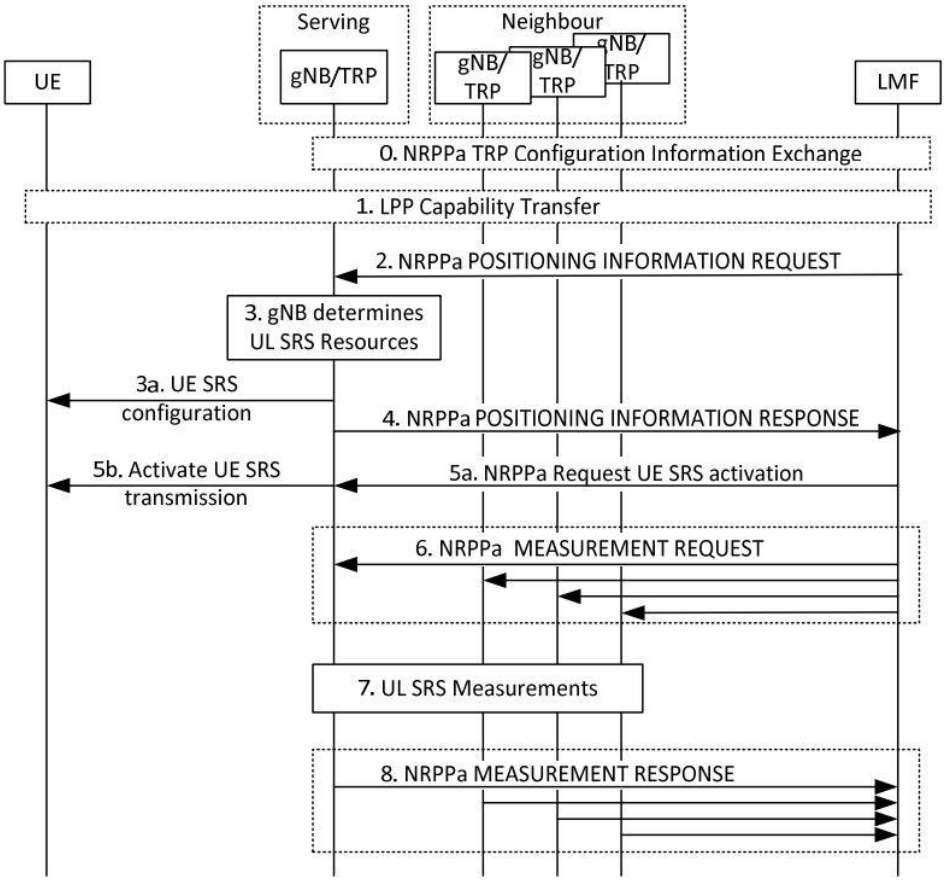

Figure 3: UL-TDoA localization procedures Taken from 3GPP TS 38.305.

Table 3 provides a target for the accuracy to be expected from the localization algorithms and the measurement accuracy derived from the SRS transmissions, respectively. The results obtained are using the simulations performed considering five single antenna base stations in a 120x60x10 indoor 3gpp_138_901_InF_LOS channel model. The accuracy requirements with 90% of the time based on bandwidth in both 2 and 3 dimensions (2D, 3D) are mentioned in the Table 3. The H in the table represents the horizontal accuracy in a 2D plane, and V represents the vertical accuracy in a 3D plane.

Table 3: Localization accuracy requirements

Bandwidth	**Accuracy**
40 MHz	H – 9m, V - 88m
80 MHz	H – 1m, V - 6m
100 MHz	H – 1m, V - 6m

5.3 Signaling between an LMF and NG-RAN node

The Signaling between an LMF and NG-RAN node is defined in Section 6.5 of 3GPP TS 38.305 [21], and illustrated in Figure 4 and Figure 5.

The following procedures shall be supported

1. **NR Positioning Protocol A (NRPPa) PDU Transfer for Positioning Support**
    1. Namf_Communication_NonUEN2MesasgeTransfer (to be implemented)
    2. NG Application Protocol (NGAP) Downlink Non UE Associated NRPPa Transport (done)
    3. NGAP Uplink Non UE Associated NRPPa Transport (done)
    4. Namf_Communication_NonUeN2InfoNotify (to be implemented)
2. **NRPPa Protocol Data Unit (PDU) Transfer for UE Positioning**
    1. Namf_CommunicationN1N2MessageTransfer
    2. NGAP Downlink UE Associate NRPPa Transport
    3. NGAP Uplink UE Associate NRPPa Transport
    4. Namf_CommunicationN2InforNotify

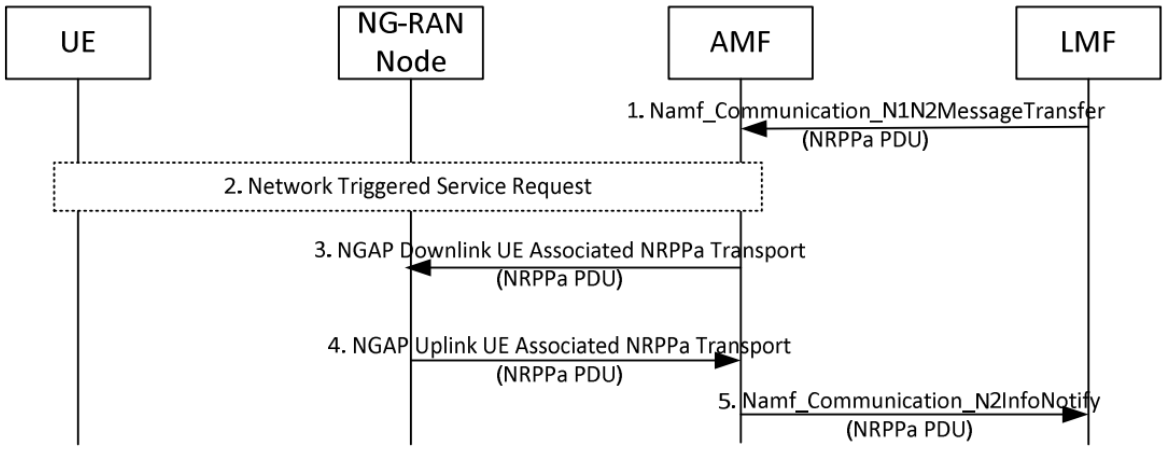

Figure 4: NRPPa PDU Transfer between an LMF and NG-RAN node for EU positioning [21].

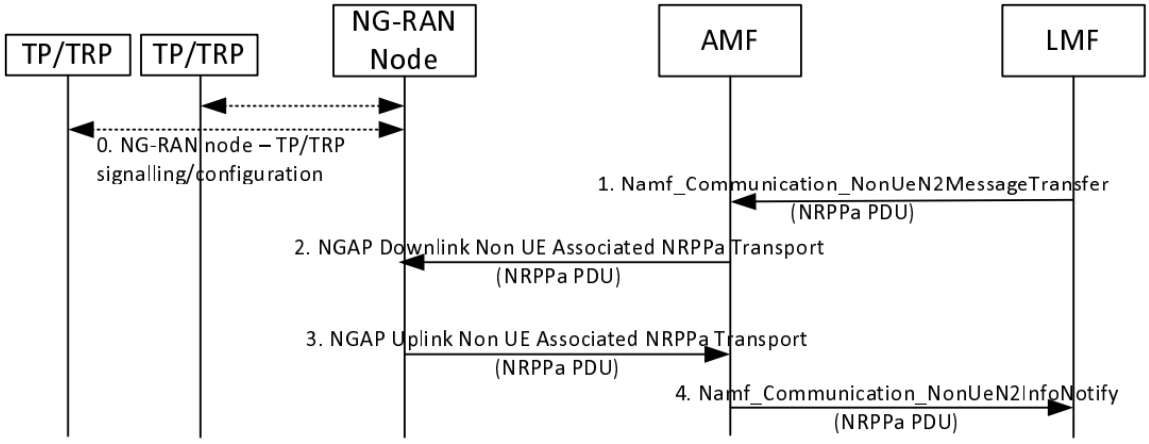

Figure 5: NRPPa PDU Transfer between an LMF and NG-RAN for obtaining NG-RAN Data [21].

6 Network Slicing

"Network slicing allows the operator to provide customized networks. For example, there can be different requirements on functionality (e.g. priority, policy control, security, and mobility), differences in performance requirements (e.g. latency, mobility, availability, reliability and data rates), or they can serve only specific users (e.g. MPS users, Public Safety users, corporate customers, roamers, or hosting an MVNO)" TS 22.261 [22]. One or several network slices can be supported by one network. Some management, constraints and cross-network slice related requirements as given by TS 22.261 [22] are listed below

6.1 Management Requirements

- It should be possible to create, delete or modify a network slice and there should be no or minimal impact on services and traffic in other network slices.
- It should be possible to update and define a set of services and capabilities provided in a network slice
- It should be possible to assign a UE to a network slice, to move a UE from one network slice to another, and remove a UE from a network slice.
- It should be possible to scale a network slice and minimum provided capacity should not be affected by scaling.
- It should be possible to define a priority order between different network slices in case of competition of resources on same network.

6.2 Network Slice Constraints Requirements

- It should be possible to prevent an unauthorized UE from accessing to a radio resource dedicated to a private slice.
- A UE should be in the geographic area in which network slice is accessible.
- A mechanism should be provided to allow UE to receive service only form authorized slice.
- When the number of registered UEs are the maximum, registration of a new UE should be prevented. Same restriction should also be provided when the maximum number of data session is established for a network slice.

7 Manageable by Automation and Orchestration Tools

The CN should support Continues Integration (CI), Continues Delivery (CD), and Continues Deployment methods. These are abbreviated as CI/CD, which specifically introduces continuous monitoring from integration, testing phase and deployment [24].

CI is a practical way of integration of changes done in the code for building, testing and merging to a shared repository. The aim is to have one common branch of an application and to avoid conflicts.

After code has been tested and built, continuous delivery automates the release of validated code to the repository. The main objective of the continuous delivery is to have a codebase which is always ready for deployment.

Continuous deployment allows organizations to deploy their applications automatically. With continuous deployment, developer's change to an application goes live after minutes of writing.

Jenkins is one of the best known open source tool for CI/CD. Tekton is also a CI/CD framework for K8S platform which provides a cloud-native CI/CD with K8S. There are also other CI/CD tools such as Spinnaker, GoCD, etc.

8 Interoperability

By definition, interoperability is a feature of a product or a system and an interoperable product or system can work with other products or systems. An interoperable core network can work with different RANs. For multi-vendor solution interoperability of 5G CN with RAN from different vendors are ensured by the 3GPP TS. Particularly, N1, N2, N3 and N4 interfaces need to be implemented as specified by standards. Addition to this, service based interfaces can also be open as described in the standards by 3GPP. As a result, network functions from different CNs can work seamlessly. An important aspect for the project is enabling multivendor core options for the RAN.

9 Scalability

Scalability is the ability of a system to adapt changes or demand by adding resources to the system. The CN might need to scale up or down based on the network traffic. Specifically, new network functions may need to be added to prevents downtime and ensure QoS. However, a load balancer is required for a pool of NFs to distribute the traffic among NFs.

10 Flexibility

Flexibility of the CN is required for 5G private network. There will be a wide range of UEs and possibly different access networks. The CN should be able to support them. It can also be helpful to place different NFs at different physical locations in the network. A use case for this separation is that if user plane traffic requires simple processing, it can be run on low-cost hardware, whilethe remainder of the traffic can run on advanced hardware. Furthermore, the CN is built on NFV, SDN and cloud computing technologies. Therefore, these technologies are also required for the CN. Network slicing can be supported by the CN to tailor and optimize solutions.

11 Conclusions

This report gives the requirement of open CNs for 5G private networks. The document covers required core network functions, security requirement of these functions, requirements for integration of TSN, requirements for localization, network slicing as well as it explains how the CN can be manageable, interoperable, scalable and flexible. The relevant standards have been searched and cited. 5G-OPERA will follow the specifications of 3GPP for developing these requirements.

This deliverable is the last of the deliverable series of WP3.

12 References

[1] Federal Office fror Information Security, "Goldene Regeln Baustein B 3.304 Virtualisierung," 2011. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/IT-GS-Bausteine/Virtualisierung/Goldene-Regeln-Virtualisierung.pdf?__blob=publicationFile&v=1. [Accessed January 2023].

[2] National Institute of Standards and Technologies (NIST), "Guide to Security for Full Virtualization Technologies," January 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-125.pdf. [Accessed January 2023].

[3] M. Souppaya, J. Morello and K. Scarfone, "Application Container Security Guide," September 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf. [Accessed January 2023].

[4] 3GPP, "Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.12.0 Release 16)," October 2022. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[5] 3GPP, "5G Security Assurance Specification (SCAS); User Plane Function (UPF) (3GPP TS 33.513 version 16.2.0 Release 16)," January 2021. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[6] 3GPP, "5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class (3GPP TS 33.515 version 16.2.0 Release 16)," August 2020. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[7] 3GPP, "5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF) (3GPP TS 33.512 version 16.3.0 Release 16)," August 2020. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[8] 3GPP, " 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class (3GPP TS 33.514 version 16.3.0 Release 16)," November 2020. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[9] 3GPP, "5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class (3GPP TS 33.516 version 16.2.0 Release 16)," January 2021. [Online].

Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[10] 3GPP, "5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class (3GPP TS 33.518 version 16.2.0 Release 16)," August 2020. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[11] 3GPP, "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (3GPP TR 33.926 version 17.3.0 Release 17)," May 2022. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[12] S. Bhattacharjee, K. Katsalis, O. Arouk, R. Schmidt, T. Wang, X. An, T. Bauschert and N. Nikaein, "Network Slicing for TSN-Based Transport Networks," *IEEE Access (Volume: 9),* pp. 62788 - 62809, 2021.

[13] K. Flynn, "5G for Industry 4.0," The 5G Standart, May 2020. [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/tsn-v-lan. [Accessed January 2023].

[14] 3GPP , "Procedures for the 5G System (5GS) (3GPP TS 23.502 version 17.7.0 Release 17)," January 2023. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[15] 3GPP, "System architecture for the 5G System (5GS) (3GPP TS 23.501 version 17.7.0 Release 17)," January 2023. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[16] A. Abdul, "Hierarchical CUC/CNC Management Model," May 2020. [Online]. Available: https://www.ieee802.org/1/files/public/docs2020/60802-abdul-hierarchical-CUC-CNC-management-model-0520-v02.pdf. [Accessed January 2023].

[17] 3GPP, "5G; 5G System; Policy Authorization Service; Stage 3 (3GPP TS 29.514 version 17.7.0 Release 17)," January 2023. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[18] 3GPP, "5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3 (3GPP TS 29.513 version 17.9.0 Release 17)," January 2023. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[19] 3GPP, "Interface between the Control Plane and the User Plane nodes (3GPP TS 29.244 version 17.7.1 Release 17)," January 2023. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[20] 3GPP, "5G System (5GS); Network to TSN translator (TT) protocol aspects; Stage 3 (3GPP TS 24.539 version 17.6.0 Release 17)," October 2022. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[21] 3GPP, "NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN (3GPP TS 38.305 version 16.8.0 Release 16)," October 2022. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[22] 3GPP, "Service requirements for the 5G system (3GPP TS 22.261 version 17.11.0 Release 17)," October 2022. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[23] 3GPP, "Service requirements for the 5G system (3GPP TS 22.261 version 17.11.0 Release 17)," October 2022. [Online]. Available: https://www.3gpp.org/dynareport?code=status-report.htm#activeRel-17. [Accessed January 2023].

[24] Red Hat, "What is CI/CD?," May 2022. [Online]. Available: https://www.redhat.com/en/topics/devops/what-is-ci-cd. [Accessed January 2023].