NIST SPECIAL PUBLICATION 1800-33B

5G Cybersecurity

Volume B:
Approach, Architecture, and Security Characteristics

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
Information Technology Laboratory
National Institute of Standards and Technology

Surajit Dey
Parisa Grayeli
Blaine Mulugeta
Sanjeev Sharma
Chuck Teague
The MITRE Corporation
McLean, Virginia

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

Stefano Righi
Muthukkumaran Ramalingam
Paul Rhea
Madhan Santharam
AMI
Duluth, Georgia

Rich Mosley
Bogdan Ungureanu
Jitendra Patel
AT&T
Dallas, Texas

Tao Wan
CableLabs
Louisville, Colorado

Peter Romness
Matthew Hyatt
Leo Lebel
Cisco
San Jose, California

Dan Carroll
Dell Technologies
Hopkinton, Massachusetts

Steve Orrin
Leland Brown
Intel Corporation
Santa Clara, California

Yong Zhou
Corey Piggott
Michael Jones
Keysight Technologies
Santa Rosa, California

Michael Yeh
MiTAC Computing
Technology Corp.
Taoyuan, Taiwan

Gary Atkinson
Dan Eustace
Nokia/Nokia Bell Labs
Murray Hill, New Jersey

Bryan Wenger
Sean Morgan
Palo Alto Networks
Santa Clara, California

Marouane Balmakhtar
Gregory Schumacher
T-Mobile
Bellevue, Washington

April 2022

PRELIMINARY DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/5g-cybersecurity

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

National Institute of Standards and Technology Special Publication 1800-33B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-33B, 74 pages, (April 2022), CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: 5g-security@nist.gov.

Public comment period: April 25, 2022 through June 27, 2022

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Organizations face significant challenges in transitioning from 4G to 5G usage, particularly the need to safeguard new 5G-using technologies at the same time that 5G development, deployment, and usage are evolving. Some aspects of securing 5G components and usage lack standards and guidance, making it more challenging for 5G network operators and users to know what needs to be done and how it can be accomplished. To address these challenges, the NCCoE is collaborating with technology providers to develop example solution approaches for securing 5G networks. This NIST Cybersecurity Practice Guide explains how a combination of 5G security features and third-party security controls can be used to implement the security capabilities organizations need to safeguard their 5G network usage.

KEYWORDS

5G; cloud security; cybersecurity; hardware root of trust (HRoT); network function containerization; network function virtualization); privacy; secure boot; Service Based Architecture (SBA); trusted compute

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Kevin Fiftal	Intel Corporation
Taylor Roberts	Intel Corporation
Donna Dodson	NIST
Kevin Stine	NIST
Adam Sedgewick	NIST
Mark Kirschner	Nokia
Steve Vogelsang	Nokia
Jason Zuno	Nokia
Ian Oliver	Nokia Bell Labs
Peter Schneider	Nokia Bell Labs

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
AMI	AMI TruE

Technology Partner/Collaborator	Build Involvement
AT&T	5G network design reviews Security feature evaluation and implementation planning
CableLabs	5G network design reviews Security feature evaluation and implementation planning
Cisco	Cisco Secure Firewall Cisco Secure Network Analytics (Stealthwatch)
Dell Technologies	Dell EMC PowerSwitch 3048, 4048, & 5232-ON switches Dell EMC VxRail Dell Networking Operating System OS10 Dell PowerEdge 650/750 servers
Intel	Intel® Security Libraries for Data Center (Intel® SecL-DC) Intel Trusted Execution Technology (TXT) Intel® Xeon® Gold 5218R Processor
Keysight Technologies	5G LoadCore
MiTAC Computing Technology Corp.	MiTAC Aowanda MiTAC Thunder SX TN76-B7102
Nokia	Nokia 7705 SAR-8 Nokia 7750 SR-a8 Nokia AirScale (5G21A) Nokia AWHHF Nokia Cloud Mobility Manager (CMM) Nokia Cloud Mobile Gateway (CMG) Nokia CloudBand Applications Manager (CBAM) Nokia Container Services (NCS) Nokia NetAct Nokia NetGuard Certificate Manager (NCM) Nokia NetGuard Identity Access Manager (NIAM)

Technology Partner/Collaborator	Build Involvement
	Nokia Network Exposure Function (NEF) Nokia Network Resource Discovery (NRD) Nokia Network Services Platform (NSP) Nokia Policy Controller (NPC) Nokia Registers Nokia Shared Data Layer (SDL) Nokia Telecom Application Server (TAS) Nokia Zero Touch Service (ZTS) tools
Palo Alto Networks	Panorama VM-Series N3/N4 VM-Series N6 Gateway
T-Mobile	5G network design reviews Security feature evaluation and implementation planning

DOCUMENT CONVENTIONS

The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms "should" and "should not" indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solution and developing other parts of the content. As a preliminary draft, this volume will have at least one additional draft released for public comment before it is finalized.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: 5g-security@nist.gov.

Contents

1 Summary

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) recognizes the challenges that organizations face in transitioning from 4G to 5G. Of particular concern is the need to safeguard new 5G-using technologies at the same time that 5G development, deployment, and usage are evolving. Some aspects of securing 5G components and usage lack standards and guidance, making it more challenging for 5G network operators and users to know what needs to be done and how it can be accomplished.

The NCCoE developed the 5G Cybersecurity project to provide sample approaches for securing 5G networks through a combination of 5G security features defined in the 5G standards and third-party security controls. This project will also seek to identify gaps in 5G cybersecurity standards that should be addressed. This project is utilizing commercial tools to implement a 5G standalone network that operates on and leverages a trusted and secure cloud-native hosting infrastructure.

This preliminary draft volume explains why we are building the example solution to address 5G cybersecurity challenges, including the risk analysis to be performed and the security capabilities that the example solution will enable and demonstrate. It will include actionable and prescriptive guidance on using standards and recommended practices for multiple use case scenarios. Characteristics of the example solution already documented here may change slightly based on the results of the demonstrations, technical implementation changes, and the continued evolution of 5G standards, products, and services. There will be at least one additional draft of this volume made available for comment.

1.1 Challenge

5G is at a transition point where the technologies are simultaneously being specified in standards bodies, implemented by equipment vendors, deployed by network operators, and adopted by consumers. Although standards for some 5G cybersecurity features have been published by standards bodies, organizations planning to deploy, operate, and use 5G networks are challenged to determine what security capabilities 5G can provide and how they can deploy these features to safeguard data and communications.

Current 5G cybersecurity standards development primarily focuses on the security of the standards-based, interoperable interfaces between 5G components. The 5G standards do not specify cybersecurity protections to deploy on the underlying information technology (IT) components that support and operate the 5G system. This lack of information increases the complexity for organizations planning to leverage 5G. With the 5G architecture based on cloud technology, 5G systems could potentially leverage the robust security features available in cloud computing architectures to protect 5G data and communications.

1.2 Solution

To address these challenges, the NCCoE is collaborating with 5G and cybersecurity technology providers to develop an example solution. In its first phase, it will demonstrate a 5G standalone (SA) network deployment that operates on and leverages a trusted and secure cloud-native hosting infrastructure. The example implementation will demonstrate how cloud technologies can provide foundational security features outside the scope of the 3rd Generation Partnership Project (3GPP)'s 5G security architecture. The first phase of the project will also showcase how 5G security features can be utilized to address known security challenges found in previous generations of cellular networks such as Long-Term Evolution (LTE). It will demonstrate how commercial products can leverage cybersecurity standards and recommended practices for different 5G use case scenarios. If gaps in 5G cybersecurity standards are identified during the project, the appropriate standards development organizations (SDOs) will be notified, and some of the project's collaborators may contribute to SDO efforts to address the gaps.

Based on expertise from the industry collaborators participating in the effort, and given the evolution of the standards, the availability of commercial products, and the alignment with commercial networks, this project is focused on the security characteristics of 5G SA networks. Telecom carriers have started or are planning to incorporate 5G SA, since the newest 3rd Generation Partnership Project (3GPP) standards-based 5G security enhancements are available only in a 5G SA network (not a 5G non-standalone [NSA] network). To fully demonstrate and showcase these 5G security capabilities, the NCCoE project is focused on a typical implementation of a secure 5G SA deployment.

The solution will be designed around two focus areas:

- The **Infrastructure Security Focus Area** will concentrate on the trusted and secure cloud resources required to operate a modern mobile network, specifically the supporting infrastructure's cybersecurity protections. The objective is to provide a trusted infrastructure to support the 5G Core Network functions, radio access network (RAN) components, and associated workloads. Since security for the underlying infrastructure is not within the scope of 3GPP specifications, this focus area is included in the project to provide a trusted platform and holistic security reference architecture for a complete 5G network.
- The **5G Standalone Security Focus Area** will deploy a 5G SA network to enable the foundational configuration of the 5G Core's security features in a manner that demonstrates the cybersecurity capabilities available in a 5G SA deployment. The deployment will include 5G New Radio base stations and a 5G Next Generation Core. The deployment will demonstrate how security capabilities can be used for continuous monitoring of 5G traffic on both signaling and data layers to detect and prevent cybersecurity attacks and threats. The initial deployment will include classical RAN components, potentially leveraging virtualized and desegregated RAN components in the future depending on the availability of commercial technology and collaborator contributions.

The future phases of the project will include an expanded focus on security for 5G-specific use cases. Possible examples of these focus areas are Network Slicing security, Roaming security, and 5G Edge Computing. These expanded areas of focus will build on the foundational system described in this document, leveraging the security capabilities already enabled.

1.3 Benefits

Once completed, the demonstrated approach will offer several benefits to organizations that implement it, including the following:

- The components of the 5G network will be less susceptible to cyber attacks and will provide better attack visibility, detection, and control, which will reduce risk, lower the likelihood of an incident occurring, and expedite recovery.
- The 5G network's supporting infrastructure will be more resistant to compromise and provide more visibility into the trust status of the underlying platforms.
- The contents of 5G communications will be safeguarded from eavesdropping and tampering, and the privacy of 5G users will also be protected.
- The demonstrated practices can play an important role as your organization embarks on a journey to zero trust.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based example solution and provides users with the information they need to replicate a secure 5G SA network. This example solution is modular and can be deployed in whole or in part.

This guide will contain three volumes once completed:

- NIST SP 1800-33A: *Executive Summary* (currently available as a preliminary draft)
- NIST SP 1800-33B: *Approach, Architecture, and Security Characteristics* – what we built/are building and why **(you are here)**
- NIST SP 1800-33C: *How-To Guides* – instructions for building the example solution (to be published)

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-33A*, which describes the following topics:

- challenges that enterprises face in mitigating 5G cybersecurity risks
- example solution built at the NCCoE

- benefits of adopting the example solution

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-33B*, which describes what we did and why. Once completed, the following sections will be of particular interest:

- Section 3.5, Risk Assessment, will provide a description of the risk analysis we will take into consideration
- Appendix A, Security Control Map, will map the security characteristics of this example solution to cybersecurity standards and recommended practices

You might share the *Executive Summary, NIST SP 1800-33A*, with your leadership team members to help them understand the importance of adopting standards-based secure 5G SA networks.

IT and telecommunications professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-33C*, once it is published to replicate all or parts of the build created in our lab. We will not re-create the product manufacturers' documentation, which is generally widely available. Rather, we will show how we integrated the products in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of secure 5G SA networks. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 4.2, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a preliminary draft guide. There will be at least one additional comment period for this volume, and the other volumes of this guide will be released for review and comment on individual schedules so that each volume is available as soon as possible. We seek feedback on the contents of this guide and welcome your input. Comments, suggestions, and success stories will improve subsequent drafts of this guide. Please contribute your thoughts to 5g-security@nist.gov.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File** > **Edit**.
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov.

3 Approach

The NCCoE issued an open invitation to technology providers to participate in demonstrating how organizations operating or using 5G networks can use technologies to mitigate identified cybersecurity risks and meet industry sectors' compliance requirements. Cooperative Research and Development Agreements (CRADAs) were established with qualified respondents, and a build team was assembled. The team fleshed out the initial architecture, and the collaborators' components are currently being composed into an example implementation, i.e., build. The build team is documenting the architecture and design of the build. As the build progresses, the team will document the steps taken to install and configure each component of the build.

Finally, the team will verify that the build provides the desired capabilities. This will include conducting a risk assessment and a security characteristic analysis, then documenting the results, including mapping the security contributions of the demonstrated approach to the *Framework for improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework), NIST SP 800-53, and other relevant standards and guidelines.

3.1 Audience

This volume is intended for technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk for 5G networks. The information is targeting three types of organizations:

- **Commercial mobile network operators**. This volume will provide them a better understanding of cloud security capabilities that are already available in the systems their vendors provide. These hardware-enabled security capabilities are beyond what 5G standards currently specify and can provide complementary protection at this time. This is increasingly important as operations move to commodity platforms and software, and as mobile network technology merges with IT.
- **Potential private 5G network operators**. Private 5G networks are expected to become a reality, such as at universities and large companies. Any organization considering deploying and operating its own 5G network will need to manage its security using a risk-based approach. This volume will explain a range of security capabilities and the risks each capability helps mitigate, which will provide valuable information for organizations' risk management purposes.
- **Organizations using and managing 5G enabled technology**. Before organizations adopt 5G enabled technologies, they should make cybersecurity risk management decisions regarding their use, management, and maintenance. The information in this volume should help to inform those decisions.

This volume may be helpful to participants in 5G-related standards efforts (e.g., from standards developing organizations) who want to identify gaps in standards to inform their future work. Cybersecurity researchers who want to build 5G cybersecurity research testbeds may also find this volume useful as a reference.

All readers should already know the basic concepts of 5G; there are many resources available on 5G basics, including those from the GSM Association (GSMA) and Nokia. Readers should also be familiar with fundamental cybersecurity concepts. No previous knowledge of 5G-specific security or hardware roots of trust is necessary.

3.2 Scope

The scope of this project is to leverage the 5G standardized security features defined in 3GPP standards to demonstrate the enhanced cybersecurity capabilities available within 5G network equipment and end-user devices. In addition, the project will enable and demonstrate security capabilities of the underlying technologies and components that make up the supporting infrastructure required to effectively operate a 5G network. The example solution will utilize commercial 5G equipment in supporting 5G implementations.

Security capabilities and administration of mobile devices are key components of adopting 5G. This project focuses on the security implications of device connections to cellular networks. It leverages current and future NIST and industry guidelines and projects, such as the NCCoE's Mobile Device Security project, for guidance for securing and administering mobile devices. A similar focus will also be made on the security implications of Internet of Things (IoT) and Industrial IoT (IIoT) device connections to cellular networks, and this project will utilize guidance from NIST's Cybersecurity for IoT Program and other current and future projects.

The project will adopt the current and future relevant standards and guidance documents developed by various standards developing organizations, industry consortiums, and community of interests. Section 4 provides examples of relevant standards and guidance.

3.3 Assumptions

This project is guided by the following assumptions:

- Because there are some strict operational requirements, such as licensing and broadcasting radio frequency (RF) signals, that apply to deploying the radio access network on-premises at the NCCoE facility, the project will be operating a small number of physical 5G devices in RF-shielded environments.
- The host servers for the 5G network functions have hardware root of trust capabilities.
- 5G core network functions are implemented as a combination of virtual machines and containers.
- The initial example solution is comprised of a single standalone 5G network. Security capabilities focused on network interconnections with roaming partners and earlier generation technology, while important, will not be possible to demonstrate in this initial example solution.
- Technology components that comprise the example solution are collaborator-contributed, commercially available product offerings. These components are viewed as black boxes, and the solution focuses on their interconnections and integrations into the larger system.
- 5G standards are continuously being developed throughout the 3GPP release cycles to provide additional capabilities. Some components needed to enable the latest security capabilities may still be under development or not yet be commercially available. The example solution will adopt and demonstrate capabilities as the project's collaborating vendors enable them in their product offerings.

3.4 Reference System Architecture Description / Components

This section presents preliminary architecture diagrams for the system design, including logical and physical diagrams. It explains the major components of the architecture and summarizes the purpose of component interactions. This section starts with the high-level 5G implementation architecture and drills down to the architectures of the proposed security solution. The intent of this section is to explain the core ideas of the architecture, and not to provide exhaustive details of each component of the architecture and its security implications. Later sections of this volume will discuss components' security capabilities in more detail.

3.4.1 High-Level Architecture

Figure 3-1 depicts the high-level architecture of the NCCoE 5G implementation. On the left side of the diagram is the 5G radio access network. It consists of user equipment (UE) (i.e., mobile devices using the 5G network); radios and antennas; and baseband units (BBUs) known as gNodeBs (gNBs), which generate RF signals.

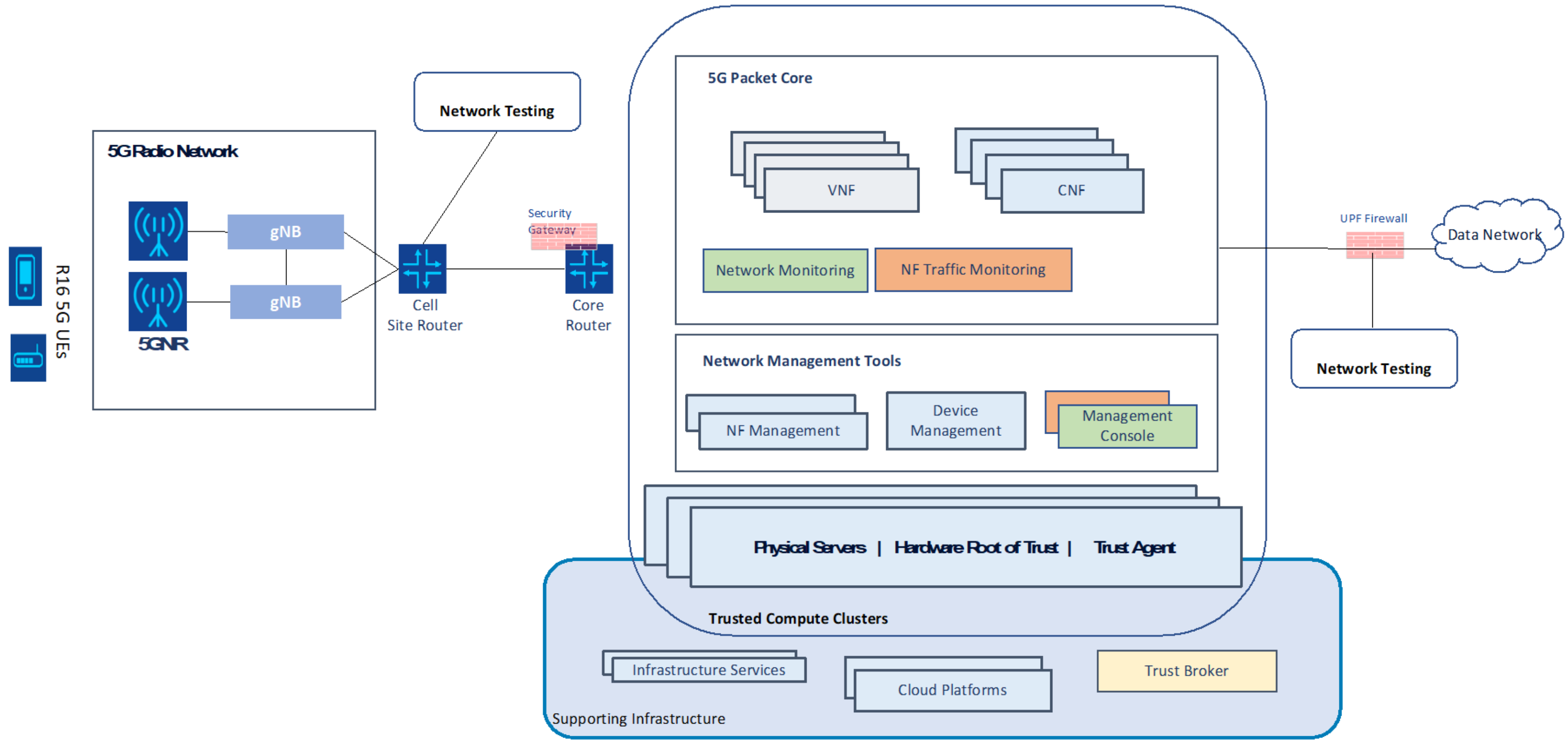
To the right of the radio access network, the diagram depicts the back haul network—the connection between the radio access network (cell sites) and the core network (data center). The cell site router and the core router denote the two ends of the back haul network in our reference implementation. Terminating the back haul network is an optional security gateway, depicted as a firewall. This firewall provides an IPsec tunnel for protecting signaling and user plane communications between the radio access network and the 5G packet core.

The data center, depicted in the middle, hosts various components that control and manage the network. The 5G packet core consists of numerous 5G network functions with various responsibilities (e.g., authentication, mobility, charging). The packet core's protocols and functions are specified in 3GPP standards. The data center also provides basic services required for configuring, managing, and maintaining all network components. This includes both infrastructure services (e.g., Network File System [NFS], File Transfer Protocol [FTP], Network Time Protocol [NTP], Domain Name System [DNS]) and management tools.

Finally, the right side of the diagram depicts a firewall connecting the data center to the data network. This firewall protects network functions within the core network in the data center from Internet Protocol (IP)-based attacks from the internet. Also, the firewall provides topology hiding for the IP addresses, so they are not directly accessible from the internet.

The network testing nodes shown in Figure 3-1 enable end-to-end validation of converged wireless and wired infrastructure, services, and security functionality. For example, the infrastructure can be stressed using concurrent connections of data, video, or voice while observing the connection rate and throughput of the simulated users. A testing node can deliver different types of traffic: legitimate, distributed denial of service (DDoS), and malware. It can simulate real-world application protocols and allows for customization and manipulation of raw data.

409 **Figure 3-1 High-Level Architecture**



3.4.2 Data Center Architecture

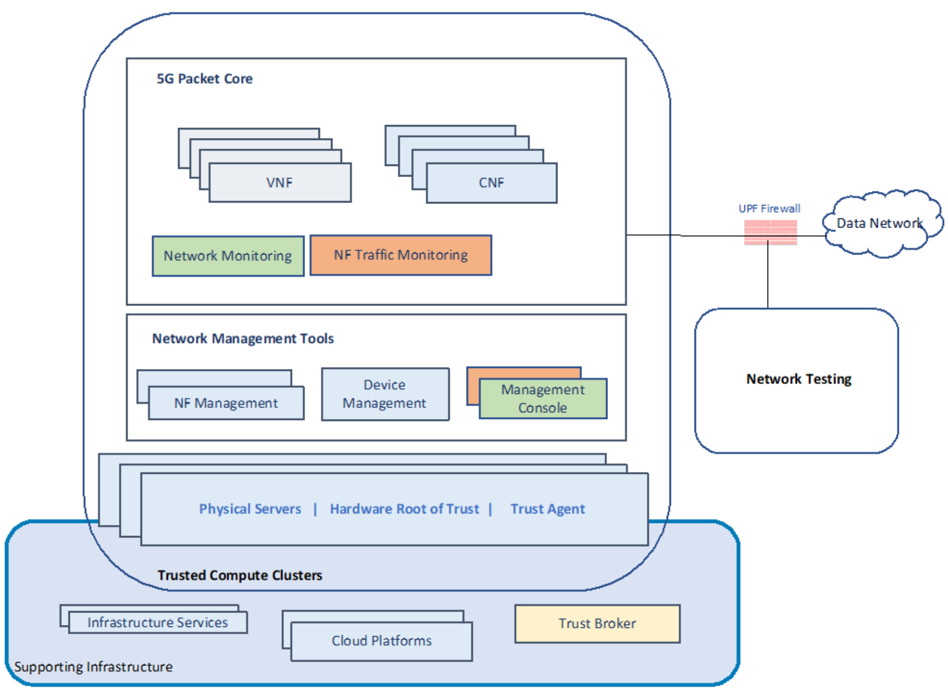
Figure 3-2 provides a more detailed view of the data center architecture specific to the NCCoE's 5G implementation. Other 5G networks might enable the same functionality described below in a different architecture or with different technologies.

In our proposed solution, the data center deploys all 5G packet core network functions (NFs) as either virtual machine-based NFs (VNFs) or container-based NFs (CNFs) using cloud computing technologies. The commodity compute platforms hosting these NFs are clusters of servers with commodity processors.

The data center also supports and provides connectivity for the tools and products used to provide security visibility and control into the network traffic. This is important for monitoring and enforcement for both the supporting IT infrastructure and the application and signaling traffic going across the 5G system.

The network management tools are necessary to operate and manage the packet core network functions, radio access network components, and various network routers and switches.

Figure 3-2 Data Center Architecture

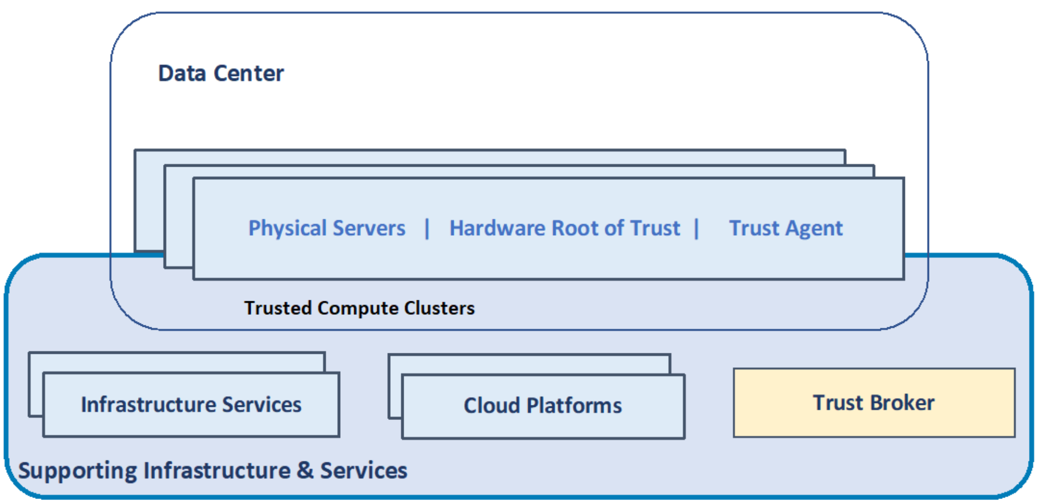


The data center uses multiple sets of tools, services, and cloud computing platforms to enable the functionality of the workloads it is responsible for hosting. This supporting IT infrastructure is shown as the "Supporting Infrastructure & Services" area at the bottom of the diagram. These types of components are often glossed over when discussing 5G systems but are critical for security and operations. This IT infrastructure is similar to what is used for cloud computing deployments, containing the security capabilities described in this document. All necessary supporting IT functions (directory services, certificate authorities, file servers, maintenance workstations, time servers, backup and recovery services, etc.) are included in the Infrastructure Services box.

3.4.3 Trusted Compute Cluster Architecture

Figure 3-3 depicts the subset of the physical computing environment within the 5G data center architecture called Trusted Compute Clusters. This name indicates that the servers have hardware roots of trust capabilities enabled. A server with hardware root of trust (HRoT) coupled with either an enabled hypervisor or an operating system and container runtime constitute the foundation for a more secure computing platform. This secure platform measures the firmware, operating system (OS), and virtual machine manager (VMM) integrity at boot and prevents rootkits or other low-level attacks. It establishes the trustworthiness of the server software and host platforms. One or more Trusted Compute Clusters can be utilized as the computing foundation that will host 5G network function workloads as VNFs or CNFs.

Figure 3-3 Trusted Compute Cluster Architecture



The HRoTs enable additional security capabilities for the infrastructure supporting 5G beyond what is defined in the 3GPP specifications. These capabilities include hardware-based controls to:

- measure platform integrity for each server in the infrastructure;
- assign specific labels for each server in the infrastructure to enforce isolation of critical workloads; and

- remotely attest each server's measurement and label against policies, feeding the results into a policy orchestrator to report, alert, or enforce rules based on the events.

These capabilities are enabled by multiple components in the diagram, including:

- hardware mechanisms to cryptographically measure hardware and firmware modules that comprise each server;
- a hardware security module to store cryptographic measurements on each server;
- a mechanism on each server that can communicate with the hardware security module onboard and report measurements to a Trust Broker, enabled by the OS or third-party software; and
- a remote attestation server, or *Trust Broker*, which collects measurements of the servers in the Trusted Compute Clusters, assigns labels to each server, and integrates with the Trusted Compute Clusters' workload schedulers.

These components are integrated together so that 5G workloads are deployed on trusted hardware that is designated for specific capabilities. The HRoT technologies for workload schedulers use platform measurements and labels as a factor in workload placement. The capabilities described in this section are based on techniques described in NIST IR 8320, Hardware Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. Specific prototype implementations for remote attestation and workload scheduling and placement can be found in NIST IR 8320A and NIST IR 8320B.

3.5 Risk Assessment

This section is preliminary and still under development. It first catalogs the technical security capabilities that this project is including. Next, it discusses the threats and vulnerabilities that each of the technical security capabilities is intended to address. The final part of this section will examine how the technical security capabilities help address requirements from relevant industry-specific references. Also, a future appendix will provide a security control map, with references for each capability to its corresponding elements in selected NIST guidance (e.g., NIST SP 800-53, Cybersecurity Framework, Security Measures for "EO-Critical Software" Use) and global telecommunications regulations.

Once completed, this section will provide a risk analysis for the reference architecture and its supporting functions and capabilities. This information could be used by an organization to inform their own risk analysis and decision making regarding how to respond to each risk (e.g., mitigate, accept, transfer, avoid).

3.5.1 Security Category

For the purposes of this document and project, *security categories* are high-level descriptions used for cataloging the technical security capabilities this implementation is considering. Table 3-1 provides a list of security categories that form the basis of this project, along with a unique reference identifier for each category. These categories are important and relevant to both commercial and private 5G networks and are inclusive of both 3GPP standards-defined security features as well as security capabilities available in the network's supporting cloud infrastructure.

Table 3-1 Security Categories

Security Category	Reference
Infrastructure Security Category (ISC)	
Hardware Roots of Trust Packet Core	ISC-1
Hardware Roots of Trust Virtualized RAN	ISC-2
Infrastructure Recommended Practice	ISC-3
5G Standalone Security Category (5GSC)	
Subscriber Privacy	5GSC-1
Radio Network Security	5GSC-2
Authentication Enhancements	5GSC-3
Interworking & Roaming Security	5GSC-4
API Security	5GSC-5
Network Slicing Security	5GSC-6
Application Security	5GSC-7
Internet Security Protocol Recommended Practice	5GSC-8

3.5.2 Security Capabilities

For the purposes of this document and project, the term *security capability* is used to describe a technical security feature which is important and relevant to commercial or private 5G networks. Security capabilities in the context of this document are inclusive of both 3GPP standards-defined security features and security capabilities available in the network's supporting cloud infrastructure. Table 3-2 highlights each security capability we plan to enable during the first phase of this project. For each capability, Table 3-2 lists its unique subreference identifier and provides a brief description, which also explains the capability. There are additional security capabilities on the project team's roadmap that will be incorporated in future project phases; see Appendix B for descriptions of capabilities tentatively planned for the subsequent phase.

Table 3-2 Security Capabilities

Security Capability	Subreference	Description
Infrastructure Security Categories		
Hardware Roots of Trust Packet Core, ISC-1		
Hardware-Based Platform Measurement	ISC-1.1	Measure platform integrity for each server in the infrastructure using hardware-based controls.
Hardware-Based Labeling	ISC-1.2	Assign specific labels for each server in the infrastructure using hardware-based controls.
Remote Platform Attestation	ISC-1.3	Attest each server's trust measurements and asset tags against policies, and allow services like workload orchestrators access to these findings so the results can be used as factors in workload placement/migration.
Network Function Orchestration Enforcement	ISC-1.4	Deploy and migrate NFs to servers that match platform measurements and labels.
Network Function Image Encryption	ISC-1.5	Encrypt each NF's image, and release the decryption keys only to servers that meet trust policies.
Infrastructure Recommended Practice, ISC-3		
Infrastructure Security Monitoring	ISC-3.1	Provide the visibility across the infrastructure needed to continuously monitor communications patterns, see threats within the extended network, and detect and respond to threats using methods such as behavioral modeling and supervised and unsupervised machine learning.
Network Segmentation	ISC-3.2	Ensure that the infrastructure design and implementation support keeping the different types of network traffic separate from each other.
5G Standalone Security Categories		
Subscriber Privacy, 5GSC-1		
Subscription Permanent Identifier (SUPI) Protection	5GSC-1.1	Encrypt the 5G SUPI with the public key of the home operator to create the Subscription Concealed Identifier (SUCI).
Reallocation of Temporary IDs	5GSC-1.2	Refresh a user device's temporary ID after initial registration, on every mobility registration update, and after use in paging.

Security Capability	Subreference	Description
Initial NAS Message Security	5GSC-1.3	After the initial service request message, security sensitive messages are re-sent encrypted in a Non-Access Stratum (NAS) Container so sensitive UE-specific information is not sent in the clear.
No SUPI-Based Paging	5GSC-1.4	Use a temporary identifier (5G-S-TMSI) as the basis of paging timing, not a permanent identifier (SUPI).
Respond to Identity Request with SUCI	5GSC-1.5	The network can request SUPI, but the UE only responds with SUCI and never sends SUPI.
Radio Network Security, 5GSC-2		
User Plane Integrity Protection	5GSC-2.1	Apply integrity protection to user plane traffic over the air at the full data rate using 5G's new capabilities.
Cryptographic Algorithms Recommended Practice	5GSC-2.3	Use strong algorithms for the air interface based on US operator-recommended practices.
Authentication Enhancements, 5GSC-3		
Native Extensible Authentication Protocol (EAP) Support	5GSC-3.1	Use access-agnostic authentication via EAP Method for 3rd Generation Authentication (EAP-AKA') to enable mutual authentication between the UE and the network, and to provide keying material that can be used between the UE and the serving network and between the UE and the home network in subsequent security procedures. While EAP support is new in 5G, the evolution of LTE's authentication, referred to as 5G AKA, will also be evaluated. Special EAP configurations like EAP-Transport Layer Security (EAP-TLS) are of interest for future project phases.
Non-3GPP Access	5GSC-3.2	Maintain one security context in the 5G core network for access from both 3GPP networks and non-3GPP networks, e.g., wireless local area networks (WLANs).
Hardware-Based Credential Storage	5GSC-3.3	Store pre-shared keys and credentials in the USIM software container running on tamper-resistant hardware in UEs in either embedded or physical Universal Integrated Circuit Cards (UICCs), commonly referred to as Subscriber Identity Module (SIM) cards.
Security Anchor Function (SEAF)	5GSC-3.4	The Security Anchor Function (SEAF) is collocated with the Access and Mobility Management Function (AMF) to provide primary authentication. The SEAF plays an important role in authentication while roaming and for non-3GPP access.

Security Capability	Subreference	Description
API Security, 5GSC-5		
API Security for Network Exposure Function (NEF)	5GSC-5.1	Securely expose network services such as voice, data connectivity, charging, and subscriber information to trusted (internal) and untrusted (third-party) applications over application programming interfaces (APIs), with standards defined and recommended practices for API security applied according to security profiles for Transport Layer Security (TLS) implementation and usage following the provisions given in clause 6.2 of 3GPP Technical Specification (TS) 33.210 [1].
Application Security, 5GSC-7		
Subscriber Traffic Security Monitoring	5GSC-7.1	Have complete visibility across the control and user planes. Correlate between UE traffic and permanent equipment identifiers (PEIs) and SUPIs.
User-Plane Security Enforcement	5GSC-7.2	Enforce authorized access for 5G implementing segmentation policies based on SUPI/PEI, Network Slice, Applications, and data. Provide inline network security protections for UE.
Internet Security Protocol Recommended Practice, 5GSC-8		
IPsec/NDS IP	5GSC-8.2	Protect communication between network entities/elements at the network layer via authentication and cryptographic secured Internet Protocol Security (IPsec) tunnels (e.g., communication within RAN, between RAN and core – backhaul, mid-haul and fronthaul and access from untrusted non-3GPP network to 5G core network).

3.5.3 Mitigated Threats and Vulnerabilities

Each security capability in Table 3-2 is intended to help mitigate certain types of threats and vulnerabilities so as to reduce overall risk to an acceptable level. This section explores the security capabilities in order and for each one, summarizes the vulnerabilities and corresponding threats it helps address, and briefly explains how it mitigates the threats and vulnerabilities.

3.5.3.1 Infrastructure Security

Hardware Roots of Trust Packet Core, ISC-1

ISC-1.1, Hardware-Based Platform Measurement

Threat/Vulnerability:

- Basic Input/Output System (BIOS) or firmware code could be altered or replaced with malicious code giving an attacker full control of the system (i.e., a rootkit). Additional hardware components could be added to the system to give unauthorized users access to the system or its data without the system owner's knowledge.

Mitigation:

- Hardware-based cryptographic measurements provide a mechanism to verify the integrity of the system composition. The BIOS, firmware, and connected hardware components can be measured so that the good known boot state is known, and any changes or modifications can easily be detected.

ISC-1.2, Hardware-Based Labeling

Threat/Vulnerability:

- Without any type of labeling of systems comprising a compute resource pool, virtual or containerized NF workloads can be instantiated on any host within the resource pool. Software labels are often applied to systems or sets of systems to designate them for specific workloads; however, labels are often enforced at the OS level, which can be circumvented on a compromised system.

Mitigation:

- Hardware-based labeling of systems provides unique user-defined labels applied to systems. These labels can help identify a system by any set of attributes – for example, location information and unique identifiers for specific workloads. Further, these labels, also called asset tags, are cryptographically signed and stored in tamper-resistant hardware, which can be used to demonstrate integrity and ownership of these labels.

ISC-1.3, Remote Platform Attestation

Threat/Vulnerability:

- Data centers are usually made up of thousands of servers, and keeping track of them and their respective firmware is an overwhelming task for an operator. Without centralized management of server platforms, unapproved modifications to their firmware could be made and not be detected by the data center operator.

Mitigation:

- Remote platform attestation provides the enforcement of what components are allowed to run on server platforms across all hardware systems in a data center. While ISC-1.1 and ISC-1.2 provide integrity mechanisms, they do not address centralized monitoring of all systems. The ability to verify against a collective allow list of server platforms and their associated firmware components as opposed to a local system enforcing a supply chain policy provides operators more flexibility and control in a cryptographically secured manner. These enforcement mechanisms can incorporate the hardware-based platform measurements and labeling into these security policies. Additionally, the remote attestation server can also be thought of as a Trust Broker because other services can query it to obtain the trust status of servers in the data center.

ISC-1.4, Network Function Orchestration Enforcement

Threat/Vulnerability:

- NF workloads could potentially be instantiated on, or migrated to, compute servers with vulnerabilities or disallowed firmware versions, or outside of a logical boundary.

Mitigation:

- Workload orchestration schedulers that are integrated with a Trust Broker use trust measurements and asset tags as factors of workload placement. This helps to ensure that the NF workloads are only instantiated on or migrated to compute servers with compliant trust measurements and asset tags which have their trust rooted in hardware.

ISC-1.5, Network Function Image Encryption

Threat/Vulnerability:

- Workload images are often stored in a shared storage location and can contain sensitive or proprietary information. A data breach could occur if the images are accessed or copied to another site by an unauthorized user.

Mitigation:

- NF workload images are encrypted in their shared storage location, and only compute servers that meet pre-defined security policies have access to the decryption keys when they are hosting the NF workload. This ensures that only the hosting platform can decrypt a workload image and access its information. Additionally, the security policy for access to decryption keys includes factors such as trust status and asset tag and integrates with the Trust Broker to obtain this information before releasing a decryption key.

Infrastructure Recommended Practice, ISC-3

ISC-3.1, Infrastructure Security Monitoring

Threat/Vulnerability:

- Threats to the infrastructure could include a malicious attacker or insider attempting to gain or gaining unauthorized access without being detected. Examples of attacks could include DDoS, man in the middle, privilege escalation, ransomware, behavioral anomaly detection, malware, and insider threats. Without monitoring or detection capabilities to find them, these attacks could continue to persist or worsen.

Mitigation:

- Use infrastructure security monitoring tools that allows visibility and insight into the infrastructure and help identify suspicious activities. The tools can provide an efficient way to detect and track security risks so that the organization can take preemptive actions.

ISC-3.2, Network Segmentation

Threat/Vulnerability:

- Different types of traffic traverse the 5G network, such as infrastructure operations, NF management, and user data. Without network segmentation, a regular 5G user could potentially interact with the management and operational components of the 5G network.

Mitigation:

- Network segmentation applies access controls to different portions of the 5G network. This technique creates isolated network segments for each type of traffic within the 5G network to prevent unauthorized access to other types of traffic.

3.5.3.2 5G Standalone Security

Subscriber Privacy, 5GSC-1

5GSC-1.1, Subscription Permanent Identifier (SUPI) Protection

Threat/Vulnerability:

- An International Mobile Subscriber Identity (IMSI) catcher is a type of false base station used for intercepting mobile phone subscriber identifying information. Essentially a "fake" mobile tower impersonating the service provider, it tricks a phone into sending its LTE permanent subscriber identity called IMSI. The false base station operator can use this information for tracking the location of mobile subscribers.

Mitigation:

- When used without the null cipher scheme, this 5G feature encrypts the 5G Subscription Permanent Identifier (SUPI) with the public key of the home operator to create the Subscription Concealed Identifier (SUCI). This prevents the permanent identifier (SUPI) from being sent in the clear and makes the information unusable for tracking subscribers.

5GSC-1.2, Reallocation of Temporary IDs

Threat/Vulnerability:

- In passive subscriber information attacks, malicious actors collect multiple Global Unique Temporary Identifiers (GUTIs) which can be used for different purposes. One example is to verify a subscriber’s presence in a certain area, and another is to reveal their past movements in that area and enable tracking of future movements [2]. When temporary IDs like GUTI are not refreshed frequently enough, they become quasi-permanent IDs.

Mitigation:

- This 5G feature provides consistent refreshing of a user device's temporary identifier under the following conditions: paging, initial registration, and mobility registration update procedures. The network can be configured to also allocate a new GUTI after each service request of the UE. The most secure arrangement is when a UE gets a new GUTI each time it has used its GUTI in the clear on the radio interface. This ensures that temporary IDs cannot be used for subscriber tracking.

5GSC-1.3, Initial NAS Message Security

Threat/Vulnerability:

- The lower radio technology-specific layers (e.g., communication between UE and gNB) of the communication protocol are called access stratum (AS), while the upper radio-agnostic layers (e.g., communication between UE and Core) are called non-access stratum (NAS). The initial NAS message is the first NAS message that is sent after the UE transitions from the idle state. Service Request is one kind of initial NAS message. If all parts of an initial NAS message are sent in the clear, some UE-specific information may be exploited.

Mitigation:

- 5G standards [3] mandate that when the UE has no NAS security context (i.e., it does not have valid encryption or integrity keys), it shall send a limited set of information elements (called the cleartext IEs), including those needed to establish security in the initial message. On the other hand, when the UE already has a security context (i.e., it has valid encryption or integrity keys), the UE shall send a message that has the complete initial NAS message ciphered in a NAS Container along with the cleartext IEs, with the whole message's integrity protected.

5GSC-1.4, No SUPI-Based Paging

Threat/Vulnerability:

- The network alerts a mobile for incoming calls or messages by using a paging message. In earlier generations of mobile networks, this paging message could contain the subscriber's permanent identifier. Attacks against the paging protocol can have severe repercussions. For instance, it could allow an attacker to infer a victim's location based on the victim's permanent identifier, or inject fabricated emergency alerts [4].

Mitigation:

- Before 5G, paging timing was typically determined based on a long-term (permanent) identifier (IMSI). 5G always determines paging timing based on a temporary identifier (called 5G-S-TMSI) [5]. In other words, 5G does not have SUPI-based paging.

5GSC-1.5, Respond to Identifier Request with SUCI

Threat/Vulnerability:

- In LTE, the network may request the Identity of a UE during certain procedures and specifically set the requested mobile ID type as the permanent identifier (IMSI). The UE then is required to respond with an Identity response message containing the requested IMSI in the cleartext. This could enable a false base station to retrieve the UE's permanent identity [6].

Mitigation:

- In 5G, the network cannot set the requested mobile ID type as the cleartext permanent identifier (SUPI). However, it can set the requested mobile ID type as the concealed permanent identifier (SUCI). This means that in the response message, the UE will be able to conceal its permanent identifier if the operator has enabled this security feature by configuring an appropriate SUCI scheme.

Radio Network Security, 5GSC-2

5GSC-2.1, User Plane Integrity Protection

Threat/Vulnerability:

- The integrity of the user plane traffic between the device and network was not protected in earlier generations. For example, in a known LTE attack referred to as aLTEr [7], a malicious actor can modify the message payload and can redirect DNS requests and then perform a DNS spoofing attack.

Mitigation:

- In 5G, integrity protection of the user plane between the device and the network was introduced as a new capability, complementing the existing confidentiality protection of user plane traffic. The enablement of user plane integrity protection prevents this type of threat. The support of this feature is mandatory for both the device and the network, while the use is optional and under the control of the operator.

5GSC-2.3, Cryptographic Algorithms Recommended Practice

Threat/Vulnerability:

- A network operator is limited to the cryptographic algorithms supported in the equipment deployed in its networks. If the algorithms configured for use are ever determined to be weak in some way, the system could be at risk.

Mitigation:

- 5G supports the same cryptographic algorithms that were available for use in LTE. Per 3GPP specifications the 5G network equipment is required to support an Advanced Encryption Standard (AES) based algorithm as well as a SNOW3G-based algorithm. The system supports switching between algorithms implemented in the network equipment. This switch could be triggered if the algorithm configured for use in a network is found to be weak. This brings some inherent algorithm agility to the 5G system.

Authentication Enhancements, 5GSC-3

5GSC-3.1, Native Extensible Authentication Protocol (EAP) Support

Threat/Vulnerability:

- In earlier generations, only AKA was used for primary authentication to mutually authenticate the UE and the network. The key was not bound to the serving network name. Hence various types of security issues could occur, such as a compromised serving network and/or key being used for unauthorized access, e.g., roaming, and non-roaming frauds. Refer to section 3.3 of [8] and [9].

Mitigation:

- 5G standards specify use of access-agnostic authentication using EAP-AKA' to enable mutual authentication between the UE and the network and provide keying material that can be used between the UE and the serving network in subsequent security procedures. EAP-AKA' binds the serving network name to the key, which prevents unauthorized access. EAP-AKA' is supported for both 3GPP and non-3GPP access technologies. Refer to sections 6.1.2 and 6.1.3.1 of [3] and [10]. Note that EAP-AKA' also prevents bidding down attacks to earlier versions of EAP [9].

5GSC-3.2, Non-3GPP Access

Threat/Vulnerability:

- 5G network subscribers can access 5G services via non-3GPP access networks. Non-3GPP networks, such as Wi-Fi, can be susceptible to various types of security attacks, including fake access points for hijacking legitimate user sessions and eavesdropping attacks.

Mitigation:

- A common security context is maintained in 5G core network when a UE connects from both 3GPP and non-3GPP networks. In 5G, the Non-3GPP Interworking Function (N3IWF) is used for access from untrusted non-3GPP networks. For non-3GPP accesses, IPsec tunnels can be used to protect subscriber and signaling traffic from the non-3GPP access point to the N3IWF. Refer to sections 6.3.2.2 and 7.2.1 of [3].

5GSC-3.3, Hardware-Based Credential Storage

Threat/Vulnerability:

- 5G standards specify that long-term keys and the home network public key are to be stored in the Universal Subscriber Identity Module (USIM) in the UE. The USIM is a software container running on a UICC, often referred to as a SIM card. For 5G networks that use EAP-AKA or 5G-AKA, all cryptographic keys except the SUCI encryption key in 3GPP protocols are derived from the pre-shared long-term key. A USIM can be either removable (physical SIM card) or embedded (eSIM). Long-term keys stored in the device are valuable targets to adversaries. If the keys are compromised, protected 3GPP subscriber traffic and signaling traffic can be intercepted by the adversary. Some examples of known attacks against keys are side-channel attacks. Refer to [11], [12], [13], [14], and sections 4 and 7 of [15].

Mitigation:

- Protection of the long-term key is important. Physical security of mobile devices can protect the keys from side-channel attacks. In 5G, USIMs are provisioned with a long-term, pre-shared cryptographic key referred to as K. This key is stored within the tamper-resistant USIM and within the core network (in the Authentication Credential Repository and Processing Function [ARPF]). The long-term key's confidentiality is protected within the USIM and in ARPF, and the key is never made available in the clear outside of those locations. Refer to sections 5.2.4 and 5.2.5 of [3] and section 3.2 of [8].
- Note that the same capability exists in earlier generations of 3GPP networks such as 4G.

5GSC-3.4, Security Anchor Function (SEAF)

Threat/Vulnerability:

- In earlier generations of 3GPP networks, the SEAF component was not present. In roaming scenarios, the serving network (in the visited Public Land Mobile Network [PLMN]) could make decisions about authentication of UEs. This created an attack surface where an adversary could use an untrusted serving network to fraudulently authorize UEs.

Mitigation:

- 5G introduces EAP-AKA' and 5G-AKA authentication methods using SEAF which prevent the above attacks by enabling home control of UE authentication. Authentication Server Function (AUSF) in the home PLMN makes the final decision on UE authentication. Refer to section 6.1.4 of [3] and [16].
- SEAF supports primary authentication of UE. SEAF also supports re-authentication of UE when it moves between different access networks (RANs in the same PLMN) or even serving networks (in roaming scenarios) without having to re-run the full authentication. Refer to section 6.1.2 of [3].
- SEAF holds the anchor key or the root key for each UE in both roaming and non-roaming scenarios. The anchor key is bound to the serving network name. SEAF needs to authenticate itself to the AUSF of the home network. It receives the anchor key from AUSF in home PLMN during UE's primary authentication and re-authentication procedure if authentication is successful. See section 6.1.3 of [3].

API Security, 5GSC-5

5GSC-5.1, API Security for Network Exposure Function (NEF)

Threat/Vulnerability:

- In earlier generations of 3GPP networks, security for a standardized network exposure mechanism was not defined. Even though the Service Capability Exposure Function (SCEF) was introduced in 3GPP R13 specifications to standardize third-party API access, it was mostly used for services related to narrowband Internet of Things (NB-IoT) devices. [17]
- Sensitive information in the network such as Data Network Name (DNN), Single Network Slice Selection Assistance Information (S-NSSAI), and subscriber data like SUPI may be unintentionally exposed through the N33 interface.

Mitigation:

- NEF acts as a secure gateway to trusted (internal) and untrusted third-party (external) application functions (AFs) for exposing various services such as analytics, user traffic routing, UE location, reachability, and mobility-related information. It authenticates and authorizes services requested by the AFs. 5G standards mandate integrity, replay, and confidentiality protection for communication between the NEF and AFs. 5G standards also mandate NEF to AF connection to support TLS and use of certificate-based mutual authentication between third-party AFs and NEF. NEF masks sensitive 5G network information such as DNN, S-NSSAI, and sensitive subscriber information such as SUPI from the third-party AFs. Refer to sections 5.20 and 6.2.5 of [18], section 4.15 of [19], sections 5.9.2.3 and 12 of [3], and [10]. For examples of third-party AFs, refer to section 6.2.10 of [18] and [20].

Application Security, 5GSC-7

5GSC-7.1, Subscriber Traffic Security Monitoring

Threat/Vulnerability:

- Although mobile network operators and enterprises have visibility into their mobility traffic, malicious actors can bypass an operator's detection mechanisms. This creates vulnerabilities for Network and Security Operations Centers (NOCs and SOCs, respectively) unable to detect a malicious actor's use of network resources. Infected network devices maliciously use network resources for Command-and-Control (C2) traffic, which impacts network and application performance. During security events like DDoS attacks generated from UE, security response teams aren't able to correlate botnet traffic or DDoS-related traffic to individual subscribers or equipment.

Mitigation:

- Inspecting user-plane and control-plane traffic allows for contextual visibility into network traffic. Inspecting either Packet Forwarding Control Protocol (PFCP) events or Session Management Function (SMF) messages and correlating them with General Packet Radio

Service (GPRS) Tunneling Protocol User (GTP-U) tunnels allows mapping SUPIs and PEIs to network traffic. When this information is paired with results from C2, vulnerability, anti-virus, and botnet inspection SOC and NOC analysts have a clear view of malicious users. Once this information is collected and analyzed from multiple sources and tracked over time, a clear understanding of what types of devices and users cause problems and what precipitates those problems can be established. This results in faster root cause analysis for network security incidents.

5GSC-7.2, User-Plane Security Enforcement

Threat/Vulnerability:

- Malware can be delivered by a number of mechanisms, such as embedded downloads in email or Short Message Service (SMS) content, downloads from malicious websites or applications, or even from malicious hardware.
- Malicious software installed on UE can cause a number of issues on the network. Malicious software can use the network to communicate with C2 servers, which causes congestion on the mobile network. The infected user equipment can also be used as a botnet to cause a DDoS attack against the 5G Core or network resources and applications.
- UE on the network can be used to access and exfiltrate sensitive data. UE could also be used to attack or log in to unauthorized network services. With controlled traffic, UE may also be used to access malicious websites or use unapproved software-as-a-service (SaaS) applications.

Mitigation:

- To stop malware delivery from the internet, ingress traffic must be inspected by a security appliance capable of malware analysis and file control. Using signature-based detection methods is an accurate way to detect known malware. To quickly identify unknown malware, using a multi-method approach is the most accurate, pairing static and dynamic analysis with machine learning to reduce latency and processing time.
- Inspecting user-plane traffic and analyzing it against known C2 signatures, known malicious domains, and domain generation algorithms is a great way to identify C2 traffic. Implementing a security appliance capable of detecting and preventing this type of traffic helps ensure the continuity of the network.
- The best way to protect data, applications, assets, and services is by removing implicit trust through zero trust architecture (ZTA) for 5G networks. Successful implementation of 5G ZTA requires implementing granular control policies on a Policy Enforcement Point (PEP). The PEP should inspect all user plane traffic and only allow benign traffic that supports business use cases. Granular control policies are defined with a subject complete with 5G attributes such as SUPI, PEI, application, or service. Implementing the PEP at N3 combined with data from N4 or N11 allows for correlating and enforcing policies that contain the SUPI and PEI.

Internet Security Protocol Recommended Practice, 5GSC-8

5GSC-8.2, IPsec/NDS IP

Threat/Vulnerability:

- When IPsec is not used in the 5G network, sensitive subscriber data and signaling data could be vulnerable to eavesdropping when sent unencrypted, i.e., over backhaul connections and over non-3GPP access network. Refer to [8].
- When IPsec is used with an incorrect configuration, it is possible to create an insecure connection by using weak or compromised protocols or algorithms. For example, pre-shared keys (PSK) could allow a third party to decrypt any intercepted traffic if a network is configured to use weak keys. Keys could be leaked if sent through unsecured connections or if stored unencrypted. The Internet Key Exchange version 1 (IKEv1) protocol could be vulnerable to offline dictionary attacks if a weak PSK is used. Refer to section 2.3.4 of [21] and [22]. Both IKEv1 and IKEv2 could be vulnerable to DDoS amplification attacks due to wrong protocol implementation. Refer to section 7.2.4.3 of [21] and [23].

Mitigation:

- IPsec is a suite of open standards for ensuring private communications over public networks. It is a common network-layer security control typically used to encrypt IP traffic between hosts in a network and to create a virtual private network (VPN). IPsec tunnels are used in 5G networks to provide subscriber and signaling traffic with integrity, confidentiality, and replay protection for backhaul connection and other connections, like untrusted non-3GPP network access. 3GPP standards mandate use of data integrity and anti-replay protection for IPsec. Confidentiality is optional for IPsec in certain scenarios. Refer to [24] and section 5.1 of [1]. For a complete list of recommended configuration options for IPsec and IKE protocols, refer to Table 1 of [21].
  - 5G standards specify that IPsec could be used to protect non-SBIs.

3.5.4 Industry Security References

This section will include all relevant industry references that were taken into consideration in the development of the solution. It will be added to a future draft of this volume.

4 Components of the Example Solution

This section highlights the components of the first phase of the example solution and the collaborators who are contributing those components and participating in the solution design, implementation, configuration, troubleshooting, and/or testing. More information on each component will be provided in the future in NIST SP 1800-33C, How-To Guides.

4.1 Collaborators

Collaborators that participated in this build and the capabilities of their contributions to the example solution are described briefly in the subsections below.

4.1.1 AMI

AMI provides foundational technology and security solutions so the world's machines Power Up, Stay On, and Run Secure - from on-premises to the cloud to the edge, each time, every time. AMI is a crucial provider to the Open Compute ecosystem and is a member of numerous industry associations and standards groups, such as the Unified Extensible Firmware Interface (UEFI) Forum, National Cybersecurity Excellence Partnership (NCEP), and the Trusted Computing Group (TCG). AMI's key product for this 5G build is AMI TruE, a platform attestation solution that ensures systems remain in a trusted state.

4.1.2 AT&T

AT&T is a global leader in telecommunications. Connectivity is our business through high-capacity broadband networks – fiber, 5G and wireless. AT&T has been and continues to be heavily involved in the guidance and development of 5G and cybersecurity standards with numerous industry associations, government commissions, and domestic and international standards bodies. As a result, AT&T has been ideally placed to help the NIST NCCoE succeed in the goals and objectives of this project, with expert technical contributions for the 5G network architecture design and practical implementation, including use cases and test plans. AT&T has helped NIST and its collaborators to design and implement the premier 5G testing lab – configuring and validating new equipment and software solutions.

4.1.3 CableLabs

CableLabs is the research and development lab for the global broadband cable industry, with over 60 network operator members serving approximately 200 million subscribers across five continents, with over half of its members also providing mobile services today. For over 30 years, CableLabs has developed and improved wired and wireless network technologies for the secure delivery of high-speed data, video, voice, and other next-generation services. CableLabs is also the cable industry's expert body on standards and participates in over 25 standards bodies and industry consortia globally, including in wireless, wired, and security. Relevant to this project, CableLabs has actively engaged in 3GPP Technical Specification Group Service and System Aspects Working Group 3 (SA3) and contributed to 5G security specifications and requirements.

4.1.4 Cisco

Cisco Systems is a provider of enterprise and industrial networking, security, collaboration and communications solutions. Cisco Secure Network Analytics (previously named Stealthwatch) provides visibility across the infrastructure to continuously monitor communication patterns, providing threat visibility into the extended network, to detect and respond to threats. Cisco Secure Firewall is a threat-focused, next-generation firewall with unified management. It provides advanced threat protection before, during, and after attacks. By delivering comprehensive, unified policy management of firewall functions, application control, threat prevention, and advanced malware protection from the network to the endpoint, it increases visibility and security posture while reducing risks.

4.1.5 Dell Technologies

Dell Technologies recognizes that 5G is not a standalone technology and is part of an overall data modernization effort that touches edge/Internet of Things (IoT), core data center, and cloud. Dell Technologies is working with industry leading technology partners to deliver comprehensive, flexible 5G solutions to meet next-generation telecommunications requirements.

4.1.6 Intel

Founded in 1968, Intel is an industry leader, creating world-changing technology that enables global progress and enriches lives. We stand at the brink of several technology inflections—artificial intelligence (AI), 5G network transformation, and the rise of the intelligent edge—that together will shape the future of technology. Silicon and software drive these inflections, and data is emerging as a transformational force in this era where an explosion of devices permeates all our interactions. That data must be moved, stored, and processed faster and more securely than ever before. Intel is unleashing the potential of data to unlock value for people, business, and society on a global scale.

4.1.7 Keysight Technologies

Keysight Technologies, Inc. is a leading technology company that helps its engineering, enterprise, government, and service provider customers accelerate innovation to connect and secure the world. Keysight's solutions optimize networks and bring electronic products to market faster and at a lower cost with offerings from design simulation to prototype validation, to manufacturing test, to optimization in networks and cloud environments. Keysight is committed to 5G readiness. We provide end-to-end Layer 1–7 test and precision measurement solutions to de-risk 5G development and enhance 5G network operations. As an active member of 3GPP and other wireless standards bodies, forums, and consortia, we help our customers ensure the innovations they create meet the latest cellular standards.

4.1.8 MiTAC

MiTAC Computing Technology Corporation is a professional IT solution provider, offering total solutions from edge to cloud with advanced R&D, TCO, and worldwide operations. Focusing on cloud and edge computing solutions and services, MiTAC's design and manufacturing experience spans over thirty years in servers and storage systems for CSP, CoSP, and Enterprise, and is supplemented with a record of implementing hyper scale data centers and telecommunication companies. MiTAC Computing Technology's IoT solutions provide the industry with innovative embedded products and industrial computers. MiTAC also serves the channel through TYAN Computer Corporation, a business unit of MiTAC, offering an entire spectrum of commodity-off-the-shelf whitebox servers, spanning rack and tower systems, high-performance and GPU-accelerated computing, cloud computing servers, storage systems, workstations, including complete systems and fully integrated server racks to offer customers the best total cost of ownership.

4.1.9 Nokia

Nokia Corporation, together with Nokia Bell Labs, creates technologies in the areas of communication networks, information technology, and consumer electronics. For communication networks, Nokia delivers products and solutions for 4G/5G cellular, fixed access (copper, fiber, and fixed wireless), optical transport, IP routing, and data center networks including software that goes beyond connectivity to enable self-optimizing, intelligent systems both locally and globally. This includes complete standards-based, cloud-native, and programmable standalone 5G network solutions that deliver performance and scalability from the RAN to the core. Nokia partners with communications service providers and enterprises to build commercial and mission-critical public and private networks with high performance, reliability, and security. Additionally, Nokia and Bell Labs are actively contributing to standards bodies relevant for this project such as 3GPP (including the Security working group SA3), Internet Engineering Task Force (IETF), and IETF RATS (Remote Attestation Procedures group).

4.1.10 Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, continually delivers innovation to enable secure digital transformation—even as the pace of change is accelerating. Palo Alto Networks Powered by PAN-OS®, ML-Powered Next-Generation Firewalls (NGFWs) for 5G offer the most granular visibility and control for your emerging 5G cybersecurity challenges. The Machine Learning (ML) NGFW was built for cloud agility and flexibility to meet scaling across VNF/CNFs. PAN-OS for 5G addresses security challenges with a robust, prevention-oriented security posture that takes advantage of application-layer visibility, across all layers, including user, control, and management planes.

4.1.11 Red Hat

Content will be added to a future draft of this volume.

4.1.12 T-Mobile

T-Mobile U.S. Inc. is delivering a transformative nationwide 5G network that will offer reliable connectivity for all. T-Mobile's customers benefit from its unmatched combination of value and quality, unwavering obsession with offering them the best possible service experience, and undisputable drive for disruption that creates competition and innovation in wireless and beyond. In collaboration with all the stakeholders and partners involved in this initiative, T-Mobile team participated in network design reviews of the 5G network, evaluated the various 3GPP security features and other general security capabilities, and advised how they can be securely implemented in the context of 5G. T-Mobile helped to identify a subset of the 3GPP security principles of 5G network capabilities which can be tested and validated as part of this 5G cybersecurity initiative. The collective purpose was to provide an exemplary 5G cybersecurity menu that is based on a comprehensive approach to 5G cybersecurity. Such approach includes multi-dimensional security that combines the 3GPP security features and general security capabilities and technologies in an effort to create a secure architecture for 5G networks.

4.2 Technologies

Table 4-1 lists the technologies being planned for implementation during the first phase of the project. Not all of these technologies have necessarily been acquired or deployed yet. Figure 4-1 depicts the high-level architecture within which all the technologies reside.

971 **Figure 4-1 High-Level Architecture**

972

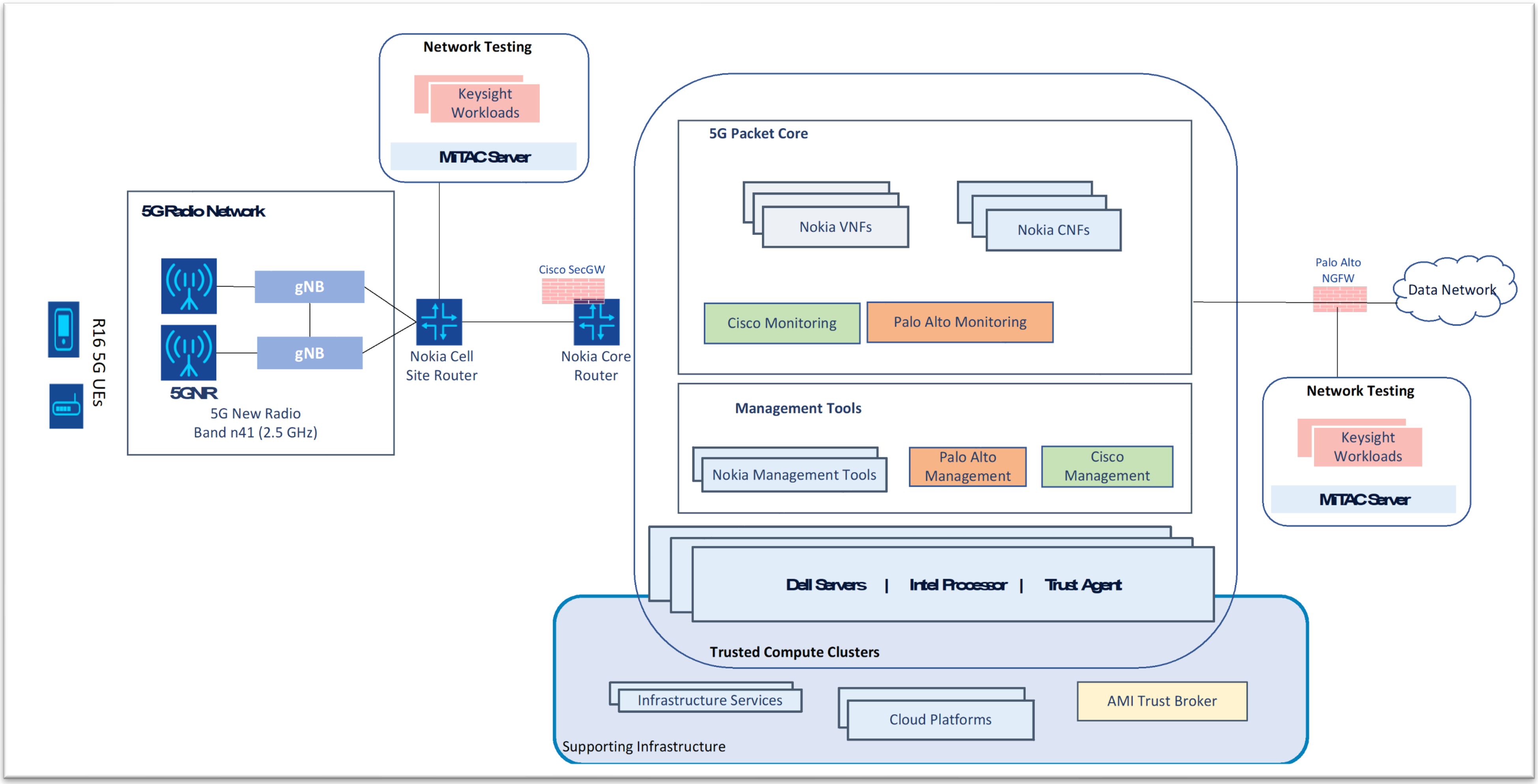


Table 4-1 Technologies

Component	Product	Functionality
Dell Servers	Dell EMC VxRail	Hyperconverged infrastructure system; provides virtualized storage, network, and compute resources to host workloads.
	Dell PowerEdge 650/750	Designed to telco-grade specifications to provide compute for evolving demands within a 5G infrastructure. Server infrastructure is designed for secure interactions and the capability to predict potential threats.
Switches	Dell EMC PowerSwitch 3048, 4048, & 5232-ON	Provides next-generation top-of-rack open networking switch capabilities to support communications transport for the 5G architecture. Leverages Dell SmartFabric OS10 for consistent DevOps framework across compute, storage, and networking elements.
Intel Processors	Intel® Xeon® Gold 5218R Processor	Provides compute for servers (i.e., central processing units [CPUs]).
	Intel Trusted Execution Technology (TXT)	Provides measured boot capabilities for secure boot. It stores the measurements in the TPM for use by attestation, workload orchestration, and policy services.
Trust Broker	AMI TruE	Verifies or attests each server’s measurements and labels against policies, feeding the results into a policy orchestrator to report, alert, or enforce rules based on the measurements.
	Intel® Security Libraries for Data Center (Intel® SecL-DC)	Implements remote attestation via open-source libraries and services.

Component	Product	Functionality
Cisco Monitoring	Cisco Secure Network Analytics (Stealthwatch)	Enables visibility across the infrastructure to continuously monitor traffic flows and provide visibility into the extended network, allowing detection of threats.
Security Gateway	Cisco Secure Firewall	Provides layer 3 and 4 stateful firewalling, which allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules and context, which refers to using information from previous connections and packets belonging to the same connection.
5G New Radio	Nokia AWHHF	2.5 GHz 5G Radio Unit (RU); acts as an access point for wireless UE interface.
gNodeB	Nokia AirScale (5G21A)	Performs baseband processing and communication with the 5G core.
Cell Site Router	Nokia 7705 SAR-8	IP router located at the cell site; does packet forwarding between the gNBs and the 5G core.
Core Router	Nokia 7750 SR-a8	IP router located at the core site; aggregates traffic from the RAN and performs packet forwarding among network elements.
Cloud Platform (for CNFs)	Nokia Container Services (NCS)	Provides a Kubernetes-based container orchestration and life-cycle management system for cloud-native network functions in the 5G core.

Component	Product	Functionality
5G Packet Core - CNFs	Nokia Cloud Mobility Manager (CMM) Nokia Cloud Mobile Gateway (CMG) Nokia Registers Nokia Policy Controller (NPC) Nokia Network Resource Discovery (NRD) Nokia Telecom Application Server (TAS) Nokia Network Exposure Function (NEF)	CNFs; provide the enabling functionality of the 5G core including access and mobility management (CMM), session management (CMG), user authentication and authorization (Registers), policy enforcement (NPC), slice management (NRD), and communication services such as (over-the-top) voice, messaging (TAS), and data streaming. It also provides an API for external applications to access certain network state information for value-added operator and user benefits (NEF).
5G Packet Core - VNFs	Nokia Shared Data Layer (SDL)	Supports multiple network functions by being a single logical repository of user data including profile, authentication data, authorized services, and policy-impacting data.
Nokia Management Tools – Network Functions	Nokia NetAct Nokia Network Services Platform (NSP) Nokia Zero Touch Service (ZTS) tools Nokia CloudBand Applications Manager (CBAM)	Provides operations, administration, and management (OA&M) functionality for each of the network functions in the 5G system. Includes element management systems (NetAct and NSP), CNF-specific zero-touch services (ZTS), and a virtual network function manager (CBAM).
Nokia Management Tools – Security	Nokia NetGuard Certificate Manager (NCM) Nokia NetGuard Identity Access Manager (NIAM)	Select applications from the Nokia NetGuard suite; provide essential security functions including certificate management (NCM) and user identity management and access (NIAM) to the 5G system.
Palo Alto Monitoring	VM-Series N3/N4	Stateful NGFW; performs layer 7 inspection and threat protection of N3, N4 interfaces.
PAN NGFW	VM-Series N6 Gateway	Stateful NGFW; performs layer 7 inspection and threat protection of N6 interfaces.

Component	Product	Functionality
Palo Alto Management	Panorama	Provides centralized logging and management of configurations, software, signatures, and licenses.
MiTAC Servers	MiTAC Aowanda	Computing platform with AMI firmware and BIOS to support trusted compute clusters.
MiTAC Server	MiTAC Thunder SX TN76-B7102	Computing platform to support networking testing workloads.
Keysight Workloads	Keysight LoadCore	Test solution product; simulates 5G traffic, enabling testing of functionality, performance, security, and reliability of mobile services on 5G core networks.

4.3 System Architecture Components

This section describes all of the components that make up the system architecture and provides information regarding their operation and roles in demonstrating the security capabilities.

4.3.1 Dell Technologies

Dell Technologies has leveraged its hardware that is designed to telco-grade specifications and is leveraging validated configurations to support the Nokia software elements to deliver critical hardware components within the infrastructure.

- **Dell PowerEdge 650/750 servers** host the virtual software elements across the 5G architecture. The PowerEdge servers address evolving compute demands with a highly scalable platform engineered to optimize the latest technology advances across processors, memory, networking, storage, and accelerators.
- **Dell EMC PowerSwitch 3048, 4048, and 5232-ON switches** support the networking requirements within the 5G architecture.
- The Open Automation Framework takes full advantage of **Dell Networking Operating System OS10 software capabilities** to bring network automation into virtual data center environments. This helps the switches efficiently respond and adapt to changes in application requirements.
- The **Dell PowerEdge servers and Dell EMC PowerSwitch solutions** provide comprehensive supply chain assurance capabilities via Dell Technologies comprehensive supply chain assurance practices and the implementation of Secure Component Validation capabilities to ensure component integrity through the shipping and delivery process. The Dell PowerEdge

servers also implement industry leading secure boot capabilities and BIOS and firmware validation capabilities.

4.3.2 MiTAC Computing Technology Corporation

Shown in Figure 4-2, the MiTAC Aowanda edge server is a server platform from the OCP Open Edge portfolio for 5G applications. The server provides commercial off-the-shelf (COTS) hardware to enable CU and DU hardware solution for next-generation 5G NR base station for fast mobile internet and wide ranges of applications. Its compact form factor and power-efficient design are ideal for telecom operators deploying vRAN and O-RAN. Aowanda server is a 2U server with three nodes. Each node has one CPU socket to support a 3rd Generation Intel Xeon Scalable processor, which supports Intel® hardware-based security features. Aowanda server enables TPM 2.0 design for the security of cryptographic keys and cryptographic processors, which can be leveraged to implement the hardware roots of trust capabilities for this project. Additionally, Aowanda has AMI BIOS and firmware on its system which can help automate the deployment of the security capabilities through integration with the AMI TruE services. These features will allow the Aowanda server to be used as a node in a Trusted Compute Cluster in the project deployment.

Figure 4-2 MiTAC Aowanda edge server

The MiTAC TYAN TN76-B7102 is a 2U, two-socket, general-purpose server that supports 2nd Generation Intel Xeon Scalable processors for computing and virtualization. Figure 4-3 depicts the server. NVIDIA EGX provides low-latency AI computing at the edge with an advanced, light-compute platform, reducing the amount of data that needs to be pushed to the cloud. The server is certificated with EGX platform for enterprises to efficiently process and respond to data. The platform is being used in the NCCoE 5G network to host the Keysight 5G simulation and testing tools.

Figure 4-3 MiTAC TYAN TN76-B7102 general-purpose server

4.3.3 Intel Hardware Root of Trust Technologies

Intel secure boot technologies including Intel Boot Guard and Intel TXT provide the hardware root of trust enabling platform integrity for each server in the infrastructure. They measure server firmware and software components during system launch so server configurations can be verified against tampering. Extending this chain of trust, additional software components, hypervisors, virtual machines (VMs), and containers can be similarly attested and verified by trust agents in the infrastructure.

The TPM included in the server infrastructure supports the assignment of specific labels for each server in the infrastructure using hardware-based controls enabled by Intel SecL-DC (Intel® Security Libraries for Data Center). Then trust agents can verify and attest each server's measurements and labels against policies, and feed the results into a policy orchestrator to report, alert, or enforce rules based on the events.

4.3.4 AMI TruE

The example solution's Trust Broker, AMI® TruE® (also known as AMI Trusted Environment), is AMI's security management solution designed to manage data center and edge infrastructure hardware resources. The backend application services discover and collect resource information from lower-level hardware layers and expose them via an intuitive web-based user interface. Administrators can also perform administrative operations such as overriding the boot source, provisioning, and power operations. AMI TruE provides platform security management that includes platform attestation, asset tag deployment, workload confidentiality, launch time protection, and more.

AMI TruE has a set of services and tools to enable remote platform attestation capabilities:

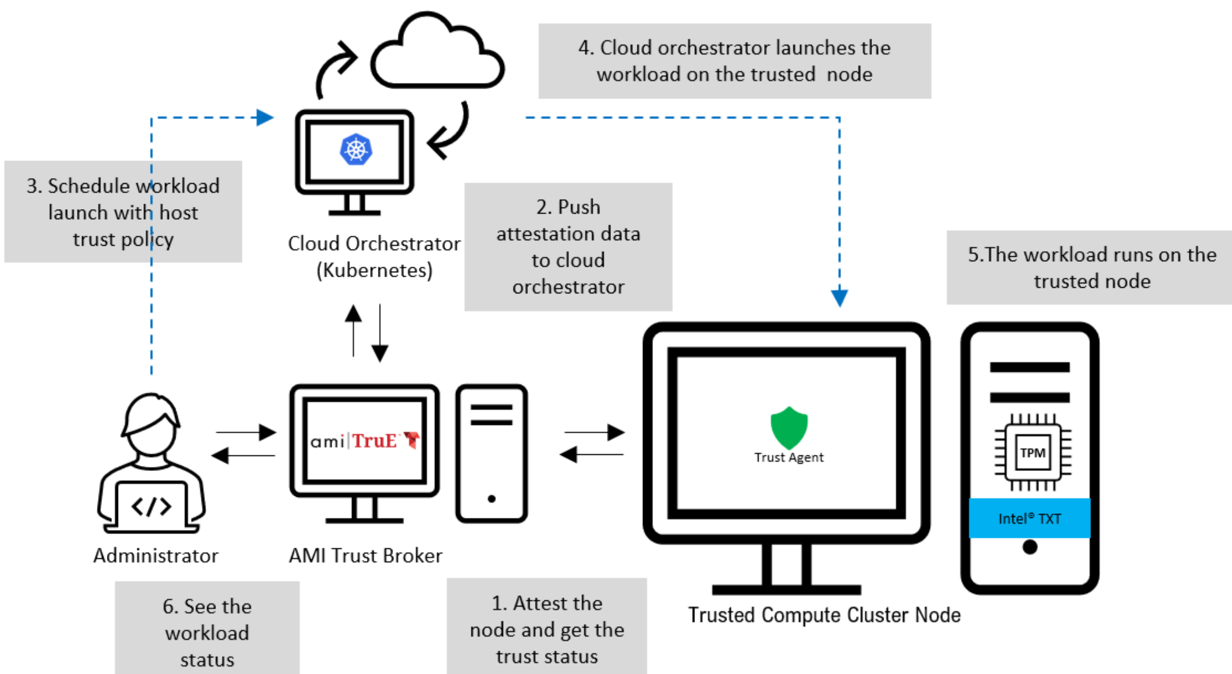
- AMI TruE Management Services includes service and tools required for the core management capabilities like API server, database libraries, utilities, account service, event service, log service, notification service, web user interface, etc.
- AMI TruE Platform Security Services are built using Intel I-SecL libraries. They provide tools and services for the foundational security. Certificate Management Service, Authentication and Authorization Service, Host Verification Service, Platform Security API Service, and

integration hub are the services included in the platform security artifacts. They can also push security status data to an orchestration layer like Kubernetes. Using this information, the Kubernetes scheduler will make launch-time decisions to choose a suitable host for each workload to be launched.

- AMI TruE requires its Platform Security Agent to be deployed on the target host to enable and monitor the platform security capabilities. This agent collects and sends the platform measurements on request from the host verification service. The agent should be installed on the physical host in the trusted computing cluster infrastructure.

Figure 4-4 depicts several of AMI TruE's capabilities and explains how they work together for remote platform attestation and workload placement purposes.

Figure 4-4 AMI TruE



4.3.5 Network Infrastructure

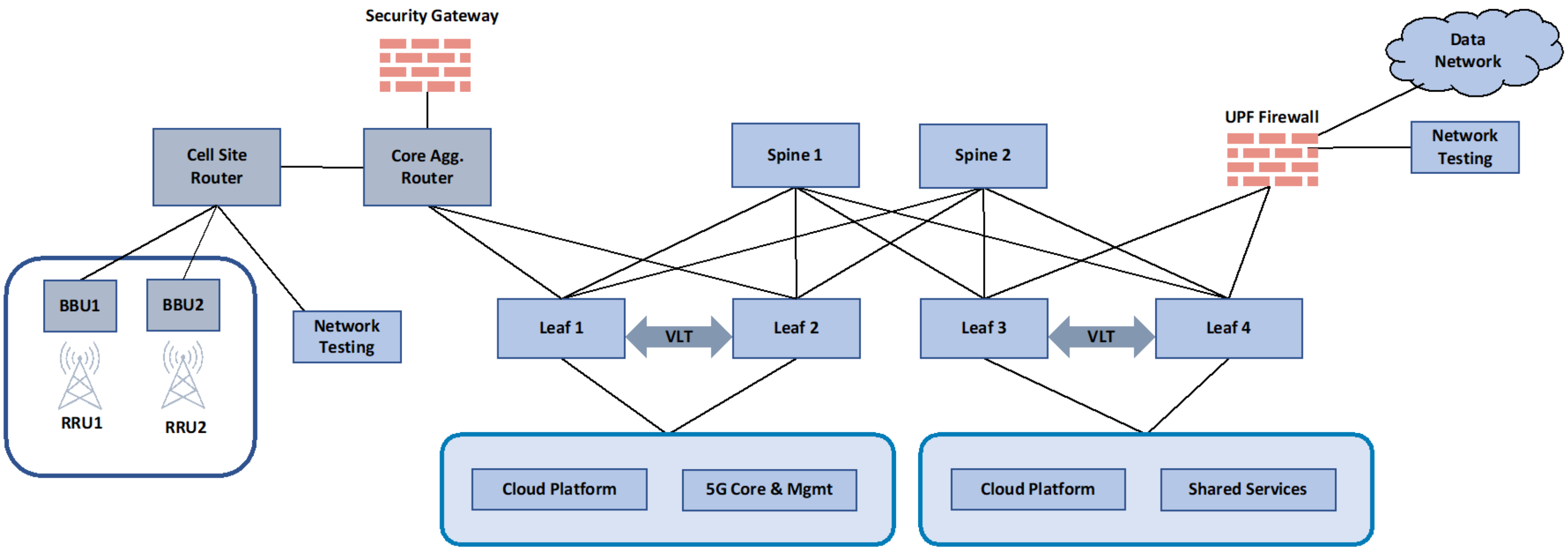
The network infrastructure supporting NCCoE's 5G system uses a spine-leaf architecture. It includes two spine switches with 40 GbE capabilities, two leaf switches with 100 GbE capabilities, and two leaf switches with 40 GbE capabilities. Each leaf switch connects to each spine switch to ensure that all leaf switches are no more than one hop away from one another; this characteristic of the spine-leaf architecture minimizes latency and increases efficiency. The two leaf switch pairs, Leaf 1 and 2 as well as

Leaf 3 and 4, use Virtual Link Trunking (VLT), allowing all connections to be active while also providing fault tolerance.

As depicted in Figure 4-5, the servers and storage are directly connected to the leaf switches. Additionally, Leaf 1 and 2 provide connectivity to the RAN through a core aggregate router. The Cisco Security Gateway is expected to be connected to the Core Aggregate Router terminating the IPsec tunnel from the 5G base band units. The Keysight testing device is connected to the Cell Site router. Also, Leaf 3 and 4 are connected to the Palo Alto firewalls for connectivity to the internet, data network, and Keysight's testing devices.

Link Aggregation Groups (LAGs) are used in a network to provide either increased link capacity or redundancy. For the backhaul connection in this project, a LAG is used between the cell site router and core aggregation router consisting of 2 x 1GE links. It is configured to use the default port threshold behavior whereby all member ports must become inactive for the LAG to be declared down.

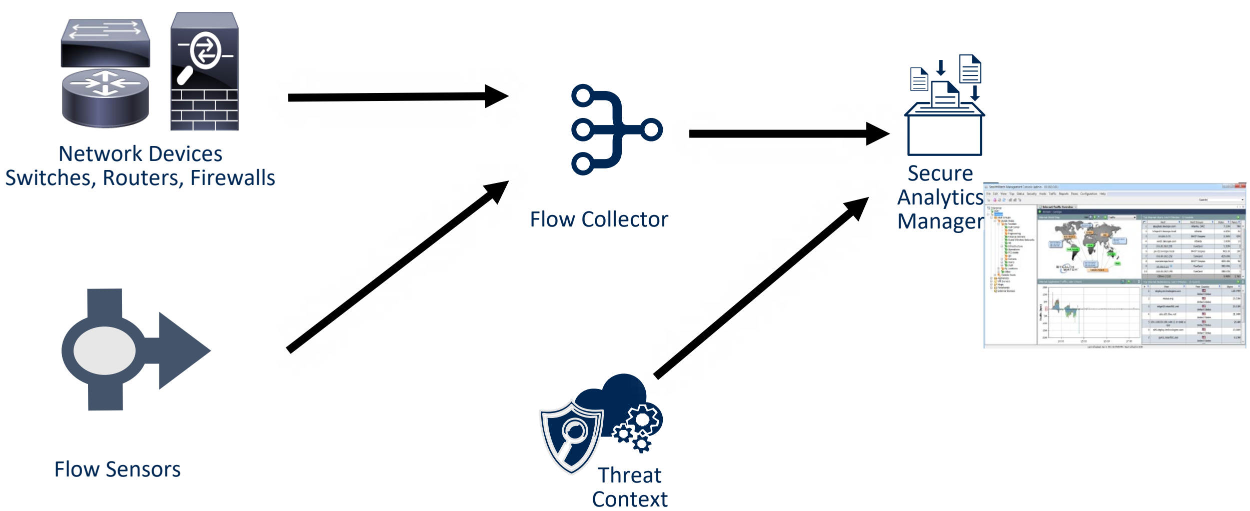
1073 **Figure 4-5 NCCoE Lab Network Infrastructure**



4.3.6 Cisco Secure Network Analytics (formerly known as Stealthwatch)

Cisco Secure Network Analytics (formerly known as Stealthwatch) enables visibility across the infrastructure to continuously monitor communications patterns, provide threat visibility into the extended network, and detect and respond to threats using methods such as behavioral modeling and machine learning. For example, behavioral modeling monitors network activity and creates a baseline of normal behavior, correlates incidents, and generates contextual alarms. Machine learning discovers advanced threats and malicious communications.

Figure 4-6 Cisco Secure Network Analytics Components



This network analysis solution consists of a Manager, Network Flow Collectors, and Flow Sensors. Figure 4-6 depicts their architecture.

The **Secure Network Analytics Manager** aggregates, organizes, and presents analyses from up to 25 Flow Collectors and other sources. It uses graphical representations of network traffic, identity information, customized summary reports, and integrated security and network intelligence for comprehensive analysis. Capabilities of the Manager include:

- **Real-time, up-to-the-minute data** - Delivers data flow monitoring traffic so that you can spot suspicious network behavior.
- **Capability to detect and prioritize security threats** - Rapidly detects and prioritizes security threats, pinpoints network misuse and suboptimal performance, and manages event response, all from a single control center.
- **Management of appliances** - Configures, coordinates, and manages Cisco Network Analytics appliances, including the Flow Collector and Flow Sensor.

- **Use of multiple types of flow data** - Consumes multiple types of flow data, including NetFlow, Internet Protocol Flow Information Export (IPFIX), and sFlow.
- **Audit trails for network transactions** - Provides a complete audit trail of all network transactions for more effective forensic investigations.
- **Real-time, customizable relational flow maps** - Provides graphical views of the current state of the organization's traffic. Administrators can construct maps of their network based on any criteria, such as location, function, or virtual environment. Operators can quickly analyze network traffic. Then, by selecting a data point in question, they can gain deeper insight into what is happening at any point in time.

The **Flow Collector** collects and stores enterprise telemetry types such as NetFlow, IPFIX, Node Version Manager (NVM), and syslog from existing routers, switches, firewalls, endpoints, and other network infrastructure devices. The Flow Collector can also collect telemetry from proxy data sources, which can be analyzed by the cloud-based machine learning engine (global threat alerts). The telemetry data is analyzed to provide a complete picture of network activity. Months or even years of data can be stored, creating an audit trail that can be used to improve forensic investigations and compliance initiatives. The volume of telemetry that can be collected from the network is determined by the total combined capacity of the deployed Flow Collectors. Capabilities of the Flow Collector include:

- **Threat detections** - Ingests proxy records and associates them with flow records to deliver the user application and URL information for each flow to increase contextual awareness. This process enhances your organization's ability to pinpoint threats and shortens your Mean Time to Know (MTTK).
- **Flow traffic monitoring** - Monitors flow traffic across network segments simultaneously so that you can spot suspicious network behavior.
- **Deduplication and stitching** - Performs deduplication so that any flows that might have traversed more than one router are counted only once. It then stitches the flow information together for complete visibility of a network transaction.

The **Flow Sensor** produces telemetry for segments of the switching and routing infrastructure that can't generate NetFlow natively. It also provides visibility into the application layer data. In addition to all the telemetry collected by Secure Network Analytics, the Flow Sensor provides additional security context to enhance the security analytics. The Flow Sensor can also generate enhanced encrypted traffic analytics telemetry to be able to analyze encrypted traffic. Advanced behavioral modeling and cloud-based, multilayered machine learning is applied to this dataset to detect advanced threats and perform faster investigations.

Each Flow Sensor is installed on a mirroring port or network tap and generates telemetry based on the observed traffic. Flow Sensors are also available as virtual appliances to monitor virtual machine environments. They also work in environments where an overlay monitoring solution requiring additional security context better fits the operations model of the IT organization. Capabilities of the Flow Sensor include:

- **Layer 7 application visibility** - Provides true Layer 7 application visibility by gathering application information. This includes data features like Round Trip Time (RTT), Server Response Time (SRT), and retransmissions.
- **Packet-level performance and analysis** – Provides packet-level metrics such as HTTP/HTTPS header data and packet payload.
- **Alerts on network anomalies** - Additional telemetry from the Flow Sensor, such as URL information for web traffic and TCP flag detail, helps generate alarms with contextual intelligence so that security personnel can take quick action and mitigate damage.

4.3.7 Cisco Secure Firewall (Security Gateway)

Cisco Secure Firewall is a layer 3,4 stateful firewall being used to provide IPsec for the network's backhaul connection in accordance with 3GPP specifications. The device allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. It enforces filtering decisions based on both administrator-defined rules and context. Capabilities relevant to the example solution include:

- **Cisco Secure Workload integration** - Enables visibility and policy enforcement for modern distributed and dynamic applications across the network and workload for consistent enforcement in a scalable manner.
- **Dynamic policies support** - Dynamic attributes support VMware, Amazon Web Services (AWS), and Azure tags for situations where static IP addresses are not available, as well as tag-based policies with Security Group Tags (SGTs) and Cisco Identity Services Engine (ISE) attribute support.
- **Snort 3 Next-Generation Intrusion Prevention System** – Provides threat protection to help improve detection, simplify customization, and enhance performance.
- **TLS Server Identity and Discovery** - Maintains Layer 7 policies on encrypted TLS 1.3 traffic. Provides visibility and control in an encrypted world where it's not realistic to decrypt and inspect every traffic flow.
- **Cisco Security Analytics and Logging (SAL)** – Provides on-premises and cloud-based firewall log management with behavioral analysis for real-time threat detection.

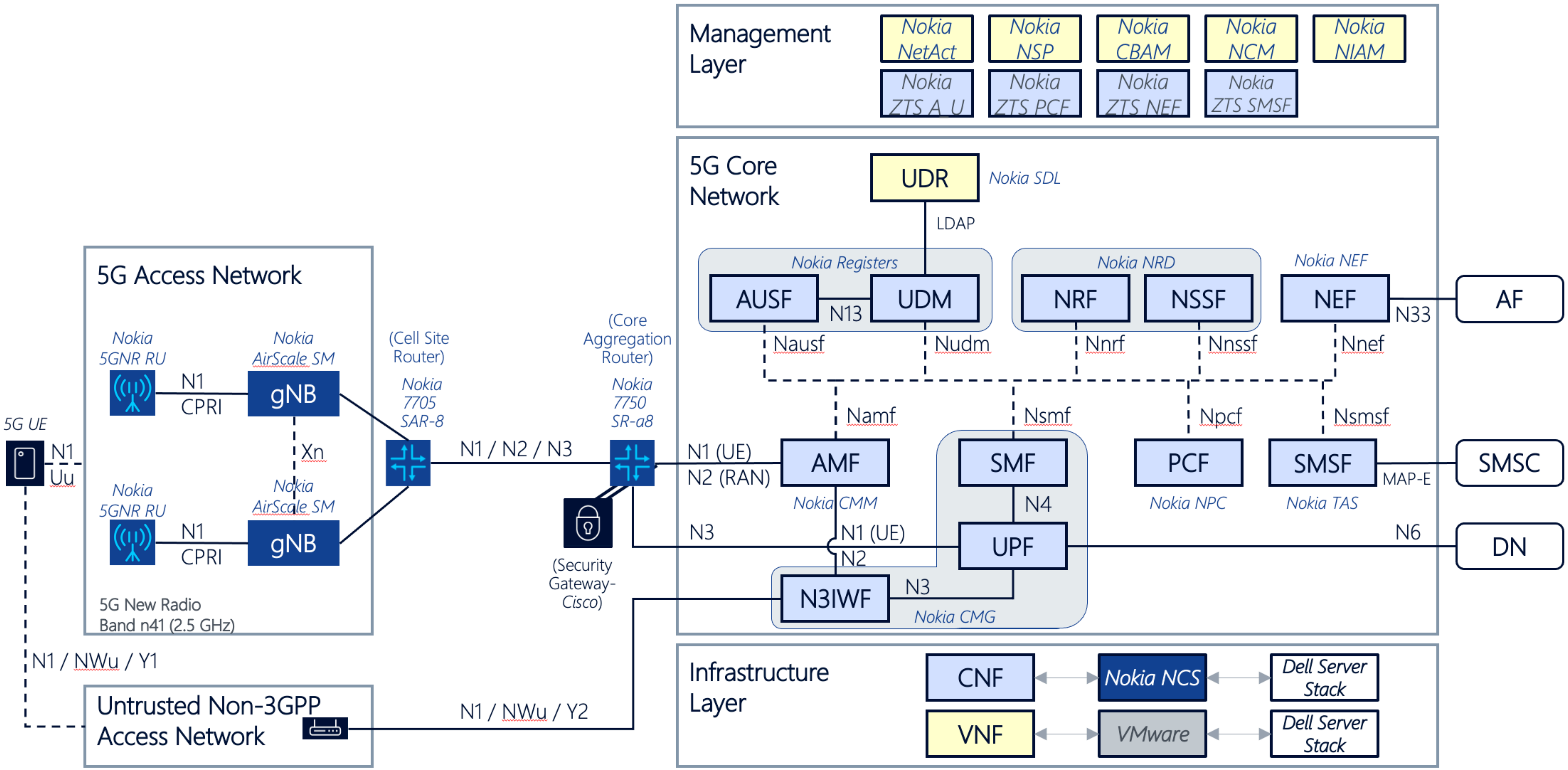
4.3.8 Nokia (5G System)

Nokia is providing a complete 5G mobile system for the project including the 5G base stations, backhaul transport, and 5G core network functions. For 5th generation mobile systems, several architecture options are defined by the telecommunications industry [25], [26]. The system being provided has a standalone architecture with classical base stations (no CU/DU split). In this architecture, the 5G New

Radio and physical base stations are supported with a 5G packet core which, for this solution, is hosted in a hybrid containerized/virtualized cloud. The system is compliant with 3GPP Release 15 standards [27], [28]. In particular, the deployed release encompasses the 3GPP standards-based security features targeted for investigation in this project.

The focus of this project is demonstrating security capabilities of commercial 5G systems. Given that focus, other characteristics of mobile systems such as capacity, performance, QoS, and resiliency are not in scope, so the provided system was architected accordingly to reduce cost and footprint. Initially, the project is focusing on non-roaming scenarios. A high-level depiction of the initial 5G system provided is shown in Figure 4-7. The acronyms for 3GPP network functions are in bold black letters, while associated Nokia product names are italicized. Selected 5G Service-Based Architecture interfaces and 3GPP reference points are indicated. The components comprising this system are described after the figure.

1178 **Figure 4-7 5G Standalone system architecture**



4.3.8.1 5G Access Network

Access for the Nokia 5G system is provided by two gNodeB systems configured as classical AirScale Base Stations. The AirScale Base Station is a compact modular system that is easy to install and grow. It also provides the flexibility to run all radio technologies and support all network topologies, including Cloud RAN. Each of the provided base stations has the minimum modular configuration as follows:

- **Radio**: Nokia AirScale Indoor Radio System (ASiR) pico-cell solution Remote Radio Head (pRRH) cmWave 5G RF System
    - ASiR-pRRH n41 (band n41, 2496 – 2690 MHz), Model AWHHF
- **Chassis**: Nokia AirScale System Module
    - AirScale Indoor Subrack (model AMIA)
    - AirScale Common Unit for 5G (model ASIK)
    - AirScale Capacity Unit for 5G (model ABIL)
- **Software**: Nokia gNodeB release 5G21A

The 5G New Radio chosen for the project is a single band (vs multiband) RU. It has an RF output power of up to 20W per transmit path with up to 4 transmit paths and supports NR carrier bandwidths up to 100 MHz and multiple modulation schemes.

The Nokia AirScale 5G System Module (SM) provides control and baseband functions for the supported radio access technologies. The ASIK Unit hosts non-real-time (NRT) functions whereas the ABIL unit hosts the (RT) real-time functions. The basic functionalities of the AirScale SM are:

- Baseband processing and decentralized control
- Central radio interface control (Radio Resource Controller [RRC])
- Packet Data Convergence Protocol (PDCP) services
- Open Base Station Architecture Initiative (OBSAI), Common Public Radio Interface (CPRI), or Enhanced CPRI (eCPRI) compatible interfaces to radio units
- Transport control, integrated Ethernet ports, and IPv4/v6 and IPSec transport
- Base Transceiver Station (BTS) clock and timing generation and distribution
- BTS operation and maintenance

The fronthaul implemented between the 5G NR and the ABIL unit is a single CPRI interface. It is optically connected at 9.8 Gbps.

5G security features for the access network follow the relevant 3GPP 5G standards (e.g., TS 33.501 [3], TS 38.323). In the project architecture, PDCP services are provided in the AirScale SM ASIK unit, including the PDCP session and bearer configuration. Thus, AS security between the UE and RRC hosted in the AirScale SM includes the key derivation function for PDCP session key generation. The user plane security between the UE and the AirScale SM includes the algorithms for cipher and integrity protection. NAS security between the UE and the 5G core network is transparent to the RAN. For backhaul transport security, IPsec tunnel connections are terminated at the gNBs by the Airscale SM (ASIK) and at the 5G core by a compatible IPsec Security Gateway (SEG).

The Access Network component is expected to enable the following security capability demonstrations:

- 5GSC-1.1, Subscription Permanent Identifier (SUPI) Protection
- 5GSC-1.2, Reallocation of Temporary IDs
- 5GSC-1.3, Initial NAS Message Security
- 5GSC-1.4, No SUPI-Based Paging
- 5GSC-1.5, Respond to Identity Request with SUCI
- 5GSC-2.1, User Plane Integrity Protection
- 5GSC-2.3, Cryptographic Algorithms Recommended Practice
- 5GSC-8.2, IPsec/NDS IP

4.3.8.2 Backhaul Transport Components

Backhaul transport between the gNB cell sites and the 5G Core Network is provided by the Nokia 7705 SAR8v2 Service Aggregation Router at the cell site and the Nokia 7750 SR-a8 Service Router as a core aggregation router at the cloud location.

The Cell Site Router, 7705 SAR-8, is a flexible service traffic aggregator for transport and connects all cell site traffic to the Core Aggregation Router. It is equipped with two line cards, each with 8 x 1 Gigabit Ethernet (GE) small form-factor pluggable (SFP) v3 ports. Among the security features the 7705 supports are IPSec, public key infrastructure (PKI), and centralized key management.

The Core Aggregation Router, 7750 SR-a8, is a 200 Gbps full-duplex router that connects to the Cell Site Router for backhaul and also to certain leaf switches in the 5G core data center network. It is equipped with four line cards: two with 10 x 10GE SFP+ ports and two with 44 x 1GE SFP ports. The 7750 family of routers can provide security gateway (SEG) functionality or can optionally interface to a third party SEG. For this project, Nokia opted to utilize a security gateway from a project collaborator, demonstrating the ability of the AirScale gNB to support IPSec tunnels to a compliant SEG.

The backhaul transport component is expected to enable the following security capability demonstrations:

- 5GSC-1.1, Subscription Permanent Identifier (SUPI) Protection
- 5GSC-1.3, Initial NAS Message Security

- 5GSC-1.5, Respond to Identity Request with SUCI
- 5GSC-8.2, IPsec/NDS IP

4.3.8.3 5G Core

The heart and brains of the 5G system is the Nokia 5G Core (5GC). As shown in Figure 4-7, the 5GC is primarily containerized, consisting of cloud-native network functions deployed in the Nokia Container Services cloud infrastructure based on Kubernetes (see next section). One NF is virtualized and is deployed in a VMware-based cloud. The 3GPP network functions comprising the 5GC are described below, including the association with the corresponding Nokia product, as shown in Figure 4-7.

- AMF (Access and Mobility Management Function) - The AMF is a pure control element in a flat network architecture that handles connection and mobility management tasks. It terminates the N1 reference point from the UE for NAS ciphering and integrity protection and N2 reference point for the RAN control plane interface. The AMF also provides session management message (SM) transport and acts as a transparent proxy for SM messages between the UE and the SMF. It is collocated with SEAF and participates in the NAS Authentication, ciphering, and integrity protection security setup with the AUSF/UDM (see below).
    - *Nokia Product: Cloud Mobility Manager (CMM)*
- SMF (Session Management Function) - The SMF handles session establishment, modification, and release, including tunnel maintenance between the UPF and RAN nodes. It communicates control instructions to the UPF over the interfaces of the N4 reference point using PFCP.
    - *Nokia Product: Cloud Mobile Gateway (CMG)*
- UPF (User Plane Function) - The UPF acts as an external protocol data unit (PDU) Session point of interconnect to the data network. The key tasks of the UPF include packet routing and forwarding, packet inspection, and the user plane part of policy rule enforcement, e.g., gating, redirection, and traffic steering as well as quality of service (QoS) handling for the user plane.
    - *Nokia Product: Cloud Mobile Gateway (CMG)*
- N3IWF (non-3GPP Interworking Function) - The N3IWF is the 5G network access point of Wi-Fi UEs and behaves similarly to a gNB but supports non-3GPP untrusted access (Wi-Fi) to the 5G core network. An IPsec session is established over the WLAN from the UE, and the N3IWF communicates with the AMF to authenticate the UE and establish an internet bearer.
    - *Nokia Product: Cloud Mobile Gateway (CMG)*
- NRF (Network Repository Function) - The NRF supports the service discovery function for the 5G service-based architecture. It receives the network function (NF) discovery requests from different NF instances, and provides information about the discovered NF instances to

the requestor. NRF maintains the NF profile of available NF instances and their supported services.

  - *Nokia Product: Network Repository Directory (NRD)*

- NSSF (Network Slice Selection Function) - The NSSF function selects the set of Network Slice instances for serving a UE, determines the set of allowed/configured slice IDs (NSSAIs), and, if needed, maps them to the Subscribed IDs (S-NSSAIs). NSSF also determines the AMF Set (when there are multiple AMF instances) to be used to serve the UE.
  - *Nokia Product: Network Repository Directory (NRD)*
- PCF (Policy Control Function) – The PCF manages user plane policies, such as QoS and data rate limits for subscribers.
  - *Nokia Product: Nokia Policy Controller (NPC)*
- SMSF (Short Message Service Function) – The SMSF supports the transfer of SMS over NAS. The SMSF conducts subscription checking and performs a relay function between the device and the SMSC (Short Message Service Center) through interaction with the AMF.
  - *Nokia Product: Telecom Application Server (TAS)*
- NEF (Network Exposure Function) – The NEF provides a secure northbound API for 3rd party applications to access the 5G network information and state. For example, applications can be notified about UE state changes or manage IoT devices or be notified of QoS for PCF modifications.
  - *Nokia Product: Network Exposure Function (NEF)*
- UDR (Unified Data Repository) – The UDR is a single logical repository that stores user and configuration data for 5G network functions, such as UDM, AUSF, and PCF. It is a cloud native database for TelCo cloud applications that is distributed to ensure availability. In this project, it is deployed as a VNF.
  - *Nokia Product: Shared Data Layer (SDL)*
- UDM (Unified Data Management) - The UDM is the main data storage for all subscriber and service-related data. This data includes user identities, SUPIs, registration information, access parameters and service-triggering information. It also processes credentials for NAS Authentication using 5G-AKA or EAP-AKA’.
  - *Nokia Product: Nokia Registers*
- AUSF (Authentication Server Function) - The AUSF supports authentication for 3GPP access, but it relies on backend processing with the UDM for computing authentication data and keys.
  - *Nokia Product: Nokia Registers*

The 5G Core component is expected to enable the following security capability demonstrations:

- 5GSC-1.1, Subscription Permanent Identifier (SUPI) Protection
- 5GSC-1.2, Reallocation of Temporary IDs
- 5GSC-1.3, Initial NAS Message Security
- 5GSC-1.5, Respond to Identity Request with SUCI
- 5GSC-3.1, Native Extensible Authentication Protocol (EAP) Support
- 5GSC-3.2, Non-3GPP Access
- 5GSC-3.4, Security Anchor Function (SEAF)
- 5GSC-5.1, API Security for Network Exposure Function (NEF)

4.3.8.4 User Services

5G networks can enable a broad range of telecommunication services in addition to traditional voice, basic text messaging, and web access services. For this project, the user services the deployed network provides are voice, data access and streaming, and SMS text messages. Slices for the network are enhanced mobile broadband (eMBB) slices and will host data flow services.

Voice services can be provided in several ways in 5G systems (see, e.g., [29]). One approach is based on the IP Multimedia Core Network Subsystem (IMS) standard developed by 3GPP [30]. IMS is the basis of the 4G voice over LTE (VoLTE) and voice over 5G (Vo5G) services. In this project, to reduce cost, complexity, and footprint, IMS was not deployed. Instead, voice calls will be Voice-over-IP (VoIP) calls using the data network (DN) connection. These are user plane calls between a VoIP-capable application on a UE and a corresponding application server in the DN.

Data access and streaming, like the VoIP services, are provided as data flows over-the-top in the user plane between UE applications and corresponding application servers (e.g., a video server) hosted in the DN.

SMS text messages in smartphone UEs typically are sent using IMS in Session Initiation Protocol (SIP) MESSAGEs. However, since many IoT devices don't support voice calls and therefore don't need to register to IMS, the Nokia TAS supports an alternate method for SMS messaging: SMS over 5G NAS (the N1 reference point shown in Figure 4-7). In this case, SMS messages are sent over the NAS and the AMF forwards them directly to the SMSF which, in turn, forwards them to the SMSC, a compliant SMS communications server. Since in this project no IMS was deployed, the SMS over 5G NAS method is used for SMS messages. The basic interface functionality of the SMSC is provided separately by a project collaborator to complete the SMS infrastructure.

4.3.8.5 Cloud Infrastructure

With one exception (Nokia SDL), the 5G Core consists of cloud-native network functions as containers. The cloud infrastructure orchestrating the containerized core is the Nokia Container Services (NCS), a platform providing Container-as-a-Service (CaaS) functionality for the on-premises deployment of containerized applications in cloud environments. It leverages Kubernetes as a container orchestration system to support shared infrastructure deployment methods and life cycle management for software applications that are composed as microservices running in Docker or other container infrastructures. It supports multiple container runtime options and it leverages Kubernetes pluggable interfaces for networking and storage integration and Helm for package management.

For the 5G core in this project, NCS is deployed on bare metal servers, also known as cluster nodes. Cluster nodes are the base resources in an NCS cluster. Four node roles were designed in NCS: Master, Worker, Edge, and Storage. A node role is a tag or label for a node, and it is captured by cluster deploy scripts to assign the corresponding resources to the target node.

- A **Master node** is designed to bind to the public OA&M network, and it is an add-on of the generic Kubernetes master.
- A **Worker node** is equivalent to the generic Kubernetes node, which is designed to run applications.
- An **Edge node** is designed to interface with an external network, and it provides a proxy for data traffic in and out of the NCS cluster.
- A **Storage role** is optional. It is only required when using persistent storage so that extra storage will be mounted to the target Master node. The Storage role can be used alone or in combination with the Master, Worker, or Edge role. If the node is assigned with a Storage role only, the node is a dedicated **Storage node**.

The Cloud Infrastructure component is expected to enable the following security capability demonstrations:

- ISC-1.4, Network Function Orchestration Enforcement
- ISC-1.5, Network Function Image Encryption

4.3.8.6 Network Management Applications

There are several Nokia applications needed for network management systems (NMS), element management systems (EMS), lifecycle management, and security. These applications are not in scope for the planned security capability demonstrations but are nevertheless needed for operation, management, and security of the Nokia 5G solution. The management applications are discussed in this section.

Nokia NetAct is a new generation network management system for multi-vendor and multi-technology networks. NetAct can serve both as an NMS and as a RAN EMS. NetAct provides southbound interfaces for integration with Nokia's and other vendors' network elements and can act as an EMS when it manages elements from a single domain. NetAct can also act in the role of a Domain Manager between the Element Management and Network Management layers when it is managing elements from various domains from a single vendor. In this project, NetAct is employed primarily as an element manager for the RAN components, but it also acts as a domain management system. As such, it provides centralized fault notifications from across the solution as well as performance monitoring for select network functions.

Nokia Network Services Platform (NSP) is a powerful suite of transport network tools. This project is utilizing the NSP Network Functions Manager for Packet (NFM-P). It provides functionalities of an EMS for physical or virtual routing, switching, and gateway network functions, including fault, configuration, accounting, performance, and security (FCAPS) functionality.

Nokia Zero Touch Services (ZTS) are management applications developed for containerized network functions to facilitate their lifecycle management. ZTS provides OA&M functions for Nokia CNFs, including fault management (FM), performance management (PM), configuration management (CM), logging, and security.

Cloudband Application Manager (CBAM) is a European Telecommunications Standards Institute (ETSI) network functions virtualization (NFV) phase 2-compliant, ready-to-use, generic Virtualized Network Function Manager (VNFM-G). It automates VNF lifecycle management and cloud resource management, and its standards-based APIs make it easy to work with any vendor's VNF, EMS, Virtualized Infrastructure Manager (VIM), and NFV Orchestrator (NFVO). CBAM visualizes the structure and status of applications and performs VNF lifecycle management, including basic functions (instantiate, commission, scale, and terminate) as well as a framework for implementing advanced functions (such as healing, patching, upgrades, backup, and restore). In this project, CBAM is used for deployment and lifecycle management of Nokia SDL, the lone VNF in the 5G core solution for this project.

In summary, the following list shows what NFs are being managed by which platform.

- NetAct
    - (FM/PM/CM) 5GNR, gNB
    - (FM/PM) SDL, Registers, NPC, NEF, TAS
    - (FM) CBAM, NCM, NIAM
- NSP – (FM/PM/CM) 7705 SAR-8, 7750 SR-a8, CMG, CMM
- ZTS – (FM/PM/CM) Registers, NPC, NEF, TAS
- CBAM – (Instantiation/Commissioning) SDL

4.3.8.7 Network Security Applications

The security applications deployed for this project are described next. These are also not directly part of the security demonstrations but are important for secure 5G system operation.

The NetGuard Certificate Manager (NCM) plays the role of Certificate Authority (CA) within a public key infrastructure (PKI-CA). It is the operator's CA within a 5G network. NCM issues X.509 certificates to the PKI-End Entities (PKI-EE) requesting them. An example of a PKI-EE is a gNB. This enables the use of secure IP protocols (IPSec, TLS), thus providing confidentiality and integrity of network data (both user and control plane data). NCM is 3GPP standards compliant, and so can be integrated with the SEG and other 3GPP-compliant End Entities. Nokia-recommended practice is to co-deploy NCM with a hardware security module (HSM) for protecting CA private keys. For this project, to save cost in the non-public laboratory environment, NCM's native software storage was used instead.

The NetGuard Identity Access Manager (NIAM) solution provides a single sign-on (SSO) and privilege identity management capabilities with scalability and resiliency. The NIAM centralizes the administration and access control of all network functions (physical or virtual) via command-line interface (CLI) and/or graphical user interface (GUI). It manages user identities and permissions, and it provides for activity monitoring. Centralized security management provides several capabilities, including:

- Separation of users from actual device credentials
- User groups
- Device grouping to manage large networks
- Monitoring of all active sessions and live keystroke mirroring
- Account lock-out support
- Alarm generation
- Centralized log management
- Full native logging of command line sessions
- Video logging of all GUI sessions
- Compliance with law enforcement requirements

4.3.9 Palo Alto Networks

Palo Alto Networks has provided its VM-Series Next-Generation Firewall (NGFW) and Panorama to secure 5G. Panorama and VM-Series software work together to manage the security of mobility solutions.

A VM-Series NGFW is a virtualized version of the industry-leading Next-Generation Firewall, which is deployed as a VNF. VM-Series virtual firewalls provide all the capabilities of the Palo Alto Networks

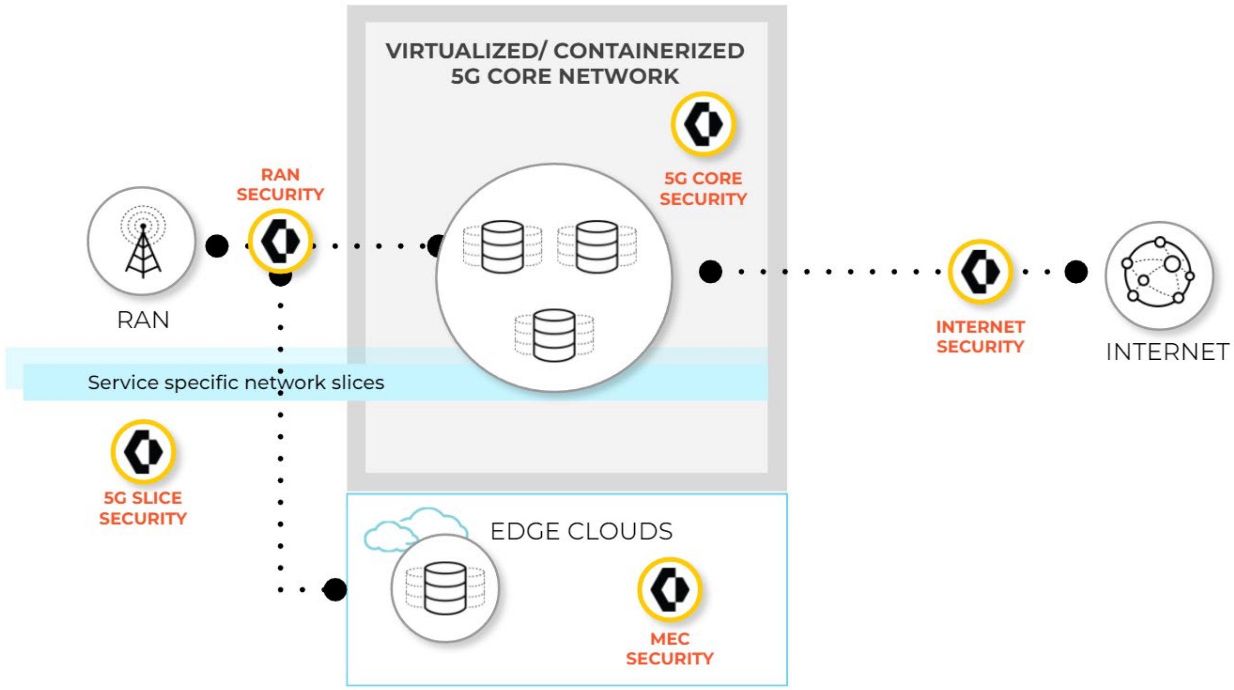
Next-Generation Firewall in a VM form factor that delivers inline network security and threat prevention.

The virtual firewall includes all the security features included in physical firewalls, such as:

- **App-ID** - Enables visibility into the applications on your network and learns how they work, their behavioral characteristics, and their relative risk. App-ID uses multiple identification techniques to determine the exact identity of applications traversing the network, irrespective of port, protocol, evasive tactics, or encryption. App-ID provides users with the knowledge and flexibility needed to safely enable applications.
- **Advanced Threat Prevention -** Inspects all traffic regardless of port, protocol, or encryption to detect and block known exploits, malware, malicious URLs, spyware, and C2.
- **Advanced URL Filtering** - Applies inline web analysis to enable safe internet access, stopping malicious URLs while also protecting your organization against known, unknown, and evasive web-based threats.
- **DNS Security -** Provides DNS-attack coverage and disrupts the 85% of attacks that use DNS for command and control and data theft, without requiring any changes to your infrastructure.
- **WildFire -** Ensures files are safe by automatically detecting and preventing unknown malware with the industry's largest threat intelligence and malware prevention engine.
- **Traffic Visibility** - Provides extensive reports, logs, and notification mechanisms for detailed visibility into network application traffic and security events. The Application Command Center (ACC) tool for the NGFW identifies the applications with the most traffic and the highest security risk.
- **Networking Versatility and Speed** - Multi-gigabit speeds and a single-pass architecture provide these services to you with little or no impact on network latency. This includes the ability to route traffic while providing Network Address Translation (NAT).
- **4G and 5G Security** – Offers complete visibility across all layers, including signaling, data, and control plane, with application-layer visibility in a mobile network, allowing granular policy enforcement and deploying a zero trust approach for the 5G user plane.

Panorama is a centralized management solution for Palo Alto Networks Next-Generation Firewalls. Panorama provides management and orchestration of the Palo Alto Networks NGFWs and visibility for SOC and NOC operators. Panorama provides a single interface for traffic and threat visibility, automation, configuration management, licensing, and software distribution. Figure 4-8 shows the security inspection and policy enforcement points for the Palo Alto Networks solution deployed in the NCCoE 5G network.

Figure 4-8 Palo Alto Networks inspection and enforcement points



5G networks require speed and agility for deployments, which require network operators to scale their infrastructure quickly. Panorama is a security management solution that provides consistent rules in an ever-changing network and threat landscape, so network security can be managed with a single security rule base for firewalls, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, access control, and data filtering. This crucial simplification, along with App-ID™ technology-based rules, dynamic security updates, and rule usage analysis, reduces administrative workload and improves your overall security posture.

When maintaining security across a 5G environment, having a centralized view of the network is important. Panorama enables this by ingesting logs from all NGFWs and providing automated threat correlation to subscribers and devices. It identifies compromised hosts and correlates malicious behavior that would otherwise be lost in the noise. This reduces the dwell time of critical threats in your network. The clean, fully customizable ACC provides a comprehensive insight into your current and historical network and threat data.

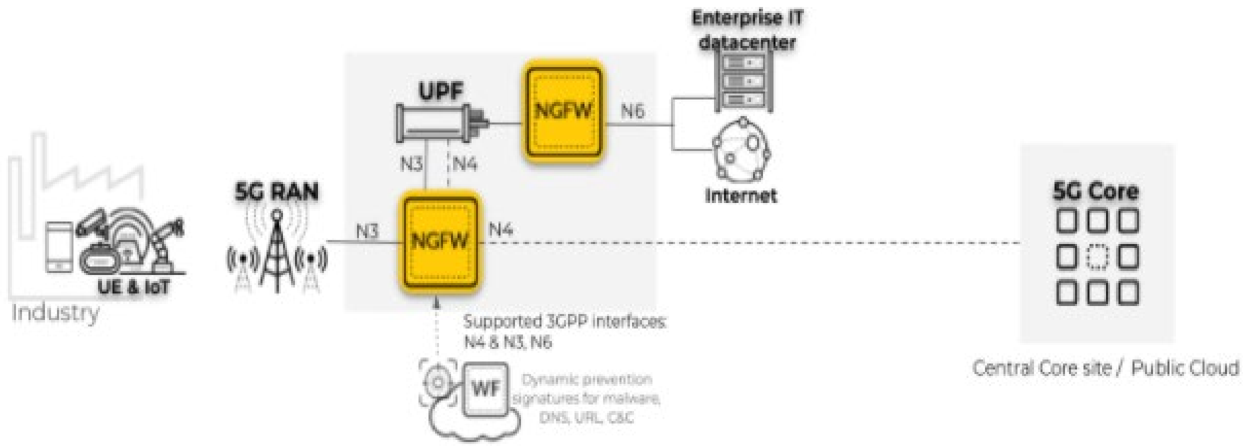
The VM-Series will be securing and controlling user plane traffic. Taking a network-centric approach, the NGFW will secure both UE and the 5G Core. All traffic is inspected to detect and prevent threats. Using Single Pass Parallel processing architecture to reduce latency, the NGFW scans traffic for vulnerability exploitation and virus techniques, command and control signatures, and malware. All detected threats can be logged or prevented. Preventing threats on the user plane is important because it conserves networks resources. C2 traffic and botnets on the user plane have the power to consume large amounts of network resources, creating a DDoS. Blocking this traffic before it can create issues ensures network continuity.

User plane traffic should also be secured from the internet. This is done through an N6 Gateway, which will be provided by the VM-Series NGFW. The N6 gateway will provide access to the internet by routing traffic and providing NAT to mask UEs behind the Mobile Network Operators' public IP addresses. The N6 Gateway will also inspect all user traffic and provide URL security. Inspecting web traffic destined for the internet will ensure that enterprise users and devices don’t connect to risky or malicious domains and that network resources are used appropriately.

As more enterprises adopt 5G, zero trust architecture for 5G will be an important control for securing access to data and applications. ZTA access is provided by using the Kipling Method of defining access policies by using Who, What, Where, When, and Why. To accurately define this level of access for 5G, operators and enterprises need to map traffic to subscribers (SUPI) and equipment (PEI). The VM-Series NGFW defines access policies using Subscriber-ID, Equipment-ID, Application-ID, and Content-ID, which enables Zero Trust Access for 5G.

To secure the user plane, inspection must happen at the N3, N4, and N6 interfaces. Figure 4-9 indicates the inspection points required for subscriber traffic correlation for this architecture. Securing traffic at the N3 interface secures the core from UE threats and, when paired with N4 security, allows for Subscriber and Equipment correlation to network traffic. 5G network functions communicate with each other using the HTTP/2 and PFCP protocols; these protocol messages carry various mobile network identifiers, such as PEI. Traffic from mobile devices is carried in GTP-U tunnels in the 5G network. The firewall is deployed inline with the N3 and N4 interfaces to inspect control and user plane traffic, and it correlates the mobile network identifier information with the IP traffic inside the GTP-U tunnels in a 5G network.

Figure 4-9 Inspection points for subscriber traffic correlation



4.3.10 Keysight Technologies 5G LoadCore

Keysight's 5G LoadCore test solution product simulates real-world subscriber models, enabling network providers and network equipment manufacturers to check the function, performance, security, and reliability of mobile services on 5G core networks. With 5G, core network complexity has reached a whole new level. Complexity is prompting the move to test in isolation. By isolating nodes, engineers can test individual interfaces, nodes, or groups of nodes and entire functionalities across the 5G core in an end-to-end approach. The ability of LoadCore to simulate UEs and gNBs across a multi-node 5G core is critical to validate functionalities and services. It allows for faster and easily repeatable test scenarios where results can be captured directly from the test tool.

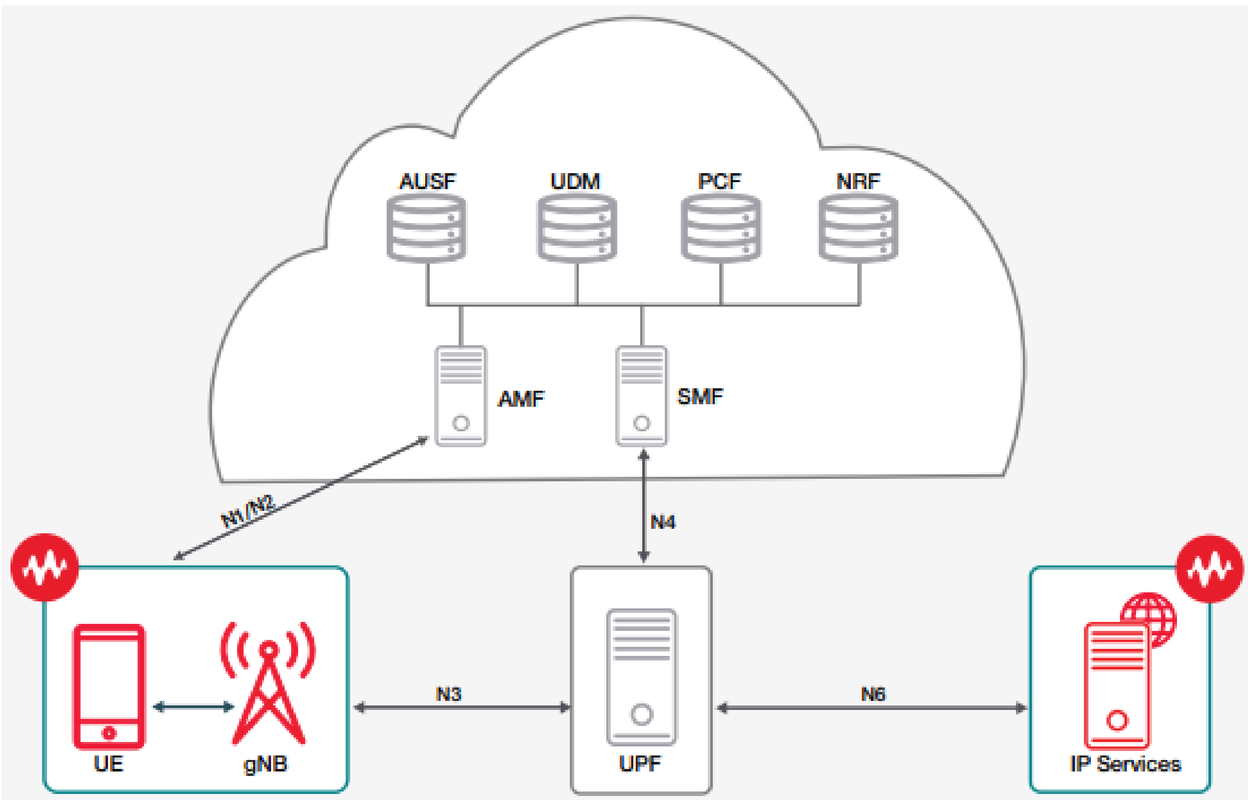
Using containerized traffic generator agents, LoadCore has the ability to emulate or place under test any of the 5G nodes, their associated interfaces or the entire 5G core network. Centered around realistic UE behavior emulation in various 5G deployments, several test topologies are available. These topologies provide flexibility for the NCCoE 5G lab, allowing different test and demonstration configurations. Using the web-based interface, you can configure and execute capacity tests, detail a device's throughput, and model a wide variety of mobility scenarios.

In this project, LoadCore is helping with the following:

- validating the functions of the 5G core network;
- benchmarking the performance of the 5G core network (both control and user planes);
- generating background UE sessions and realistic traffic mixes; and
- validating the security and robustness of the 5G core network with supported control plane traffic profiles.

As Figure 4-10 illustrates, LoadCore is emulating the UE and gNB on the originating side of the 5G core network, communicating over the N1/N2 and N3 interfaces. On the terminating side, LoadCore is emulating the data network (IP services) communicating to the 5G core network over the N6 interface. The Wireless gNB Test Module can test and validate key aspects of the N1/N2/N3 Interfaces. Feature test cases cover control and user plane procedures such as NG setup, UE registration, encryption verification, single/multiple PDU establishment, multiple QoS flows, various traffic type validation, handovers and exit/enter idle state, simulation of multiple gNBs and UEs, and UE deregistration.

Figure 4-10 Notional Wireless gNB Test Network Architecture



From a user plane perspective, LoadCore agents allow configuration of each UE group with a distinct objective consisting of single or multiple flows with the ability to specify overall throughput and distribution per flow. Support for triple play and fully stateful traffic (data, voice, video, and applications mix) enable connections to terminate on emulated or real servers. LoadCore also allows the validation of network performance by assessing traffic throughput, packet loss, One Way Delay (OWD), Delay Variation Jitter (DVJ), Mean Opinion Score (MOS), and application transaction key performance indicators (KPIs).

LoadCore agents can be used in the NCCoE 5G network to emulate the following types of control plane traffic profiles to help with security demonstrations of the 5G core network:

- excessive load of control plane traffic for network stress and denial-of-service test
- UE/gNB misconfiguration (including security capabilities and secret keys)
- negative NAS procedure via impairment model
- 3GPP 5G core NF(s) SCAS test suite(s) for component-level security assessment

5 Security Characteristic Demonstration

This section will describe how each scenario demonstrates the security characteristic/category and associated security capabilities/properties. This section will be written for a future draft.

5.1 Assumptions and Limitations

This section about the limitations of the demonstration scenario will be written for a future draft.

5.2 Functional Demonstration Scenarios

This section will describe short functional demonstration scenarios. It will include all functional scenarios that are enabled by the current system architecture and indicate additional ones that are planned for later. The operation of each security capability for the example solution will be verified in the context of the demonstration scenario described below, as well as for additional scenarios to be added to a future draft.

5.2.1 Scenario 1 – 5G SA deployment using single PLMN

This section will provide a brief overview of the equipment, the architecture, and the call flow used in this scenario. The functionality of data, voice, and video will be tested for the non-roaming case. Specific details will be described in the in the functional demonstration plan.

5.2.1.1 Data Call

This section will provide a brief overview of the data call setup. Detailed information on the test procedure and test results for the 5G data call will be described in the functional demonstration plan. In the real world, this test is equivalent to a subscriber browsing a web site on the internet or sending an email to another subscriber.

5.2.1.2 Voice over IP Call

This section will provide a brief overview of the VoIP call setup. Detailed information on the test procedure and test results for the 5G VoIP call will be described in the functional demonstration plan. In the real world, this test is equivalent to a subscriber making a VoIP call over the internet to another subscriber.

5.2.1.3 Video Streaming

This section will provide a brief overview of video streaming. Detailed information on the test procedure and test results for the 5G video streaming will be described in the functional demonstration plan. In the real world, this test is equivalent to a subscriber making a video-on-demand request for a particular video file to a video streaming server on the internet.

5.3 Findings

This section will highlight how well the security capabilities instantiated in the system architecture demonstration address the security risks that it was intended to support. This section will be written for a future draft.

Appendix A Security Control Maps

This appendix will provide tables mapping the cybersecurity capabilities of the technologies being used for the first phase of the example solution to applicable NIST guidance. This appendix will be added to a future draft.

Appendix B Future Capabilities

There are many additional security capabilities that will be incorporated during this project. Section 3.5.2 describes those that are planned for the project's first phase. This appendix describes additional security capabilities tentatively planned for the subsequent phase.

Security Capability	Subreference	Description
Infrastructure Security		
Hardware Roots of Trust Packet Core, ISC-1		
Network Function Policy Enforcement	ICS-1.6	Technically enforce policies that define the servers in the compute environment where NFs can run based on trust values and asset tags.
5G Standalone Security		
Radio Network Security, 5GSC-2		
CU/DU Split	5GSC-2.2	Split gNB into Central Unit (CU) and Distributed Unit (DU), with the CU performing security functions (confidentiality/integrity) and being located closer to the core.
Security Visibility	5GSC-2.4	Enable applications to check the security being applied to the radio connection.
256-Bit Algorithms	5GSC-2.5	Use stronger cryptographic algorithms on this interface once they are adopted by 3GPP SA3.
Interworking & Roaming Security, 5GSC-4		
Security Edge Protection Proxy (SEPP)	5GSC-4.1	Implement application-layer security for the service layer information exchanged between two PLMNs. Provide security functions for integrity, confidentiality, replay protection, mutual authentication, authorization, negotiation of cipher suites, and key management, as well as the notion of topology hiding and spoofing protection.
5G to LTE Interworking Mobility Within the Same Operator Network	5GSC-4.2	Use secure procedures and security demarcations to secure LTE to 5G interworking as defined in 3GPP 23.501 [18]. Includes protecting the transmission of security keying materials between LTE and 5G.
5G to LTE Interworking Mobility Across Operator Networks	5GSC-4.3	Protects handovers involving 5G to LTE internetworking across two operators' network using N26 because 4G does not offer subscription identities encryption, so a UE moving from 5G to LTE will be subject to IMSI catching attacks. GSMA has not finalized work on 5G SA to LTE roaming across different operators.

Security Capability	Subreference	Description
API Security, 5GSC-5		
Common API Framework (CAPIF)	5GSC-5.2	Use secure interfaces, such as TLS-PSK, TLS-PKI and TLS-OAuth, provided by a common API interface between internal functions and external functions. Use CAPIF Core Function (CCF) to manage all internal and external APIs.
Network Slicing Security, 5GSC-6		
Network Slice Resource Isolation	5GSC-6.1	Enable the creation of multiple logical networks over the same physical infrastructure. Demonstrate orchestrated deployment and configuration of network functions to provide services that are required for a specific usage scenario. Tie into infrastructure security capabilities to isolate slice resources.
Network Slice Additional Authentication	5GSC-6.2	Perform secondary authentication with Network Slice Specific Authentication and Authorization Function (NSSAAF) to check if the user is authorized to use that slice (3GPP TS 29.526). Do additional authentication of subscriber identity.
Application Security, 5GSC-7		
Application Security Onboarding	5GSC-7.3	Ensure that applications are onboarded securely and that communications between applications are secure. Leverage the zero trust concept.
Internet Security Protocol Recommended Practice, 5GSC-8		
TLS Security	5GSC-8.1	Implement TLS security where possible to protect NF communication at the transport layer via mutual authentication and transport security. Ensure protection of the communication's confidentiality and integrity, and implement anti-replay measures.
DNSSEC	5GSC-8.3	Use DNS Security Extensions (DNSSEC) to protect the integrity of any 5G-related DNS communication.
OAuth for Service-Based Architecture (SBA)	5GSC-8.4	Use the OAuth 2.0 framework at the API layer to ensure that only authorized network functions are permitted access to a service offered by another NF. Use CAPIF with TLS-Oauth for all internal and external APIs.

1606 Appendix C List of Acronyms

3GPP	3rd Generation Partnership Project
5G	5th Generation
5GC	5G Core
5GSC	5G Standalone Security Category
ACC	(Palo Alto Networks) Application Command Center
AES	Advanced Encryption Standard
AF	Application Function
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
API	Application Programming Interface
ARPF	Authentication Credential Repository and Processing Function
AS	Access Stratum
ASiR	(Nokia) AirScale Indoor Radio System
AUSF	Authentication Server Function
AWS	Amazon Web Services
BBU	Baseband Unit
BIOS	Basic Input/Output System
C2	Command and Control
CA	Certificate Authority
CaaS	Container-as-a-Service
CAPIF	Common Application Programming Interface Framework
CBAM	(Nokia) Cloudband Application Manager
CCF	CAPIF Core Function
CLI	Command-Line Interface
CM	Configuration Management

CMG	(Nokia) Cloud Mobile Gateway
CMM	(Nokia) Cloud Mobility Manager
CNF	Container-Based Network Function
CPRI	Common Public Radio Interface
CPU	Central Processing Unit
CRADA	Cooperative Research and Development Agreement
CSRIC	Communications Security, Reliability, and Interoperability Council
CU	Central Unit
DDoS	Distributed Denial of Service
DN	Data Network
DNN	Data Network Name
DNS	Domain Name System
DNSSEC	Domain Name System Security
DoS	Denial of Service
DU	Distributed Unit
EAP	Extensible Authentication Protocol
EAP – AKA’	Extensible Authentication Protocol Method for 3rd Generation Authentication
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
eCPRI	Enhanced Common Public Radio Interface
eMBB	Enhanced Mobile Broadband
EMS	Element Management System
eSIM	Software-Based SIM
ETSI	European Telecommunications Standards Institute
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FM	Fault Management

FTP	File Transfer Protocol
GbE	Gigabit Ethernet
Gbps	Gigabits Per Second
GE	Gigabit Ethernet
gNB	gNodeB
GPRS	General Packet Radio Service
GSMA	GSM Association
GTP-U	GPRS Tunneling Protocol User
GUI	Graphical User Interface
GUTI	Global Unique Temporary Identifier
HRoT	Hardware Root of Trust
HSM	Hardware Security Module
ID	Identifier
IE	Information Element
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Core Network Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IPsec	Internet Protocol Security
IR	Internal Report
ISC	Infrastructure Security Category
ISE	(Cisco) Identity Services Engine
IT	Information Technology

LAG	Link Aggregation Group
LTE	Long-Term Evolution
LTKUP	Long Term Key Update Procedures
MHz	Megahertz
ML	Machine Learning
MTTK	Mean Time to Know
N3IWF	Non-3GPP Inter-Working Function
NAS	Non-Access Stratum
NAT	Network Address Translation
NB-IoT	Narrowband Internet of Things
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partnership
NCM	(Nokia) NetGuard Certificate Manager
NCS	Nokia Container Services
NDS	Network Domain Security
NDSS	Network and Distributed Systems Security Symposium
NEF	Network Exposure Function
NF	Network Function
NFM-P	(Nokia) NSP Network Functions Manager for Packet
NFS	Network File System
NFV	Network Functions Virtualization
NFVO	Network Functions Virtualization Orchestrator
NGFW	Next-Generation Firewall
NIAM	(Nokia) NetGuard Identity Access Manager
NIST	National Institute of Standards and Technology
NMS	Network Management System

NOC	Network Operations Center
NPC	Nokia Policy Controller
NRD	(Nokia) Network Repository Directory
NRF	Network Repository Function
NRT	Non-Real-Time
NSA	Non-Standalone (Network)
NSP	(Nokia) Network Services Platform
NSSAAF	Network Slice Specific Authentication and Authorization Function
NSSF	Network Slice Selection Function
NTP	Network Time Protocol
NVM	Node Version Manager
OA&M	Operations, Administration, and Management
OBSAI	Open Base Station Architecture Initiative
OS	Operating System
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
PEP	Policy Enforcement Point
PFCP	Packet Forwarding Control Protocol
PKI	Public Key Infrastructure
PKI-CA	Public Key Infrastructure-Certificate Authority
PKI-EE	Public Key Infrastructure-End Entities
PLMN	Public Land Mobile Network
PM	Performance Management
pRRH	Pico-Cell Solution Remote Radio Head

PSK	Pre-Shared Keys
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RFC	Request for Comments
RMF	Risk Management Framework
RRC	Radio Resource Controller
RT	Real-Time
RTT	Round Trip Time
RU	Radio Unit
SA	Standalone (Network)
SA3	3GPP Technical Specification Group Service and System Aspects Working Group 3
SaaS	Software as a Service
SAL	(Cisco) Security Analytics and Logging
SBA	Service-Based Architecture
SBI	Service Based Interface
SCEF	Service Capability Exposure Function
SDL	(Nokia) Shared Data Layer
SDO	Standards Development Organization
SEAF	Security Anchor Functions
SecL-DC	(Intel) Security Libraries for Data Center
SEG	Security Gateway
SEPP	Security Edge Protection Proxy
SFP	Small Form-Factor Pluggable
SGT	Security Group Tag

SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SM	(Nokia) AirScale 5G System Module, Session Management Message
SMF	Session Management Function
SMS	Short Message Service
SMSC	Short Message Service Center
SMSF	Short Message Service Function
S-NSSAI	Single Network Slice Selection Assistance Information
SOC	Security Operations Center
SP	Special Publication
SRT	Server Response Time
SSO	Single Sign-On
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TAS	(Nokia) Telecom Application Server
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TNGF	Trusted Non-3GPP Gateway Function
TPM	Trusted Platform Module
TS	Technical Specification
TXT	(Intel) Trusted Execution Technology
UDM	Unified Data Management
UDR	Unified Data Repository
UE	User Equipment
UEFI	Unified Extensible Firmware Interface

UICC	Universal Integrated Circuit Card
UPF	User Plane Function
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
VIM	Virtualized Infrastructure Manager
VLT	Virtual Link Trunking
VM	Virtual Machine
VMM	Virtual Machine Manager
VNF	Virtual Machine-Based Network Function
VNFM-G	Virtualized Network Function Manager
Vo5G	Voice Over 5G
VoIP	Voice Over IP
VoLTE	4G Voice Over Long-Term Evolution
VPN	Virtual Private Network
W	Watt
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
ZTA	Zero Trust Architecture
ZTS	(Nokia) Zero Touch Services

Appendix D References

[1] *Network Domain Security (NDS): IP network layer security*, Specification #33.210, 3rd Generation Partnership Project (3GPP), 2021. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279

[2] A. Shaik et al., "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," NDSS '16, San Diego, California, February 21-24, 2016. Available: https://arxiv.org/pdf/1510.07563.pdf

[3] *Security architecture and procedures for 5G System*, Specification #33.501, 3rd Generation Partnership Project (3GPP), 2022. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[4] A. Singla et al., "Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks," *Proceedings on Privacy Enhancing Technologies*, 2020, pp. 126-142. Available: https://petsymposium.org/2020/files/papers/issue1/popets-2020-0008.pdf

[5] P. K. Nakarmi, "Fighting IMSI catchers: A look at 5G cellular paging privacy." Available: https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy

[6] S. Tabbane, "4G and 5G networks security techniques and algorithms," ITU PITA Workshop on Mobile network planning and security, October 23-25, 2019. Available: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/ITUPITA2018/ITU-ASP-CoE-Training-on-/4G%20and%205G%20network%20security%20techniques%20and%20algorithms.pdf

[7] D. Rupprecht et al., "Breaking LTE on Layer Two." Available: https://alter-attack.net/media/breaking_lte_on_layer_two.pdf

[8] J. Cichonski et al., *Guide to LTE Security*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-187, Gaithersburg, Md., December 2017, 49 pp. Available: https://doi.org/10.6028/NIST.SP.800-187

[9] J. Arkko et al., *Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 5448, May 2009. Available: https://datatracker.ietf.org/doc/rfc5448/

[10] GSM Association (GSMA). *Securing the 5G Era*. Available: https://www.gsma.com/security/securing-the-5g-era/

[11] B. Jun and G. Kenworthy, “Is Your Mobile Device Radiating Keys?”, RSA Conference 2012. Available: https://www.rambus.com/wp-content/uploads/2015/08/2012-Jun-Kenworthy-MobileDeviceLeakage1.pdf

[12] P. O’Hanlon et al., “Mobile Subscriber WiFi Privacy,” MoST IEEE S&P Workshop 2017. Available: https://www.ieee-security.org/TC/SPW2017/MoST/slides/OHanlon_MoST17_slides.pdf

[13] M. Kuhn, “Compromising emanations: eavesdropping risks of computer displays,” University of Cambridge Computer Laboratory, Technical Report Number 577, December 2003. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf

[14] S. Khandelwal, “Hacker Can Steal Data from Air-Gapped Computers through Power Lines,” The Hacker News, April 12, 2018. Available: https://thehackernews.com/2018/04/hacking-airgap-computers.html

[15] *Study on Long Term Key Update Procedures (LTKUP)*, Specification #33.834, 3rd Generation Partnership Project (3GPP), 2019. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3255

[16] CableLabs, “A Comparative Introduction to 4G and 5G Authentication,” Winter 2019. Available: https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication

[17] *Architecture enhancements to facilitate communications with packet data networks and applications*, Specification #23.682, 3rd Generation Partnership Project (3GPP), 2021. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=862

[18] *System architecture for the 5G System*, Specification #23.501, 3rd Generation Partnership Project (3GPP), 2022. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[19] *Procedures for the 5G System*, Specification #23.502, 3rd Generation Partnership Project (3GPP), 2022. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145

[20] Nokia. *Network Exposure Function*. Available: https://www.nokia.com/networks/products/network-exposure-function/

[21] E. Barker et al., *Guide to IPsec VPNs*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-77 Revision 1, Gaithersburg, Md., June 2020, 149 pp. Available: https://doi.org/10.6028/NIST.SP.800-77r1

[22] Software Engineering Institute, "IKEv1 Main Mode vulnerable to brute force attacks," Vulnerability Note VU#857035, August 14, 2018. Available: https://www.kb.cert.org/vuls/id/857035

[23] Software Engineering Institute, "IKE/IKEv2 protocol implementations may allow network amplification attacks," Vulnerability Note VU#419128, February 29, 2016. Available: https://www.kb.cert.org/vuls/id/419128

[24] Communications Security, Reliability, and Interoperability Council (CSRIC) VII, *Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security*, March 10, 2021. Available: https://www.fcc.gov/file/20606/download

[25] Nokia, "Start 5G deployment with an eye on the future: Understanding the strange language of NSA vs SA and options 3, 2, 7 and 4," SR1808027862EN, September 2018. Available: https://onestore.nokia.com/asset/f/202255

[26] "5G Architecture Options – Full Set," RP-161266, Joint RAN/SA meeting, June 14, 2016. Available: https://telecoms.com/wp-content/blogs.dir/1/files/2016/06/5G-architecture-options.pdf

[27] *Security architecture and procedures for 5G System*, Technical Specification 133.501 V15.4.0, European Telecommunications Standards Institute (ETSI) 3rd Generation Partnership Project (3GPP), 2019. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/ts_133501v150400p.pdf

[28] *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UTMS); LTE; 5G; Release description; Release 15*, Technical Report 121.915 V15.0.0, European Telecommunications Standards Institute (ETSI) 3rd Generation Partnership Project (3GPP), 2019. Available: https://www.etsi.org/deliver/etsi_tr/121900_121999/121915/15.00.00_60/tr_121915v150000p.pdf

[29] Nokia, "Voice over 5G (Vo5G) core: Build IMS voice communications into your new 5G services." Available: https://www.nokia.com/networks/solutions/voice-over-5g-vo5g-core/

[30] "IP Multimedia Subsystem (IMS)," Specification # 23.228, 3rd Generation Partnership Project (3GPP), 2021. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=821