5G Security Guide
Version 3.0
16 July 2024

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.34 - Policy and Procedures for Official Documents.

Table of Contents

1 Introduction

1.1 Overview

The fifth generation (5G) telecommunication system delivers Enhanced Mobile Broadband (eMBB), massive machine type communications, and ultra-reliable and low latency communications to subscribers. 5G provides multi-network slicing, multi-tenancy, multi-level of services and multi-connectivity network capabilities thereby enabling various industries to join the operation and development of the 5G services.

Alongside the new capabilities in 5G, there are also changes in how networks are built, secured, and managed. These include virtualisation and containerisation, Network Function Virtualisation (NFV), Open-Source Software (OSS), SDN security monitoring, security assurance, security of Open RAN (O-RAN) interfaces and components, network slicing, network slicing security, programmable network, multi-access edge computing (MEC) and its security, and combined development and operations functions, so called DevOps. These new technologies will give future networks flexibility and agility in developing and deploying services and network infrastructures. However, they also introduce new attack vectors in next generation telecommunications systems and the organisations that use them.

It is noteworthy that considerable thought has gone into the planning and design of the security enhancements in 5G. These efforts have been contributed to by a range of industry stakeholders as well as government agencies such as the German Bundesamt fuer Sicherheit in der Informationstechnik (BSI) and the National Technology Security Coalition (NTSC) in the USA. This has seen the introduction of security enhancements such as default mandatory encryption of network and privacy-sensitive information as well as another principles-based concepts and methodologies, including:

- Use of mutual authentication – ensure that sender and receiver have an established trusted and secured relationship.
- Assume Zero Trust design principles – operate on the basis of not automatically trusting anybody or anything inside or outside the network perimeter, while not automatically assuming encrypted traffic to be valid (see Section 8.9.1 for more details).
- Do not assume transport links are secure – use encryption to ensure any compromised information is of no value to recipients.

This document discusses different aspects of 5G security identified by GSMA as requiring attention within appropriate bodies (e.g. 3GPP, IETF, ETSI, and GSMA).

1.2 Scope

Unless stated otherwise, the discussions in this document refer to the capabilities supported by 3GPP Release 17, i.e. the third release of 3GPP standards for 5G. The content of this version 3.0 reflects current understanding in 2023.

Further updates of this document will be made to reflect the 3GPP work on future 5G Releases. The next version of the document will ensure the document reflects Release 18.

NOTE: A number of topics included in this document are managed by organizations and standards development organizations other than 3GPP. These topics

continue to evolve but not necessarily in step with 3GPP Releases. Key developments on these topics will be covered in future versions of this document.

1.3 Abbreviations

Term	Description
5G-GUTI	5G Globally Unique Temporary Identifier
5G-RG	5G Residential Gateway
5G NSA	5G Non-Standalone
5GS	5G System
5GSTF	GSMA 5G Security Task Force
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
ALS	Application Layer Security
AMF	Access Management Function
ARPF	Authentication credential Repository and Processing Function(ality)
ASN.1	Abstract Syntax Notation One
AUSF	Authentication Server Function
AV	Authentication Vector
BGP	Border Gateway Protocol
BSR	Binding Security Requirement
CAP	Camel Application Protocol
CDR	Call Detail Record
cIPX	IPX-Provider of the service consumer PLMN
CIRM	Cloud Infrastructure Reference Model
CN	Core Network
CNTT	Cloud infrastructure Telecom Taskforce
COTS	Commercial Off the Shelf
CP	Control Plane
CRAN	Cloud Radio Access Network
cSEPP	Consumer Security Edge Protection Proxy
CSP	Communication Service Provider
CSRIC	Communications Security, Reliability and Interoperability Council
CU-DU	Central Unit Distributed Unit
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DEA	Diameter Edge Agent
DNS	Domain Name Server
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol

Term	Description
ECIES	Elliptic Curve Integrated Encryption Scheme
EAP-AKA	Extensible Authentication Protocol – Authentication and Key Agreement
EDCE5	EPC enhancements to support 5G New Radio via Dual Connectivity
EECC	European Electronic Communications Code
eMBB	Enhanced Mobile Broadband
E-UTRA	Evolved Universal Terrestrial Radio Access
EPS	Evolved Packet System
FMS	Fraud Management System
FN-RG	Fixed Network Residential Gateway
GBA	Generic Bootstrapping Architecture
GDPR	General Data Protection Regulation
gNB	Next Generation Node B
GRX	GPRS Roaming Exchange
GTP	GPRS Tunneling Protocol
GTP-C	GPRS Tunneling Protocol – Control
GTP-U	GPRS Tunneling Protocol – User Data
HPLMN	Home Public Land Mobile Network
HSM	Hardware Security Module
HTTP/2	Hypertext Transfer Protocol version 2
IAB	Integrated Access and Backhaul
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IPRAN	IP Radio Access Network
IPUPS	Inter-PLMN User Plane Security
IPX	IP Exchange
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
KMS	Key Management System
LLS	Lower Layer Split
LTE	Long Term Evolution
MANO	Management And Network Orchestration
MIB	Master Information Block
MSIN	Mobile Subscriber Identification Number
MCC	Mobile Country Code
MCData	Mission Critical Data
MCPTT	Mission Critical Push to Talk
MCS	Mission Critical Services

Term	Description
MCVideo	Mission Critical Video
MEC	Multi-Access Edge Computing
MISP	Malware Information Sharing Platform
MITM	Man-In-The-Middle
MME	Mobility Management Entity
MNC	Mobile Network Code
MNO	Mobile Network Operators
MPS	Multimedia Priority Service
MR-DC	Multi-RAT Dual Connectivity
N3IWF	Non-3GPP Inter-Working Function
N5FC	Non-5G-Capable devices
N5CW	Non-5G-Capable over WLAN
NaaS	Network as a Service
NAI	Network Access Identifier
NAS	Non-Access Stratum
NDS/IP	Network Domain Security / Internet Protocol
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
NFV	Network Function Virtualisation
NFVI	Network Function Virtualisation Infrastructure
ng-eNB	Next Generation Evolved Node B
NPN	Non-Public Networks
NR	New Radio
NSA	Non-Stand Alone
NSaaS	Network Slice as a Service
NSI	Network Slice Instance
NSSAAF	Network Slice Specific Authentication and Authorisation Function
NSSF	Network Slice Selection Function
O-DU	O-RAN Distributed Unit
OITF	Open Infrastructure Task Force
O-RAN	Open RAN
O-RU	O-RAN Radio Unit
OS	Operating System
OSS	Open-Source Software
PDCA	Plan–Do–Check–Act or Plan–Do–Check–Adjust
PDR	Packet Detection Rule
PFCP	Packet Forwarding Control Protocol
pIPX	IPX-Provider of the service producer

Term	Description
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
POI	Point Of Interconnect
PQC	Post-Quantum Cryptography
PRD	Permanent Reference Document
PRINS	PRotocol for N32 INterconnect Security
pSEPP	Producer Security Edge Protection Proxy
PSK	Pre-shared Secret Key
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
RAND	Random Number
REST	Representational State Transfer
RESTFUL	REST Conformant
RPKI	Resource Public Key Infrastructure
RRC	Radio Resource Control
SA	Stand-Alone
SAAS	Software as a Service
SBA	Service Based Architecture
SBOM	Software Bill of Materials
SCAS	Security Assurance Specification
SCP	Service Communication Proxy
SDM	Software Defined Monitoring
SDMN	Software Defined Mobile Networks
SDN	Software Defined Networks
SDO	Software Defined Operations
SDR	Software Defined Radios
SEAF	Security Anchor Function
SECAM	Security Assurance Methodology
SeGW	Security Gateway
SEPP	Secure Edge Protection Proxy
SIDF	Subscription Identifier De-concealment Function
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SMF	Session Management Function
SMSoIP	SMS over IP
SMSoNAS	SMS over NAS
SON	Self-Organising Networks
SoR	Steering of Roaming

Term	Description
SRVCC	Single Radio Voice Call Continuity
SS	Synchronisation Signal
SSH	Secure Shell
SUCI	Subscription Concealed Identity
SUPI	Permanent Subscription Identity
T-ISAC	Telecommunication Information Sharing & Analysis Centre
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TN	Transmission Network
TNAN	Trusted Non-3GPP Access Network
TNAP	Trusted Non-3GPP Access Point
TNGF	Trusted Non-3GPP Gateway Function
TPM	Trust Platform Module
TSC	Time Sensitive Communications
TTP	Tactics, Techniques and Procedures
TWIF	Trusted WLAN Interworking Function
UAC	Unified Access Control
UDM	Unified Data Management
UE	User Equipment
UICC	Universal Integrated Circuit Card
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable Low-Latency Communication
USIM	Universal Subscriber Identity Module
VoNR	Voice over New Radio
VPLMN	Visited Public Land Mobile Network
W-5GAN	Wireline 5G Access Network
W-AGF	Wireline Access Gateway Function
WAF	Web Application Firewall
WEF	World Economic Forum
ZT	Zero Trust
ZTA	Zero Trust Architecture

1.4 References

Ref	Doc Number	Title
[1]	3GPP TS 33.501	Security architecture and procedures for 5G
[2]	IETF RFC 7540	Hypertext Transfer Protocol Version 2 (HTTP/2)

Ref	Doc Number	Title
[3]	IETF RFC 793	Transmission Control Protocol (TCP)
[4]	IETF RFC 7159	The JavaScript Object Notation (JSON) Data Interchange Format
[5]	GSMA PRD IR.73	Steering of Roaming Implementation Guidelines
[6]	GSMA PRD FS.07	SS7 and SIGTRAN Network Security
[7]	GSMA PRD FS.11	SS7 Interconnect Security Monitoring and Firewall Guidelines
[8]	GSMA PRD IR.82	SS7 Security Network Implementation Guidelines
[9]	GSMA PRD FS.19	Diameter Interconnect Security
[10]	GSMA PRD IR.88	LTE and EPC Roaming Guidelines
[11]	ENISA Signaling Security	Signaling Security in Telecom SS7/Diameter/5G – EU level assessment of the current situation
[12]	FCC CSRIC WG3 report March 2018	Network Reliability and Security Risk Reduction – Final Report – Recommendations to Mitigate Security Risks for Diameter Networks
[13]	IETF RFC 5216	The EAP-TLS Authentication Protocol
[14]	arXiv2018	Louis Waked, Mohammad Mannan, and Amr Youssef – “The Sorry State of TLS Security in Enterprise Interception Appliances”
[15]	3GPP TR 23.898	3GPP; Technical Specification Group Services and System Aspects; Access Class Barring and Overload Protection
[16]	GSMA PRD FS.13	Network Equipment Security Assurance Scheme Overview
[17]	GSMA PRD FS.21	Interconnect Signaling Security Recommendations
[18]	GSMA PRD FS.32	T-ISAC Service Offering
[19]	David Basin and others	“A Formal Analysis of 5G Authentication https://arxiv.org/pdf/1806.10360.pdf
[20]	GSMA CVD-2018-0013 Briefing	Briefing on “A Formal Analysis of 5G Authentication” Security Research Paper
[21]	Syed Rafiul Hussain and others	“Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information” https://relentless-warrior.github.io/files/paging-ndss19-preprint.pdf
[22]	GSMA CVD-2018-0014 Briefing	Briefing on “Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information” Security Research Paper
[23]	3GPP TS 38.304	3GPP; Technical Specification Group Radio Access Network; NR; User Equipment (UE) procedures in Idle mode and RRC Inactive state (Release 15)
[24]	David Rupprecht and others	“On LTE Network Security Testing and Attack Detection Techniques with Full Baseband Control”
[25]	GSMA CVD-2018-0013 Briefing	Briefing on “LTE Network Security Testing and Attack Detection Techniques with Full Baseband Control” Security Research Paper
[26]	3GPP TS 24.501	3GPP; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3

Ref	Doc Number	Title
[27]	Ravishankar Borgaonkar and others	"New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols"
[28]	Hongil Kim KAIST and others	"Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane"
[29]	GSMA CVD-2019-0021 Briefing	Briefing on "Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane" Security Research Paper
[30]	S.893	Secure 5G and Beyond Act of 2020, March 23, 2020
[31]	3GPP TS 23.501	3GPP; Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2
[32]	3GPP TS 31.115	3GPP; Technical Specification Group Core Network and Terminals; Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications
[33]	GSMA PRD BA.30	Fraud Prevention Procedures
[34]	3GPP TS 38.331	3GPP; Technical Specification Group Radio Access Network; NR; Radio Resource Control (RRC) protocol specification
[35]	ETSI TS 103 457	CYBER; Trusted Cross-Domain Interface: Interface to offload sensitive functions to a trusted domain
[36]	HardenStance Briefing No.22, 28th March 2019	"ETSI Secures Public Clouds for Telcos"
[37]	FASG14 Doc 005	"Why does the World Economic Forum care about 5G?"
[38]	FCC CSRIC WG3 report March 2019	"Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols"
[39]	Katharina Kohls and other	"Lost Traffic Encryption: Fingerprinting LTE/4G Traffic on Layer Two"
[40]	GSMA CVD -2019-0022 Briefing	Briefing on "Lost Traffic Encryption: Fingerprinting LTE/4G Traffic on Layer Two" Security Research Paper
[41]	Altaf Shaik and others	"New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities" https://dl.acm.org/citation.cfm?id=3319728
[42]	GSMA CVD-2019-0018 Briefing	Briefing on "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities"
[43]	5GSTF11 Doc 001	"Security for E2E 5G network slice isolation", Zhaoji Lin, ZTE
[44]	ETSI TS 103 457	"CYBER; Trusted Cross-Domain Interface: Interface to offload sensitive functions to a trusted domain"
[45]	Altaf Shaik and Ravishankar Borgaonkar	"New Vulnerabilities in 5G Networks" https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks.pdf

Ref	Doc Number	Title
[46]	CISA 5G Risks Overview	Critical Infrastructure Security and Resilience Note “Overview of Risks Introduced by 5G Adoption in the United States” 31 July 2019
[47]	CISA Market Penetration and Risk Factors	5G Wireless Networks - Market Penetration and Risk Factors by the Cybersecurity and Infrastructure Security Agency, July 2019
[48]	EU NIS Directive	“EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks”, 9 October 2019
[49]	ETIS	Telco Security Landscape
[50]	3GPP TS 23.003	3GPP; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification
[51]	3GPP TS 22.101	3GPP; Technical Specification Group Services and System Aspects; Service accessibility
[52]	GSMA PRD FS.36	5G Interconnect Security
[53]	GSMA PRD FS.34	Key management for 4G and 5G inter-PLMN security
[54]	Syed Rafiul Hussain and others	5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol https://relentless-warrior.github.io/wp-content/uploads/2019/10/5GReasoner.pdf
[55]	GSMA CVD Governance Team	Briefing on “5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol” Security Research Paper
[56]	GSMA PRD IR.65	IMS Roaming, Interconnection and Interworking Guidelines
[57]	GSMA PRD IR.90	RCS Interworking Guidelines
[58]	GSMA PRD NG.113	5G Roaming Guidelines
[59]	GSMA PRD IR.77	InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers
[60]	ENISA	“ENISA Threat Landscape for 5G Networks – Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)”, December 2020
[61]	NIS Cooperation Group	“Cybersecurity of 5G networks EU Toolbox of risk mitigating measures”, CG Publication 01/2020
[62]	GSMA PRD FS.20	GPRS Tunneling Protocol (GTP) Security
[63]	GSMA PRD FS.31	Baseline Security Controls
[64]	GSMA PRD FS.37	GTP-U Security
[65]	3GPP TS 22.153	3GPP; Technical Specification Group Services and System Aspects; Multimedia Priority Service
[66]	US Secretary of Defense	Department of Defense (DoD) 5G Strategy (U), 2 May 2020 https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf
[67]	FCC CSRIC WG2 report June 2020	Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation

Ref	Doc Number	Title
[68]	5G ACIA White Paper, May 2020	Security Aspects of 5G for Industrial Networks, 5G Alliance for Connected Industries and Automation
[69]	5GAA White Paper, May 2020	5GAA Efficient Security Provisioning System, 5GAA Automotive Association
[70]	David Rupprecht and others	IMP4GT: IMPersonation Attacks in 4G Networks
[71]	GSMA CVD Governance Team	Briefing on “IMP4GT: IMPersonation Attacks in 4G Networks” Security Research
[72]	David Rupprecht and others	Eavesdropping Encrypted LTE Calls With REVOLTE
[73]	GSMA CVD Governance Team	Briefing on “Eavesdropping Encrypted LTE Calls With REVOLTE” Security Research
[74]	3GPP TR 29.829	3GPP; Technical Specification Group Core Network and Terminals; Service-based support for SMS in 5GC; (Release 17)
[75]	GSMA PRD FS.41	RCS Fraud and Security Assessment
[76]	Tao Wan and Mansour Ganji	Security analysis of 5G mobile networks
[77]	Merlin Chlosta and others	SUCI-Catchers: Still catching them all?
[78]	Haibat Khan and Keith M. Martin	A Survey of Subscription Privacy on the 5G Radio Interface
[79]	MITRE ATT&CK® Framework	MITRE ATT&CK: Design and Philosophy, MITRE, March 2020
[80]	GSMA PRD NG.126	Cloud Infrastructure Reference Model, Version 1.0, November 11, 2020
[81]	Nitya Lakshmanan and others	A Stealthy Location Identification Attack Exploiting Carrier Aggregation in Cellular Networks
[82]	3GPP TS 33.117	Catalogue of general security assurance requirements
[83]	3GPP TS 29.244	Interface between the Control Plane and the User Plane nodes; Stage 3
[84]	5G Americas	A 5G Americas White Paper “Security Considerations for the 5G ERA”, July 2020
[85]	3GPP TS 29.500	3GPP; Technical Specification Group Core Network and Terminals; 5G System; Technical Realization of Service Based Architecture; Stage 3
[86]	3GPP TS 29.573	3GPP; Technical Specification Group Core Network and Terminals; 5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3
[87]	NIS Cooperation Group	“Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity”, July 2020

Ref	Doc Number	Title
[88]	ENISA	Guideline on Security Measures under the EECC, 3rd Edition, December 2020
[89]	CISA 5G Strategy	Ensuring the Security and Resilience of 5G Infrastructure in Our Nation, August 2020
[90]	GSMA PRD FS.43	Security Guidelines for Storage of UICC Credentials
[91]	FCC CSRIC WG3 report Sept 2020	Report on Risks introduced by 3GPP Releases 15 and 16 5G Standards
[92]	IEEE 802.1AS-Rev	Timing and Synchronization for Time-Sensitive Applications
[93]	O-RAN Alliance	Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components, October 24th 2020
[94]	ENISA	5G SUPPLEMENT to the Guideline on Security Measures under the EECC, December 2020
[95]	UK Bill 216	Telecommunications (Security) Bill, Ordered, by The House of Commons, to be Printed, 24th November 2020
[96]	Explanatory Notes UK Bill 216	Explanatory notes to the Bill, prepared by the Department for Digital, Culture, Media and Sport
[97]	GSMA PRD FS.25	Requirements for Mobile Device Software Security Updates
[98]	Draft NISTIR 8320A	Hardware-Enabled Security: Container Platform Security Prototype
[99]	GSMA Whitepaper	Open networking and security of open-source software deployments – A white paper presenting security considerations for practical deployment, January 2021
[100]	GSMA Report	Open-Source Software Security – A research summary, December 2020
[101]	European Commission	The EU's Cybersecurity Strategy for the Digital Decade, 16 December 2020
[102]	Positive Technologies	5G Standalone core security research
[103]	Trusted Connectivity Alliance	Protecting Subscriber Privacy in 5G, July 2020
[104]	NGMN Alliance	5G Smart Devices Supporting Network Slicing, 15 December 2020
[105]	5GJA15_107r1	Proposal for Subscription based 5G Core selection for Roaming, Deutsche Telekom
[106]	3GPP TS 22.280	Mission Critical Services Common Requirements; Stage 1
[107]	3GPP TS 22.179	Mission Critical Push to Talk (MCPTT); Stage 1
[108]	3GPP TS 22.281	Mission Critical Video services
[109]	3GPP TS 22.282	Mission Critical Data services
[110]	GSMA Report 2017	GSMA – Future Networks – An Introduction to Network Slicing https://www.gsma.com/futurenetworks/resources/an-introduction-to-network-slicing-2/
[111]	3GPP TS 28.530	Aspects; Management and orchestration; Concepts, use cases and requirements

Ref	Doc Number	Title
[112]	3GPP TS 23.502	Procedures for the 5G System (5GS); Stage 2
[113]	GSMA PRD FS.30	Security Manual
[114]	NIST SP 800-204B	Attribute-based Access Control for Microservices-based Applications Using a Service Mesh, Draft, January 2021.
[115]	FCC CSRIC WG2 report Dec 2020	Report on Review & Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture
[116]	3GPP TS 33.401	3GPP System Architecture Evolution (SAE); Security architecture
[117]	Jeremy Horwitz	South Korean carriers agree to build single 5G network, saving money and time https://venturebeat.com/2018/04/11/korean-carriers-agree-to-build-single-5g-network-saving-money-and-time/
[118]	Yue Cao and others	A side channel vulnerability that allows attacker hijacking TCP connection under LTE/5G Network
[119]	CyberSecurity Magazine	Why 5G will lead to improved security for mobile communications https://cybersecurity-magazine.com/why-5g-will-lead-to-improved-security-for-mobile-communications/
[120]	Aruba Networks	Comparing 5G to Wi-Fi 6 from a security perspective https://blogs.arubanetworks.com/corporate/comparing-5g-to-wi-fi-6-from-a-security-perspective/
[121]	3GPP TS 23.540	3GPP; Technical Specification Group Core Network and Terminals; 5G System; Technical realization of Service Based Short Message Service; Stage 2
[122]	3GPP TS 29.577	Technical Specification Group Core Network and Terminals; 5G System; IP Short Message Gateway and SMS Router for Short Message Services; Stage 3
[123]	3GPP TS 29.578	Technical Specification Group Core Network and Terminals; 5G System; Mobile Number Portability Services; Stage 3
[124]	3GPP TS 29.579	Technical Specification Group Core Network and Terminals; 5G System; Interworking MSC For Short Message Services; Stage 3
[125]	3GPP TS 33.535	Technical Specification Group Services and System Aspects; Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)
[126]	GSMA 5GMRR Whitepaper	Issues to be solved for SMS_SBI Interworking for 5G SA Interconnections
[127]	O-RAN Alliance	O-RAN Alliance WG11 Specifications, under WG11 https://orandownloadsweb.azurewebsites.net/specifications
[128]	GSMA PQ.01 PQTN Whitepaper	Post Quantum Telco Network Impact Assessment - https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf
[129]	ENISA	NFV Security in 5G Challenges and Best Practices - February 2022

Ref	Doc Number	Title
[130]	3GPP TS 33.102	3G Security; Security architecture
[131]	3GPP TS 31.102	Characteristics of the Universal Subscriber Identity Module (USIM) application
[132]	3GPP TS 31.105	Characteristics of the Slice Subscriber Identity Module (SSIM) application
[133]	3GPP TS.33.210	Network Domain Security (NDS); IP network layer security
[134]	3GPP TS.33.310	Network Domain Security (NDS); Authentication Framework (AF)
[135]	ETSI ISG ETI 002	Encrypted Traffic Integration (ETI); Requirements definition and analysis
[136]	IETF RFC 5062	Security Attacks Found against the Stream Control Transmission Protocol (SCTP)
[137]	NIST SP 800-207	Zero Trust Architecture
[138]	3GPP TS 33.220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)
[139]	GSMA PQ.02 PQTN Whitepaper	Guidelines for Quantum Risk Management for Telco - https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/09/Guidelines-for-Quantum-Risk-Management-for-Telco-v1.0.pdf
[140]	ETSI QSC	ETSI Quantum Safe Cryptography https://www.etsi.org/technologies/quantum-safe-cryptography
[141]	NIST PQC	NIST Post Quantum Cryptography Standardizationhttps://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
[142]	GSMA FS.42	Binary SMS Filtering Guidelines
[143]	GSMA PQ.03 PQTN Whitepaper	Post Quantum Cryptography – Guidelines for Telecom Use Cases https://www.gsma.com/newsroom/wp-content/uploads//PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf
[144]	NIST SP 800-190	Application Container Security Guide https://csrc.nist.gov/pubs/sp/800/190/final
[145]	Android Security	Disable 2G https://source.android.com/docs/security/features/cellular-security/disable-2g
[146]	ISO/IET 19790:2012	Information technology, security techniques, Security requirements for cryptographic modules.
[147]	ETSI NFV SEC 023	Network Functions Virtualisation (NFV) Release 5; Security; Container Security Specification
[148]	IMT-2020 (5G) Promotion Group	5G Security Report http://www.caict.ac.cn/kxyj/qwfb/bps//202002/P020200204353105445429.pdf
[149]	Ministry of Industry and Information Technology of China	Action Plan for 5G Application (2021-2023) https://www.gov.cn/zhengce/zhengceku/2021-07/13/content_5624610.htm

Ref	Doc Number	Title
[150]	CCSA	Security Assurance Specification (SCAS) for the 5G mobile network product class CN network function https://www.ccsa.org.cn/standardDetail/?standardNum=YD%2FT%204204-2023
[151]	GSMA	NESAS conformance result https://www.gsma.com/security/nesas-results/
[152]	CSRIC	Communications Security, Reliability and Interoperability Council, FCC
[153]	DHS	Program Guidebook: Secure & Resilient Mobile Network Infrastructure & Emergency Comms Program R&D Guidebook (dhs.gov)
[154]	CISA	5G Security and Resilience
[155]	ESF	The Enduring Security Framework
[156]	GSMA CVD Programme	https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/
[157]	GSMA Whitepaper	GSMA whitepaper “Open networking and security of open-source software deployments”

2 Summary of 5G Security Features

2.1 Overview

5G delivers security enhancements over earlier generations of mobile and Wi-Fi technologies. Some of the key security features in the 5G specifications are described in this section. For further details please refer to the appropriate 3GPP standards, such as TS 23.501 [31] and TS 33.501 [1].

2.2 Unified Authentication Framework & Access-Agnostic Authentication

The following is a list of Unified Authentication Framework & Access Agnostic Authentication features:

- Access security is managed in a unified manner whereby the Network Function (NF) Authentication Server Function (AUSF) enables a unified framework for 3GPP and non-3GPP accesses. No access type limitation exists over 3GPP access or non-3GPP access. Release 15 supports unified authentication to 3GPP and Untrusted non-3GPP accesses. With Release 16 this is extended to all access types, including trusted non-3GPP access.
- Unlike Long Term Evolution (LTE), starting with the NF Non-3GPP Inter-Working Function (N3IWF) in Release 16, 5G includes a single authentication infrastructure for both 3GPP access and non-3GPP access. Authentication methods used include 5G AKA, Extensible Authentication Protocol – Authentication and Key Agreement (EAP-AKA) and any Extensible Authentication Protocol (EAP) method.
- Any method can be used to authenticate the User Equipment (UE) over both access types.

2.3 Primary Authentication and Secondary Authentication

The following is a list of Primary Authentication features:

- Newly developed 5G AKA and EAP–AKA' (both are mandatory to be supported for the UE and the serving network).
- EAP-TLS [13], which may be used in isolated deployments and EAP-TLS 1.3 is supported.
- AUSF is the authentication server function in the home network which terminates the authentication procedure, unlike LTE where it is terminated in in the visited network Mobility Management Entity (MME).
- The following is a list of Secondary Authentication features: It is optional between a UE and an external data network.
- Supports authentication between the UE and external DN-AAA by any EAP method
- The SMF (Session Management Function) shall perform the role of the EAP Authenticator.

2.4 Increased Home Control

In the case of both EAP-AKA' and 5G AKA, the AUSF receives confirmation of UE if successfully authenticated and Unified Data Management (UDM) is informed about the authentication result. The final device authentication to a visited network is only completed after the home network has checked the authentication status of the device in the visited network.

Binding serving network ID to session keys ensures that they are used only by the roaming network that proved it is actively serving the roaming UE, and that the UE is reassured that the serving network is the intended one.

Useful in preventing fraud, e.g. registering the subscribers serving Access Management Function (AMF in UDM if UE is not present in the visited network, can be detected

Note: For roaming users the Home-Public Land Mobile Network (HPLMN) will send the Subscription Permanent Identifier (SUPI) after successful completion of the authentication procedure by the HPLMN, which can support lawful intercept solutions.

2.5 Enhanced Subscriber Privacy

The following are Enhanced Subscriber Privacy features:

- 5G introduces a Subscription Concealed Identifier (SUCI), a privacy preserving identifier concealing the SUPI. Unless configured otherwise, SUCI is generated using the Elliptic Curve Integrated Encryption Scheme (ECIES) as a protection scheme based on the home operator’s Home Network Public Key known to its subscribers.
- When a non “null-scheme” protection scheme is enabled, the privacy preserving SUCI will be sent over the air interface that prevents tracking of users by “IMSI catchers”. Note - Null-scheme would provide no privacy protection over the air interface, but it may be required by some regulatory environments.
- Concealing the SUPI is not a mandatory feature and thus depends on both the UE to support and the carrier to enable. It also requires that the Physical SIM (pSIM) or

Embedded SIM (eSIM) is provisioned with the public key of the operator's home network. If a user upgrades to a 5G-SA capable device, but reuses the previous pSIM, which is a non-5G-SA configured for SUCI management as per 3GPP TS 31.102 [131], SUPI concealing would not be supported by the UE regardless of the configuration of the carrier.

- It is strongly recommended that carriers enable a non "null scheme" protection and that they ensure all UEs are provisioned with the necessary pSIM or eSIM for this critical privacy feature to operate globally.
- SUPI is decoupled from the paging procedure, i.e. no paging of the UE using SUPI is allowed, and paging occasions use temporary identifier.
- 5G requires the use of Global Unique Temporary Identifier (5G-GUTI) with stricter temporary subscription identifier refreshment.
- Use of Initial Non-Access Stratum (NAS) message ciphering.
- Special care should be given to the privacy protection with CDRs that leave the home network because these will need to include the SUPI to allow billing, accounting and monitoring processes. Hence, it is advised that CDR records that are transferred from one network to the other should be encrypted.
- Implementing a robust Key Management System (KMS) is essential to secure the encryption and integrity of CDRs during their transfer, ensuring compliance and data protection in a 5G landscape. This KMS is important in safeguarding sensitive data against unauthorised access, especially in the complex and dynamic networks characteristic of 5G technology.

2.6 RAN Security

The following is a list of RAN-Security features:

- Support of User Plane (UP) integrity in addition to confidentiality protection.
- Mandatory Support of Datagram Transport Layer Security (DTLS), in addition to IPsec, for backhaul control traffic (N2) and handover (Xn).
- Mandatory Support of DTLS and IPsec ESP and IKEv2 certificates-based authentication with confidentiality, integrity and replay protection on internal (CU/DU) RAN with the (F1) signalling interface connecting the gNB-CU to the gNB-DU and the E1 signalling interface connecting the gNB-CU-CP).
- Support for certificate enrolment mechanism and the Next Generation Node B (gNB) supports software updates function verification before installation.
- Support PDCP Counter check to detect maliciously inserted packets.
- Implement stateful SCTP inspections to remediate vulnerabilities identified in RFC 5062[136], in which the SCTP inspections can be host-based or using an inline firewall for interfaces Xn-C, E2, and E1.

2.6.1 Security for Integrated Access and Backhaul in EN-DC

Integrated Access and Backhaul (IAB) as specified in 3GPP TS 23.501 [31] enables wireless in-band and out-of-band relaying of NR Uu access traffic via NR Uu backhaul links. See Figure 1 for the IAB architecture for 5GS.

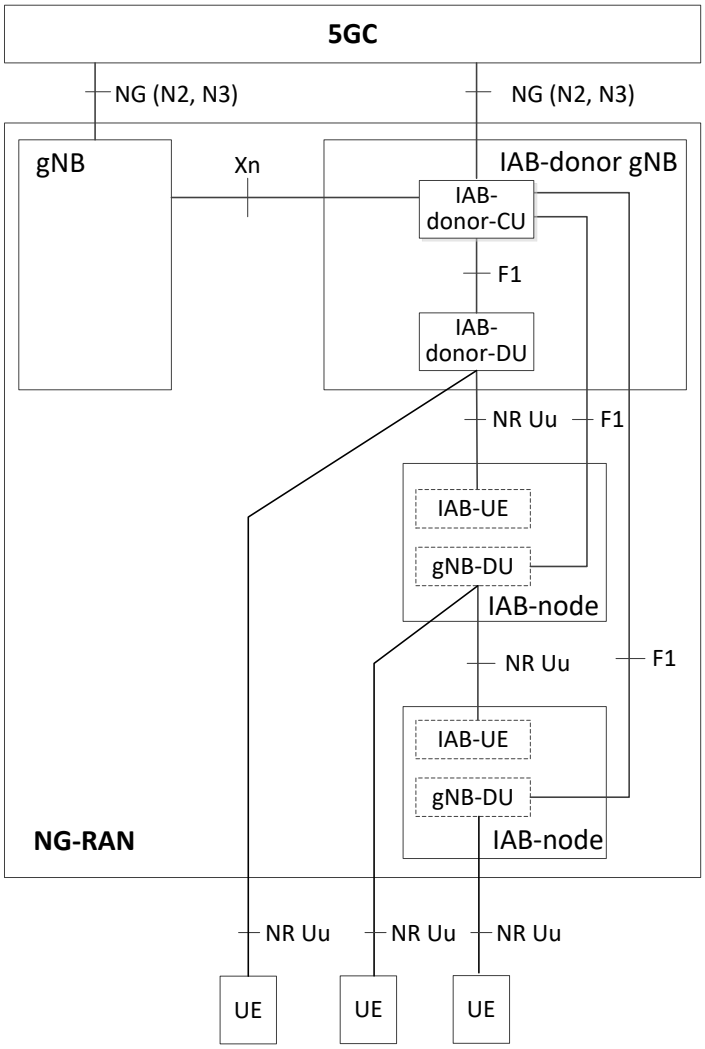

Figure 1 – IAB architecture for 5GS

The following is a list of Security for Integrated Access and Backhaul in EN-DC:

- IAB uses the CU/DU architecture, the IAB operation via F1 (between IAB-donor and IAB-node) is invisible to the 5G Core Network.
- IAB performs relaying at layer-2, supports multi-hop backhauling and dynamic topology updates.
- The IAB-node (IAB-UE).
    - Supports ciphering, integrity protection and replay protection of NAS-signalling. between the IAB-UE and the 5G Core Network and IAB-UE and the IAB donor.
    - IAB-node (IAB-UE) and the 5G Core Network supports mutual authentication.
- IAB donor supports ciphering, integrity protection and replay protection of RRC-signalling between the IAB donor and the IAB-node (IAB-UE).
- IAB-node (gNB-DU) and the IAB-donor support a secure environment for storage of sensitive data, execution of sensitive functions, execution of parts of the boot process and assurance of the secure environment's integrity.

- F1 interface between the IAB-node (gNB-DU) and the IAB-donor-CU:
    - F1-C interface shall support confidentiality, integrity and replay protection.
    - All management traffic carried over the link shall be integrity, confidentiality and replay protected.
    - gNB DU-CU F1-U interface for UP supports confidentiality, integrity and replay protection for the UP.
    - F1-C and management traffic carried over the Central Unit Distributed Unit (CU-DU) link shall be protected independently from F1-U traffic.
    - IKEv2 Pre-shared Secret Key (PSK) authentication shall be supported.
    - F1-U and F1-C interfaces support IPsec ESP and IKEv2 certificates-based authentication.
    - F1-C interface may support DTLS (optional).
- Support for authentication and authorisation of IAB-node.
- Protection of management traffic between IAB-node and OAM.

2.7 Service Based Architecture

The following is a list of Service Based Architecture features:

- NFs support Hypertext Transfer Protocol version 2 (HTTP/2) over Transport Layer Security (TLS) with both server and client-side certificates.
- Use of the OAuth 2.0 authorisation framework for authorisation of NF service access
- Higher level of granularity for the authorisation tokens allows specific service operations and/or resources/data sets per NF consumer.
- Provides confidentiality, authentication, integrity protection and authorisation for all service-based interfaces within the Public Land Mobile Network (PLMN).
- Between PLMNs, interconnect security is provided for all service-based signalling traffic, which solves the IP Exchange (IPX) network security issue prevalent in LTE networks.
- Service Communication Proxy (SCP) provides additional communication security (e.g. authorisation of the NF Service Consumer to access the NF Service Producer API), load balancing, monitoring, overload control, etc) when used in indirect communications mode between NFs.
- Non-SBA interfaces internal to the 5G Core such as N4 and N9 shall be confidentiality, integrity, and replay protected.

NF Service Consumers may support the Client Credentials Assertion (CCA), which enables the NF Service Consumer to authenticate towards the receiving end point (NRF, NF Service Producer).

The Service Based Architecture (SBA) security architecture in Figure 2illustrates the different sets of security features as described in TS 33.501 [1]:

- Network access security (I).
- Network domain security (II).
- User domain security (III).
- Application domain security (IV).

- SBA domain security (V).
- Visibility and configurability of security (VI).

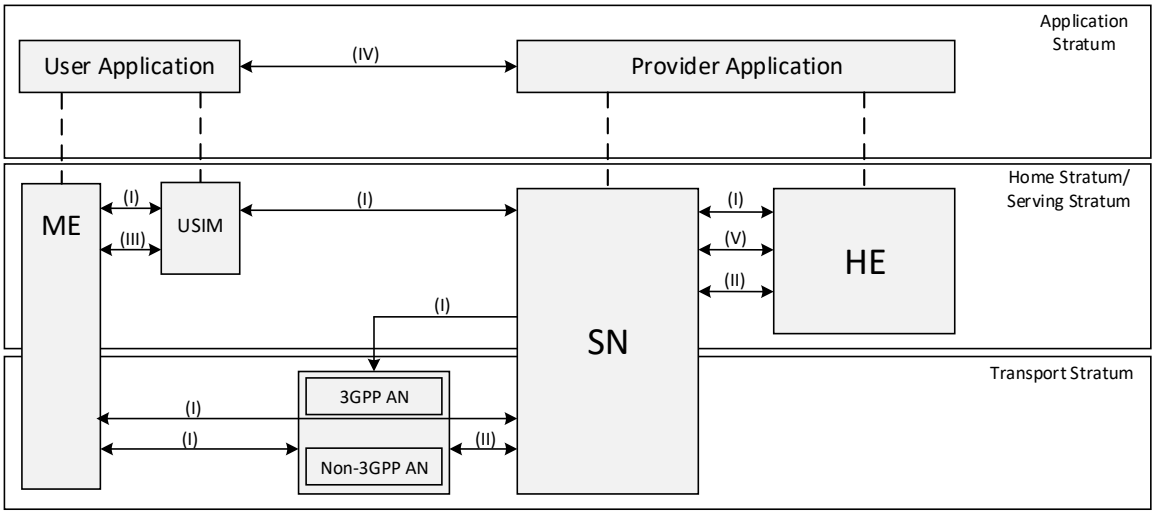

Figure 2– Overview of the security architecture

2.8 Roaming Security

2.8.1 Roaming interfaces between PLMNs

Roaming interfaces shall be provisioned with confidentiality, integrity, and replay protected. Origin of messages should be authenticated. N32-f interface may use either Protocol for N32 Interconnect Security (PRINS) or TLS. Accordingly, one of the following additional transport protection methods shall be applied between Secure Edge Protection Proxy (SEPP) and IPX provider for confidentiality and integrity protection:

- Network Domain Security / Internet Protocol (NDS/IP) as specified in TS 33.210 [133] and TS 33.310 [134], or
- TLS VPN with mutual authentication following the profile given in clause 6.2 of TS 33.210 [133] and clause 6.1.3a of TS 33.310 [134]. The identities in the end entity certificates shall be used for authentication and policy checks, with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [2].

It is up to the operators' decisions to use cryptographic solutions or other mechanisms to protect N9, as described in the section 9.9 of 3GPP TS 33.501 [1].

Recommendations and guidelines, specified in GSMA Permanent Reference Document (PRD) FS.37 [64] v3.2 shall be applicable to the N9 interface traffic.

2.8.2 Secure Edge Protection Proxy (SEPP)

SEPP, a non-transparent proxy, protects the messages that are sent over the N32 interface between Service Consumers and Service Producers. See sections 3.1 and 8.3 for more details on the SEPP and for the inter-PLMN signalling message flow over the N32 interface.

The receiving SEPP should be able to verify whether the sending SEPP is authorised to use the PLMN ID or SNPN ID in the received N32 message.

2.9 5GS-EPS Interworking Security

The following is a list of 5GS-EPS Interworking Security features:

- Security for seamless mobility between Evolved Packet System (EPS) and 5G system.
- Different UE connected states (i.e. security handling in state transition).
- Support of legacy security measures for core network messages i.e. SS7, GPRS Tunnelling Protocol (GTP), Diameter monitoring, filtering and threat intelligence [6], [7], [9].[64]
- Restriction of interworking functions to a need-to-use basis (i.e. not every node should be allowed to use all interworking features, only those that really need it for their purpose).

2.10 LTE-NR Dual Connectivity

The following is a list of LTE-NR Dual Connectivity:

- EPC enhancements to support 5G New Radio (NR) via Dual Connectivity.
- DC provides higher per-user throughput and mobility robustness, and load balancing by using 2 base stations.
- 5G NR attached to 4G EPC using Dual Connectivity approach.
- LTE security algorithms and procedures similar to LTE are used.

2.11 Non-Public Networks (NPN)

The following is a list of NPN features:

- NPNs support additional authentication methods other than AKA e.g. EAP-TLS.
- The serving network name (SN Id) = PLMN*:NID, PLMN* = PLMN ID or a shortened one.
- The UE modifies its CAG ID list only after receiving an integrity protected NAS message.
- NPNs support SUPI privacy. Support exists for PNI-NPN authentication. K_{AUSF} key derivation is based on the EAP-method credentials in the UE and AUSF, for non-EAP-AKA' authentication.
- Core Network (CN) security should use the 3GPP Security aspects of Common API Framework (CAPIF) in TS 33.122 or equivalent security.
- For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, OAuth 2.0 authorisation as specified in TS 33.501 [1] clause 13.4.1.2 applies.
- SNPN and Credentials Holder communicate via SEPPs with the security requirement defined in clause 2.7.

2.12 5G Single Radio Voice Call Continuity (SRVCC) from NR to UTRAN

SRVCC from UTRAN to 5G shall not be allowed. The MSC should never know K_{AMF} nor should K_{AMF} be revealed to entities other than an AMF. When SRVCC moves from 5G to UTRAN, AMF derives a new K_{ASME_SRVCC} key.

2.13 Security for URLLC (Ultra-Reliable Low-Latency Communication) services

5G architecture includes the ability to have redundant UP paths based on dual connectivity. Figure 3 illustrates a 5G architecture with redundant UP paths over the N3 interface. Similarly, the N9 roaming interface can have redundant UP paths.

If encryption is used for UP traffic, then the two redundant PDU sessions should have the same setting for encryption and integrity protection. Further, UP traffic, carried over N3 and N9 interfaces, should adhere to the GTP-U security recommendations and guidelines, specified in the GSMA PRD FS.37 [64]. See sections 2.8.1, 5.3, 8.9, and 11 for more details. Figure 3

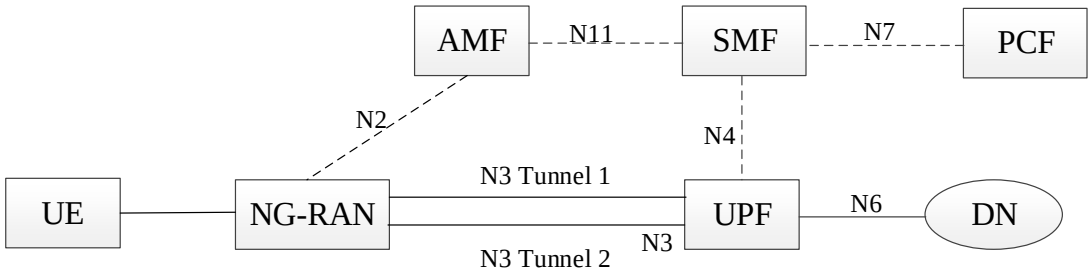

Figure 3 – Redundant transmission with two N3 tunnels between the UPF and a single NG-RAN node

2.14 Security For Time Sensitive Communications (TSC)

In Release 16, the 5G System supports TSC:

- Access security for a TSC-enabled UE.
- Protection of UP data in TSC including (g)PTP control messages.

It is defined in IEEE 802.1 Working Group Time Sensitive Networking (TSN) standards, IEEE 802.1AS-Rev [92], which is depicted in Figure 4:

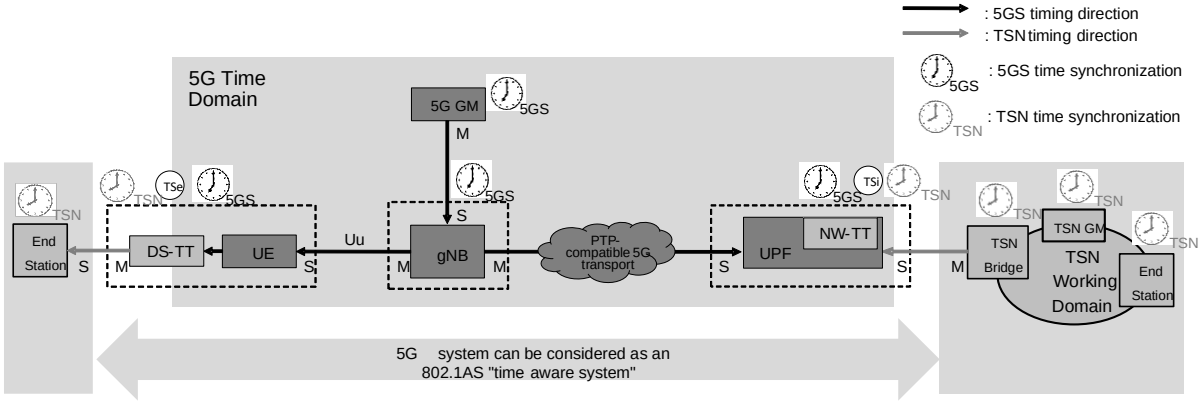

Figure 4 – 5G system modelled IEEE 802.1AS compliant for TSN time synchronization

2.15 Security for 5GLAN services

Release 16 introduced a new N19 reference point between two PSA (PDU Session Anchor) User Plane Function (UPF) for 5G LAN-type service as shown in Figure 5. The UE access to the 5G LAN i.e. authentication and authorisation is performed via secondary authentication procedures. Consistent UP security policy for All PDUs associated with a specific 5G LAN group should be applied.

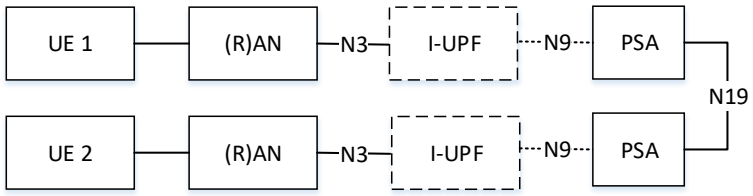

Figure 5 – N19-based user plane architecture in non-roaming scenario

2.16 Security for Trusted non-3GPP access to the 5G core network

Security of trusted non-3GPP access to a 5G Core Network is achieved when a UE registers via a Trusted Non-3GPP Access Network (TNAN) using Trusted Non-3GPP Access Point (TNAP) and Trusted Non-3GPP Gateway Function (TNGF), as depicted in Figure 6.

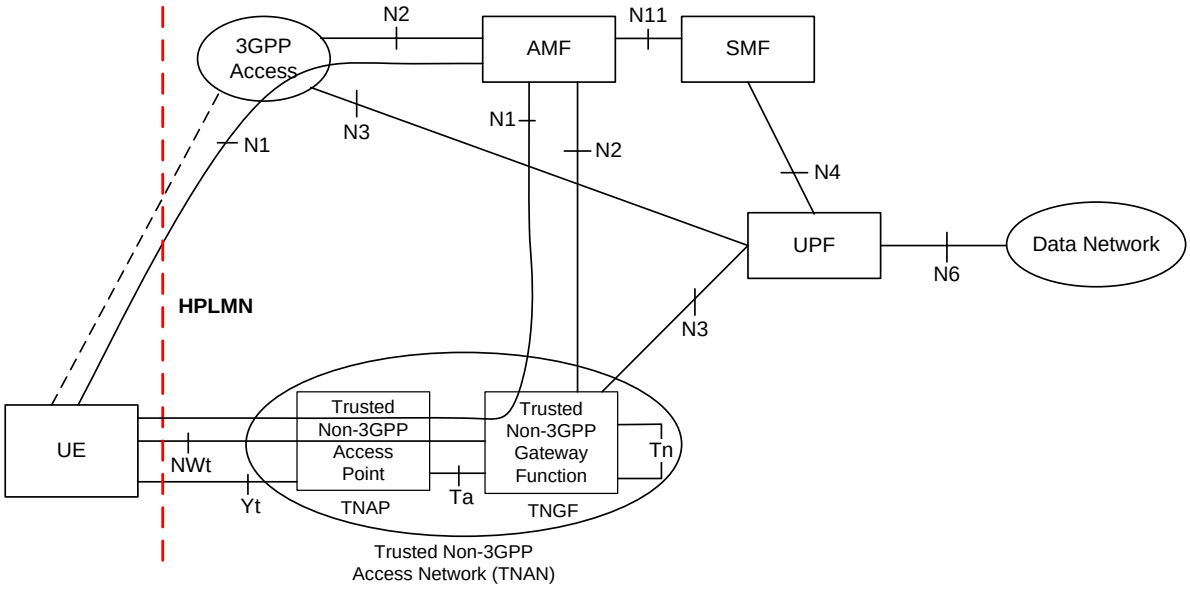

Figure 6 – Non-roaming architecture for 5G Core Network with trusted non-3GPP access

The following are the procedural steps for trusted non-3GPP access to the 5G core network:

- UE registers to the 5G Core Network via the TNAN using the EAP-5G procedure.
- The security relies on Layer-2 security between UE and TNAP, which is a trusted entity so that no IPsec encryption is necessary between UE and TNGF, i.e. NULL encryption is sufficient for the UP and signalling.
- Separate IPsec SAs may be used for NAS transport and PDU Sessions.
- Authentication for trusted non-3GPP access based on EAP-5G.

- Authentication for devices that do not support 5G Core Network NAS over WLAN access based on EAP-AKA'.
- Support for subscriber privacy for Non-5G-Capable over WLAN (N5CW) over trusted WLAN access (5G-GUTI and SUCI).
- Key hierarchy for trusted non-3GPP access as shown in Figure 7.

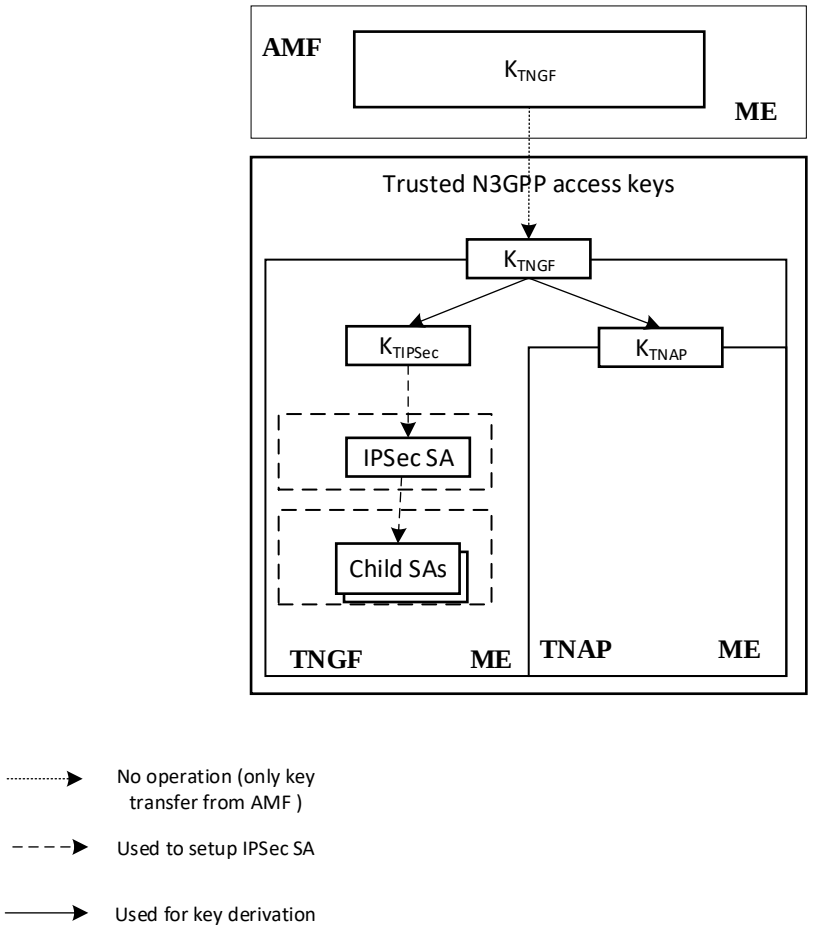

Figure 7 – Key hierarchy for trusted non-3GPP access

2.17 Security for wireline access to the 5G core network

A Wireline 5G Access Network (W-5GAN) connects to the 5G Core via a Wireline Access Gateway Function (W-AGF). The W-AGF interfaces' traffic for 5G Core Network CP and UP functions is sent through N2 and N3 interfaces, respectively.

A 5G Residential Gateway (5G-RG) can connect via a NG-RAN and via a W-5GAN with multiple N1 instances:

- UE connected to a 5G-RG, see Figure 8, or
- Fixed Network Residential Gateway (FN-RG), see Figure 9, can access the 5G Core Network via the N3IWF or via the TNGF.

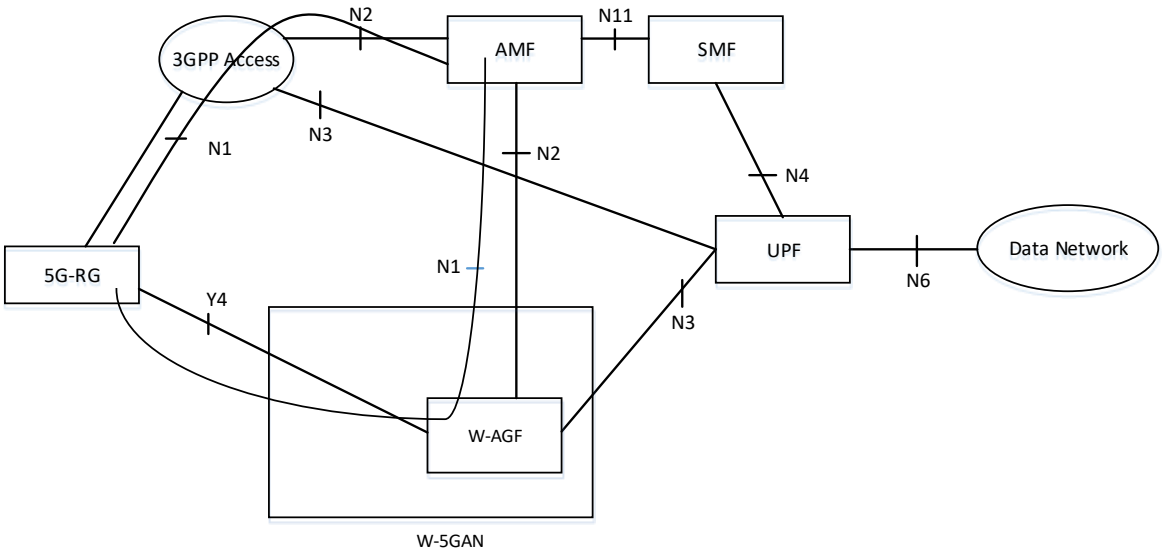

Figure 8 – Non-roaming architecture for 5G Core Network for 5G-RG with W-5GAN and NG RAN

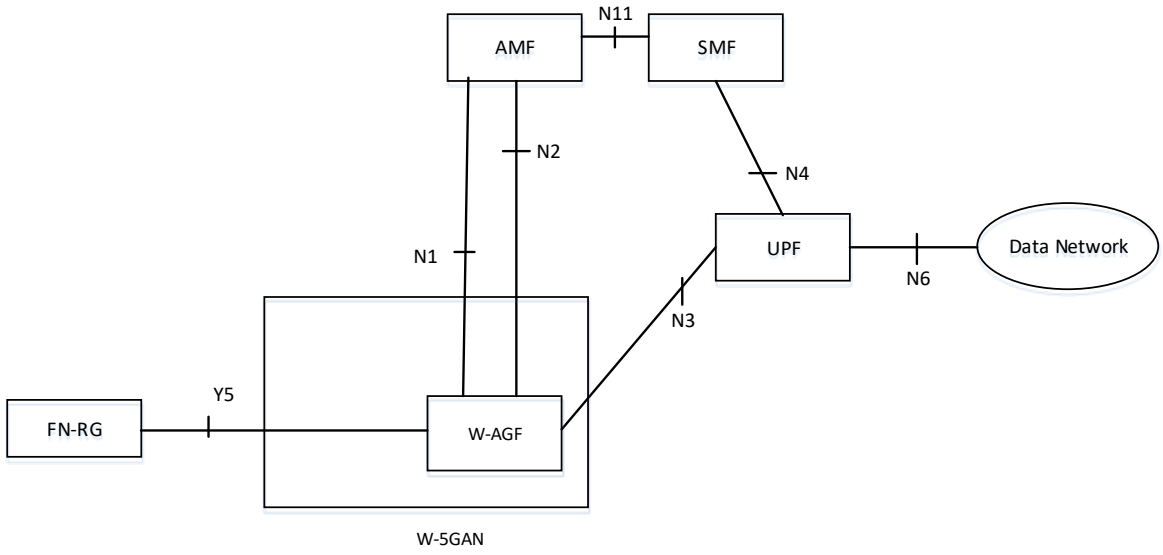

Figure 9 – Non-roaming architecture for 5G Core Network for FN-RG with W-5GAN and NG RAN

To support Wireless and Wireline Convergence for the 5G system, two new network entities, 5G-RG and FN-RG are introduced:

- Support for 5G-RG Authentication via NG-RAN and W-5GAN (authentication method EAP-5G).
- 5G-RG supports 5G-AKA and EAP-AKA' and authenticated by the 3GPP home network.

The FN-RG is authenticated by the W-AGF. Authentication method used for FN-RG is defined by the Broadband Forum or CableLabs and is out of scope of 3GPP.

5G-RG supports subscriber privacy for wireline access (5G-GUTI and SUCI). N2 interface between the W-5GAN and the AMF protected with IPsec ESP and IKEv2 certificates-based authentication. N3 interface between the W-5GAN and the UPF protected with IPsec ESP and IKEv2 certificate-based authentication. Support for authentication for non-5G capable devices (N5GC) behind residential gateways (RGs) in private networks or in isolated deployment scenarios wireline access based on EAP methods.

It is advisable that data validity be performed prior to any encryption taking place, as identified in ETSI ISG ETI 002 [135] and as NIST SP 800-207 [137] standard on Zero Trust Architecture specifies. Section 8.9.1 (Zero Trust Methodology) provides more details on Zero Trust.

Telecom operators are encouraged to choose a resilient encryption solution with advanced capabilities to bolster security measures.

2.18 UE Security Visibility and Configurability

3GPP TS 33.501 [1] clause 5.10.1 states that the UE must provide the following security information to the applications in the UE (e.g. via APIs) on a PDU session granularity:

- AS confidentiality (AS confidentiality, Confidentiality algorithm, bearer information).
- AS integrity: (AS integrity, Integrity algorithm, bearer information).
- NAS confidentiality: (NAS confidentiality, Confidentiality algorithm).
- NAS integrity: (NAS integrity, Integrity algorithm).

As of the writing of the current version of this document, no commercial UE supports this. It is strongly recommended to chipset manufacturers and OEMs to enable and support these mandatory requirements, given their potential impact in mitigating fraud and abuse (e.g. SMS blasters disseminating phishing messages).

UE supports a Man Machine Interface to individually disable/enable ME's radio technologies, regardless of PLMNs such as GSM/EDGE, WCDMA, Evolved Universal Terrestrial Radio Access (E-UTRA), and NR. UE shall support a secure mechanism for the home operator to individually disallow/allow the ME's radio technologies for access to the network, regardless of PLMNs. Allowing/disallowing are at least for GSM/EDGE, WCDMA, E-UTRA, and NR radios.

2.19 Cryptographic Enhancements

The following is a list of Cryptographic enhancements:

- TLS Profile:
    - Support in OCSP Status extension.
    - TLS 1.2 - support only cipher suites with AEAD and PFS (e.g. ECDHE, DHE).
    - Removal of TLS Cipher suites without encryption.
- IKEv2 Profile:

  - Removal of weaker cryptographic algorithms.
  - Confidentiality: ENCR_AES_CBC with 128-bit key length.
  - Pseudo-random function: PRF_HMAC_SHA1.
  - Integrity: AUTH_HMAC_SHA1_96.
  - Diffie-Hellman group 14 (2048-bit MODP) and RSA Digital Signature – no longer recommended as it uses PKCS#1v1.5 padding.

- CRL profile:

  - Signature algorithm - RSAEncryption no longer recommended.
  - MD5 MD2, and SHA-1 shall not be supported.
  - ECDSA: Except curve25519, ed25519, and W-25519, elliptic curve groups of less than 256 bits shall not be supported. A key length of at least 384-bit shall be supported.

To address the security challenges presented by emerging quantum technologies, a dedicated GSMA PQTN group is following this topic. Although its first version of GSMA PQ.01 Post Quantum Telco Network Impact Assessment Whitepaper [128] is not addressing the Post-Quantum Cryptography (PQC) aspect, it will be taken into consideration in the coming versions. In addition, GSMA PQ.02 whitepaper - Guidelines for Quantum Risk Management for Telco whitepapers [139] - addresses risk exposure and risk management in the post quantum world for telecommunications ecosystems.

In February 2024 GSMA PQTN published PQ.03 whitepaper – Post Quantum Cryptography - Guidelines for Telecom Use Cases [143]. Various standards bodies are working on quantum-safe cryptographic algorithms, addressing the challenges of the quantum era. Those include and are not limited to ETSI QSC [140], NIST PQC [141].

2.20 Network Slice Security

Authorisation from a home/serving PLMN is required for a UE to gain access to a network slice. UE is granted an authorised S-NSSAI only after it has completed successfully primary authentication. Network Slice Specific Authentication and Authorisation (NSSAA) can be associated with specific S-NSSAIs.

EAP framework is used for NSSAA between the UE. SEAF/AMF performs the role of the EAP Authenticator and communicates with an AAA-S via the Network Slice Specific Authentication and Authorisation Function (NSSAAF). NSSAAF provides any AAA protocol interworking with the AAA-S.

The SSIM [132], application on Universal Integrated Circuit Card (UICC), can be involved in the NSSAA procedure as follows:

- Support for AAA Server-side Network Slice-Specific Re-authentication and Re-authorisation procedure.
- Support for AAA Server triggered Slice-Specific Authorisation Revocation.

The following describes security for network slice management:

- Support for mutual authentication between the management service consumer and the management service producer using TLS, based on either client and server certificates or pre-shared keys for TLS 1.2 or TLS 1.3.
- Support for OAuth-based authorisation and local policy authorisation of management service consumer's requests. The core network should support slice specific authorisation and authentication.
- For data in transit, Network Slice must be always re-affirmed to avoid slice hijacking.

See Section 14 for more details about network slicing.

2.21 Authentication and Key Management for Applications (AKMA)

3GPP TS 33.535 [125] describes the Authentication and Key Management for Applications. By leveraging on the 5G subscriber's credentials, AKMA enables the authentication and generation of keys for the subscriber's application service, such as the Internet of Things (IoT) and vertical applications.

AKMA is also supported within the scope of the 5G Network Exposure Function (NEF), hence may allow external Application Functions (AF) to interwork securely with the 5G network via the specified APIs for AKMA-related operations.

Figure 10 describes the AKMA architecture with the AKMA Anchor Function (AAnF) interworking with the AUSF and internal AF, and the NEF with external AF.

Since AKMA leverages on the 5G subscriber's credentials, it allows the subscriber to be authenticated with the AKMA-supported application in an automated manner without any stored credentials such as password. This is crucial for constrained devices, such as for IoT.

3GPP TS 33.501 [1] has specified that the security aspects of Message Service for MIoT over the 5G System (MSGin5G) shall be based on AKMA. The MSGin5G Server shall act as the AF while the MSGin5G Client as the UE, where both shall support authentication and authorisation based on the AKMA framework.

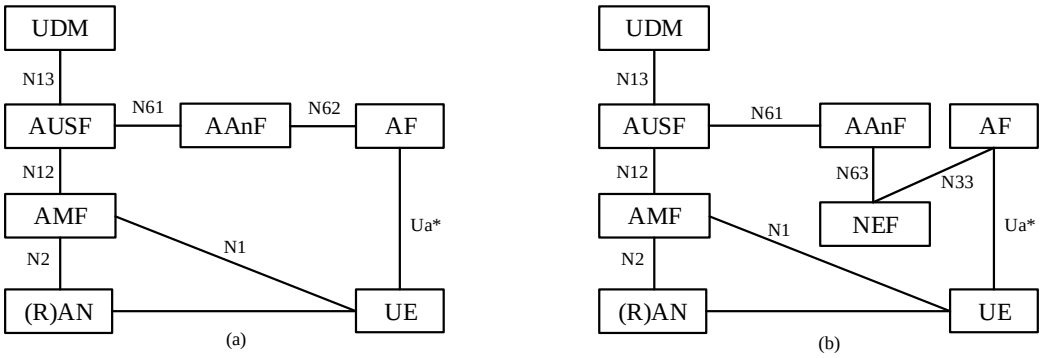

Figure 10– AKMA Architecture for (a) internal AFs and (b) external AFs [125]

2.22 Generic Bootstrapping Architecture (GBA) enhancements

3GPP TS 33.220 [138] describes Generic Bootstrapping Architecture. GBA is a generic mechanism enabling the establishment of shared keys between the UE and any Application

Server (NAF in GBA description) thanks to 3GPP subscriber authentication (AKA authentication).

New security features of GBA have been specified in 5G:

- Annex N (normative) of 3GPP TS 33.220 [138] specifies support of SBA in GBA.

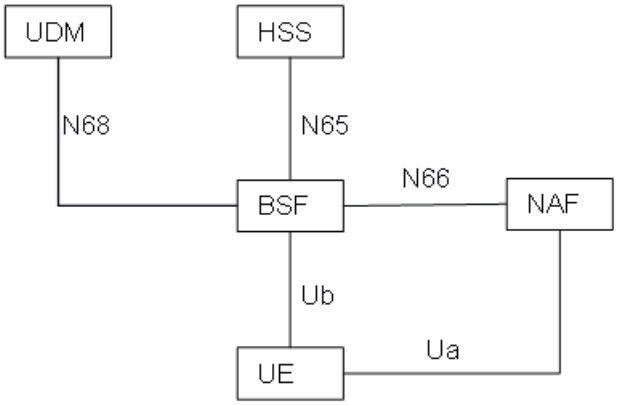

Figure 11– System Architecture to support SBA in reference point representation

Annex O (normative) of 3GPP TS 33.220 [138] covers the aspects specific to the GBA Ua protocol based on DTLS.

Annex P (normative) of 3GPP TS 33.220 [138] describes how to secure access to NAF using Object Security for Constrained (REST Conformant (RESTful) Environment (OSCORE).

3 New Elements and Functions in 5G Security Architecture

3.1 SEPP: Secure Edge Protection Proxy (Network Entity, NF)

The SEPP is the entity sitting at the perimeter of the PLMN network to interconnect with the SEPP of another PLMN directly, via IPX providers or roaming hubs. It implements ALS for all the signalling messages exchanged between any two NFs (behind the SEPPs) across two different PLMNs and provides protection against eavesdropping on sensitive information and replay attacks.

It also provides the following:

- End-to-end authentication during N32 setup for security method selection, integrity and confidentiality protection via signatures and encryption of all HTTP/2 roaming messages.
- Key management mechanisms for setting the required cryptographic keys and performing the security capability negotiation procedures.
- Message filtering and policing, topology hiding and validation of JavaScript Object Notation (JSON) objects including cross-layer information checking with address information on the IP layer.

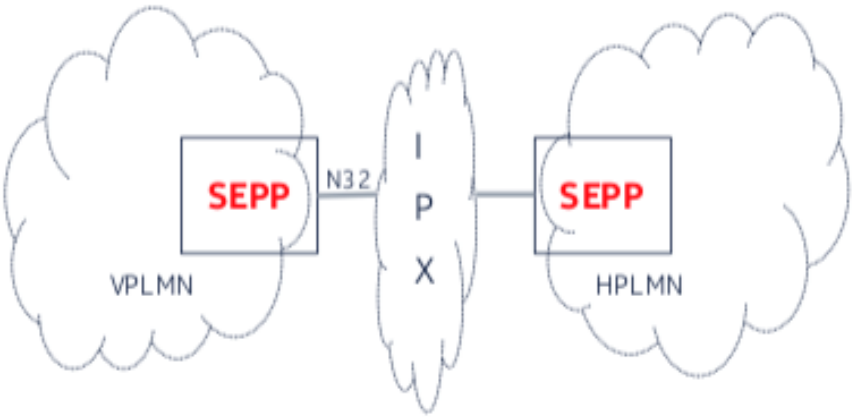

Figure 12 - New SEPP and N32 Interface for 5G inter-operator working

Note: The information transfer over the N32 interface needs to be encrypted as the N32 interface is also used for sensitive information e.g. sending key material during authentication procedure.

The enhanced security in 5G of the mobile roaming services is introduced to overcome the existing security risks linked to SS7 and Diameter usage. This introduction of a dedicated security node within the 5G standards is a major improvement over the existing practices in 4G/3G/2G networks with SS7 and Diameter by enabling the operator to have control about which signalling messages are visible to roaming intermediaries of the IPX.

For user plane data protection please refer to section 11.

3.2 AMF: Access and Mobility Management function

AMF is responsible to provide the following:

- Lawful intercept (for AMF events and interface to LI System).
- Access Authentication and Authorisation.
- Authentication of UEs connected over N3IWF and TNGF.
- Assigning 5G-GUTI to the UE.
- Slicing support.

3.3 SEAF: Security Anchor Function (in serving network's AMF)

Security Anchor Function (SEAF) serves as the anchor for security in a 5G serving network. The anchor key K_{SEAF} is provided by the AUSF of the home network during authentication and used for derivation of subsequent security keys.

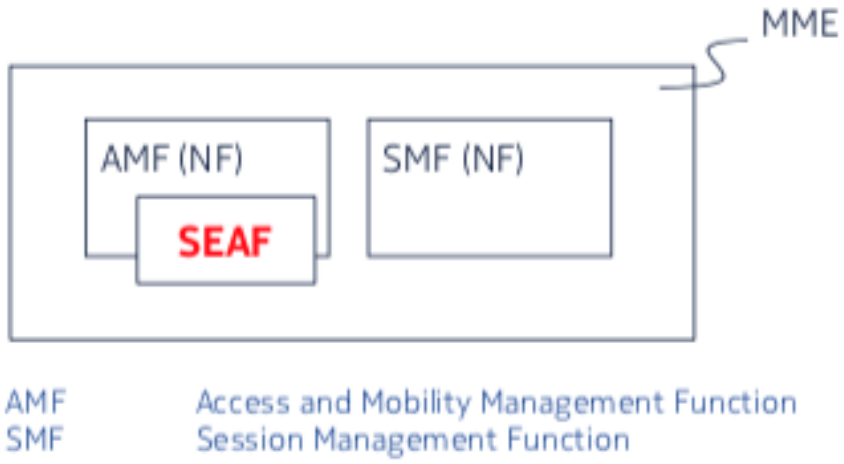

Figure 13 - New SEAF as anchor for security in 5G

Note: The MME is the related functional component in an LTE CN.

3.4 AUSF: Authentication Server Function (in home network)

AUSF creates the authentication vector (5G AV or EAP-AKA' AV) from the home environment AV received from the UDM/ARPF (Authentication Credential Repository and Processing Function). The ARPF is a functional element in the UDM responsible for generation of 5G authentication vectors (5G AVs). It also checks that the requesting AMF/SEAF in the serving network is entitled to use the serving network name. If an EAP authentication method is used, the AUSF takes the role of the EAP server in primary authentication.

In standalone non-public networks (SNPN), the AUSF can act as an authenticator with external authentication server, i.e. AAA.

Release 15 introduced network slicing without authentication. Release 16 supports the Network Slice-Specific Authentication and Authorisation.

Note: TS 33.501 [1] and FS.43 [90] define the requirements for storing the authentication credentials encrypted in a secure hardware component. The requirements for the Hardware Security Module (HSM) can be found in section 3 of this document as part of the section on “Impact of Cloud on 5G Security”.

Note: For roaming users, the HPLMN sends the SUPI after successful completion of the authentication procedure by the HPLMN to assist lawful intercept solutions.

3.5 UDM/ARPF: Unified Data Management/Authentication Credential Repository and Processing Function

UDM/ARPF chooses the authentication method, based on the SUPI. It provides 5G home environment (HE) AV to the AUSF. It retrieves services for user consent parameters and notification if the user consent parameters are changed.

UDM/ARPF supports the delivery of UE Parameters Update (UPU) Data from the UDM to the UE after the UE has successfully registered to the 5G network. The UDM should invoke Nausf_UPUProtection service operation message by including the UPU Data to the AUSF to get UPU-MAC-I_{AUSF} and $Counter_{UPU}$.

3.6 UDM/SIDF: Unified Data Management/Subscription Identifier De-concealment Function

SUCI (concealed subscription identifier) -> SUPI

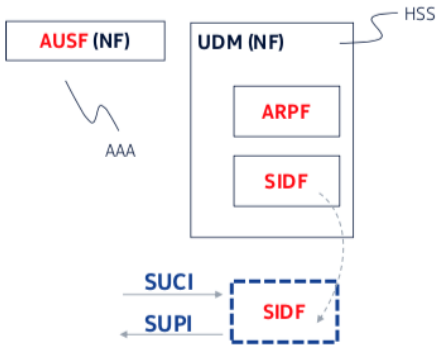

Figure 14 - New elements introduced in 5G for the authentication vector working between SUCI and SUPI

Note: The HSS is the related functional component in a LTE CN.

It is outside the scope of 3GPP's work to define how the Subscription Identifier De-concealment Function (SIDF) for SUCI -> SUPI is implemented as an integrated UDM/SIDF, or as separate SIDF instances.

By design, many functions resident in network functions have been pulled apart and defined as separate functions in 5G. In a Software-Defined-Network it is important to be able to add resources where they are needed most, and not have to add resources to an entire entity. If there is a need for more computing resources for the SIDF, but not for the UDM, then it should be possible to add the necessary resources for the SIDF without impacting the UDM.

3.7 SCP: Service Communication Proxy

SCP provides the following:

- Indirect Communications support between NFs.
- Delegated Discovery from the NRF.

- Message forwarding and routing to a destination NF/NF service.
- Message forwarding and routing to a next hop SCP.
- Communications security (e.g. authorisation of the NF Service Consumer to access the NF Service Producer API), load balancing, monitoring, overload control, etc.

SCP and the SEPP mutually authenticate before forwarding requests.

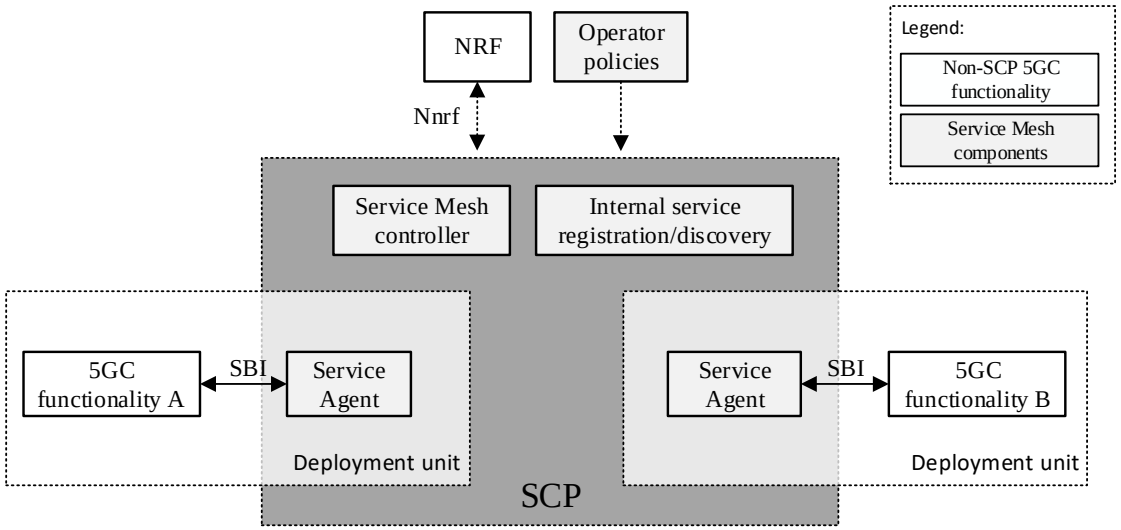

Figure 15 - SCP Service mesh co-location with 5G Core Network functionality

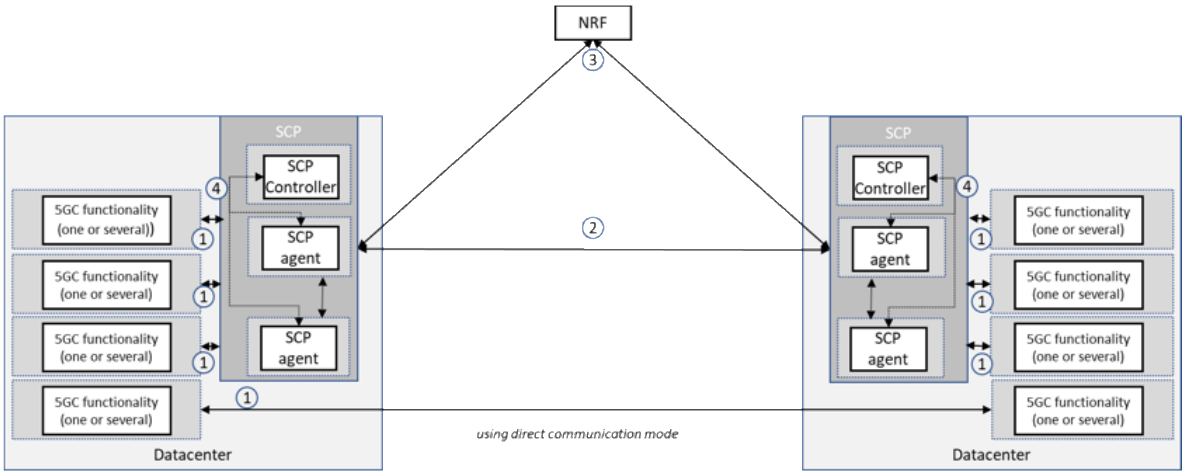

Figure 16 - Overview of SCP deployment

3.8 IPUPS: Inter PLMN UP Security

Operators can deploy UPFs with Inter-PLMN User Plane Security (IPUPS) functionality at the network border to protect against invalid inter PLMN N9 traffic in home routed roaming scenarios as in Figure 17.

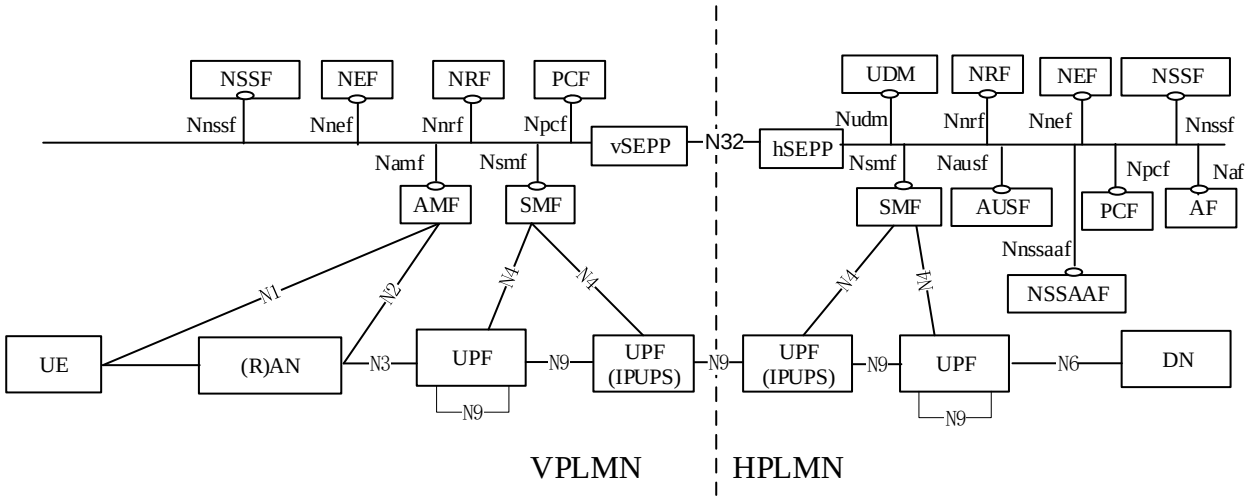

Figure 17 - Roaming 5G System architecture - home routed roaming scenario in service-based interface representation employing UPF dedicated to IPUPS

IPUPS discards malformed GPRS Tunneling Protocol – User Data (GTP-U) messages. IPUPS only forwards GTP-U packets that contain a F-TEID that belongs to an active PDU session and discards all others.

3.9 NSSAAF: Network Slice Specific Authentication and Authorisation Function

The following are the reference points related to NSSAAF:

- N58: Reference point between AMF and the NSSAAF.
- N59: Reference point between UDM and the NSSAAF.
- N83: Reference point between AUSF and NSSAAF.

The NSSAAF handles network slice-specific authentication and authorisation with a AAA Server (AAA-S). If the AAA-S belongs to a 3rd party, the NSSAAF can contact the AAA-S via a AAA proxy (AAA-P).

NSSAAF supports AAA-S triggered Network Slice-Specific Re-authentication and Re-authorisation and Slice-Specific Authorisation Revocation.

The NSSAAF handles access to SNPN using credentials from Credentials Holder (CH) or from Default Credentials Server (DCS) using AAA-S. If the CH or DCS belongs to a third party, the NSSAAF can contact the AAA-S via a AAA-P.

When the NSSAAF is deployed in a PLMN, the NSSAAF supports NSSAA. Whereas, when the NSSAAF is deployed in a SNPN, the NSSAAF can support NSSAA and/or access to SNPN (using credentials from Credentials Holder). It relays EAP messages towards a AAA-S or AAA-P and performs protocol conversion as needed. Further it notifies the current AMF where the UE is of the need to re-authenticate and re-authorise the UE or to revoke the UE authorisation. Table 1 illustrates security related services for Network Slice Specific Authentication and Authorisation that NSSAAF provides.

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnssaaf_NSSAA	Authenticate	Request/Response	AMF
	Re-AuthenticationNotification	Notify	AMF
	RevocationNotification	Subscribe/Notify	AMF

Table 1 – NF services for the NSSAA service provided by NSSAAF

For more details about Network Slicing see the descriptions in section 14.

3.10 AAnF: AKMA Anchor Function

The AAnF performs the following functions:

- Anchor function in the HPLMN. Deployments can choose to collocate AAnF with AUSF or with NEF according to operators' deployment scenarios.
- Store function of the AKMA Anchor Key (K_{AKMA}) for AKMA service, which is received from the AUSF after the UE completes a successful 5G primary authentication.
- Key generation function to be used between the UE and the Application Function (AF) and maintain UE AKMA contexts.
- Interaction function with the AUSF and the AF using Service-based Interfaces. When the AF is located in the operator's network, the AAnF shall use Service-Based Interface to communicate with the AF directly. When the AF is located outside the operator's network, the NEF shall be used to exchange the messages between the AF and the AAnF.

3.11 NSWOF: Non-Seamless WLAN Offload Function

The NSWOF interfaces to the WLAN access network using SWa interface and interfaces to the AUSF using Service Based Interface (SBI).

4 5G Enhancements in Subscription Identifier Privacy

4.1 SUPI and SUCI

The SUPI is a globally unique identifier allocated to each 5G Subscription, equivalent to the International Mobile Subscriber Identity (IMSI) or Network Access Identifier (NAI) and is structured as follows.

MCC || MNC || MSIN *or*
username@123mcc.456mnc.example.com

The Subscription Concealed Identifier (SUCI) is a privacy preserving identifier containing the concealed SUPI, with Mobile Country Code (MCC) and Mobile Network Code (MNC) in the clear and the encrypted Mobile Subscription Identity Number (MSIN), which is encrypted with the Home Network public key of the home operator. Additional parameters are used for home routing and AUSF/UDM selection, key set identifier, ephemeral public key (ECIES scheme), and MAC tag.

Format details of SUPI and SUCI are described in [50].

Protection schemes for concealing the SUPI comprise null-scheme, profile A and profile B, as specified in 3GPP TS 33.501 [1], Annex C. Encryption of the SUPI, or the use of a non-null SUPI encryption scheme, is optional and decided by the network. Encrypting the SUPI also requires having the SIM in the device provisioned with a Home Network public key of the operator.

It is strongly recommended that carriers support and enable a non-null SUPI encryption scheme.

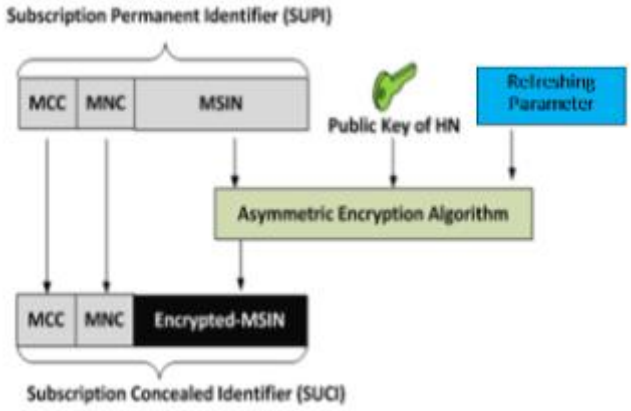

Figure 18 - Illustration of generating a SUCI from SUPI

If the EAP method supports SUPI privacy, the UE may use anonymous SUCI to protect privacy [1].

4.2 5G-GUTI Refresh

It is mandatory to refresh a 5G-GUTI at "initial registration", "mobility registration update", and network triggered Service Request. This feature makes identifying or tracing subscribers, based on 5G-GUTI, impractical.

In addition, there is no longer a paging option based on SUPI. The calculation of the paging frame index and paging occasions is no longer based on SUPI and is instead based on 5G-GUTI. As a result, with this enhancement it is infeasible for false base stations to use paging messages for identifying or tracing subscribers.

4.3 Defeating False Base Stations

The use of SUCI for the initial authentication of the UE to the network prevents false base stations (IMSI catchers or Stingrays) from retrieving the subscriber identity by forcing the UE to attach to the False base Station (FBS). Because of this, it is strongly recommended that carriers support and enable a non-null SUPI encryption scheme. SUPI encryption only protects the subscriber identity from being intercepted but does not protect from other FBS attacks.

Preventing devices to connect to a FBS is not possible but can be mitigated by preventing insecure downgrade to legacy generations (e.g. 2G or 3G), disabling any CSFB optimisation

in the radio network that uses insecure Radio Resource Control (RRC) redirection to 2G or 3G, and configuring the “redir-policy” bit in the Network side (e.g. UDM, etc). The redir-policy bit that will be forwarded to the UE, protects 3GPP release-15 and later mobiles from insecure RRC redirection to 2G and release-18 and later mobiles from insecure RRC redirection to both 2G and 3G. The presence of false base stations can be detected by data in measurement reports from devices and the 5G system like the detection of a 2G false base station is detected in a Mobile Network Operator’s (MNO) network without any 2G deployment or when the received signal of a base station deviates from the expected value.

5 Authentication in 5G

5.1 Overview

Compared to authentication in 2/3/4G networks, 5G authentication is specified in 3GPP TS 33.501 [1] as a mandatory procedure and offers the following novel aspects.

5.2 Authentication Confirmation

As part of authentication, the UE computes a cryptographic checksum (RES*) that binds the challenge Random Number (RAND) issued by the home network to the Universal Subscriber Identity Module (USIM) as well as the name of the serving network as seen by the UE. This checksum is sent from the UE to the visited network, which shall forward it to the home network in the subsequent authentication request. The home network is now in a position to verify the checksum and to ensure that the visited network as seen by the UE is identical to the visited network as seen by the home network. Finally, after RES* verification, the home network responds an "authentication confirmation" in an authentication response message (message 12 in Figure 6.1.3.2-1 in TS 33.501 [1]) I.e. it provides an indication on whether or not the checksum is correct (and the necessary information for key derivation between UE and visited network, if the authentication was successful from the home network perspective).

The goal of this authentication confirmation is to combat fraud, so a missing or failed authentication enables the home network to deny network access. Because the home network provides the authentication details only at the final message after authentication confirmation, the visited network can only provide the service to a UE if no authentication failure was signalled. If there was an authentication confirmation failure, this allows an MNO to feed missing/failed authentication confirmation for UEs and networks into their anti-fraud systems and/or other signalling functions in order to prevent service for UEs where confirmation is not achieved. This also allows to distinguish if there is a different outcome with 5G AKA, i.e. there is either a technical error, or one party is ‘cheating’.

In addition, a modified f5* function using MAC-S as an additional input can be used [130]. Including MAC-S as an input to f5* ensures that AK is unique for each SQN_{MS}. It is home network decision to include or not MAC-S as input to f5*. The possible leakage of some bits of SQN_{MS} are avoided.

5.3 Increased Subscriber Privacy

The USIM may choose to identify itself towards the visited network using an encrypted version of its long-term identifier which can only be resolved by the special SIDF in the home

network. While this protects the long-term identity over the radio link against eavesdropping by third parties, it does not hide it from the visited network, as the specification requires the visited network to be able to successfully resolve the subscriber's long-term identifier, or otherwise deny service to the subscriber. Emergency calls are exempted from this requirement.

Note: There is no process where the visited network must first authenticate prior to this. The visiting network has the power to reject the authentication request by the UE, but successful authentication needs to be done by the home network and then signalled back to the visited PLMN (VPLMN).

The above aspects enable the home network to potentially exercise more stringent control over the privacy and experience of its roaming subscribers and over the network's exposure to fraud. The challenge is to create incentives for operators, both in the role of "home" and "visited" networks, and for "home" operators to mandate the use of these mechanisms whenever possible. GSMA could assume a role to create incentives and offer support to achieve this goal. In this regard, the feasibility of the following ideas could be examined.

GSMA PRD FS.37 [64] discusses various vulnerabilities within the GTP-U security, addressing the importance for MNOs to have visibility into UP, where the attack vectors would be detected and security bridges prevented when detection happens early enough in the kill chain. [64]Although there are no standards addressing this issue, GSMA PRD FS.37 [64] provides recommendations and guidelines to MNOs. This scenario applies to all use cases.

5.3.1 Steering of Roaming (SOR)

IR.73 [5] defines mechanisms by which a home operator can force roaming subscribers onto specific “preferred” visited networks. These mechanisms can be used to avoid networks without authentication confirmation support. They could also be used to avoid non-5G networks altogether.

The 5GS introduces a CP SOR solution that allows the HPLMN to direct the UE during or after registration on the Visited Public Land Mobile Network (VPLMN). Details on the interfaces and how the registration process occurs in a 5GS can be found in 3GPP TS 23.501 (Rel. 15) [31] and 3GPP TS 24.501 (Rel.15) [26], respectively.

The solution allows the HPLMN to update the "Operator Controlled PLMN Selector with Access Technology" list in the UE by providing the HPLMN protected list of preferred PLMN/access technology combinations via NAS signaling.

The general description and the procedural flows are specified in 3GPP TS 23.501 (Rel. 15) [31] and 3GPP TS 24.501 (Rel.15) [26], and the SOR security mechanisms are specified in 3GPP TS 33.501 [1]. Mechanisms to ensure message security and integrity have been developed and can be found in 3GPP TS 31.115 Rel 15 [32].

This 5GS SOR solution does not preclude the use of the existing mechanisms for SOR as defined earlier in this document. Implementation impacts are documented in GSMA PRD IR.73 [5] and business guidelines in GSMA BA.30 [33].

5.3.2 Creation of Potential Fraud Databases

The GSMA's long-term goal could be to persuade MNOs to deny service to their roaming customers on the basis of missing authentication confirmation. It is, however, unlikely that MNOs will agree to lose revenue on this basis alone. In order to be able to differentiate between situations in which service should be granted vs. situations in which service should be denied, it is important to be able to refer to reliable data.

Based on a geomap, an MNO can identify roaming partners and areas where changing the policy from "grant service even without authentication confirmation" to "deny service unless authentication confirmation is successful" would be a viable policy (i.e. would not lead to loss of connectivity).

Operators could, in addition, measure the number of authentication events per roaming partner per area and count how many of these events were performed with authentication confirmation. Based on these statistics, potentially combined with other statistics from fraud management data, the MNO could prioritize which areas to switch over to the new policy.

A further improvement in 5G is offered with the policing of incoming Location Updates with the authentication confirmation messages.

5.3.3 Creating Customer Choice

The subscriber's profile could be enhanced with options that indicate if roaming without authentication confirmation, and if GUTI-based identification instead of the SUCI-based identification in a roaming situation is acceptable from the subscriber's point of view. Since the decision whether to grant or deny service to a roaming subscriber can be based on such individual indications, the subscriber could be empowered to choose its own acceptable level of privacy and exposure to fraud. Of course, in case of mandating SUCI-based identification, the handset has to be compatible.

Operators could consider charging subscribers a premium for such security configuration options. Depending on certain details, a business model-driven approach may be beneficial or detrimental to the adoption of the underlying standard mechanisms.

GSMA could provide guidance and define a rule set with the goal to increase the adoption of the security enabling technologies.

5.4 UEs with 4G and 5G SIMs Connecting to a 5G Network

The connection of 4G and 5G SIMs to a 5G network requires consideration as the following 3 scenarios could apply:

5.4.1 Legacy 4G UICC with USIM application

It is assumed that UEs can connect to a 5G network with a 4G USIM with its existing file structure and data settings. This would imply the same authentication procedures as with 4G, with no use of SUCI.

The use of 4G SIMs is not excluded as this would otherwise imply costs and logistical challenges that would result in significant service disruption if legacy 4G SIMs are excluded. However, from a pure security perspective, the use of 4G legacy SIMs does not take

advantage of the 5G security enhancements, not least because the SUCI enhancement will not work.

5.4.2 Updated 4G UICC with USIM application

In this case the SIM is updated over the air with a new file structure and data settings, e.g. SUPI Type, Routing ID, Protection Scheme and its ID, Home Network Public key and its ID, etc.. Then the 5G UE can use the 5G security procedures with the transfer of the SUCI encryption of the SUPI executed by the logic within the Mobile Equipment according to the "SUCI calculation is to be performed by the ME" configuration only [130].

This scenario depends on the ability of the SIM to be updated over the air with a new file structure and data settings to support SUCI information storage.

5.4.3 5G UICC with USIM application

The encryption of the SUPI is executed by the logic inside the 5G UICC according to the "SUCI calculation is to be performed by the USIM" configuration [130].

Mandatory replacement of SIMs is not desirable but, for specific use cases like customers with heightened security needs (enterprises, governments, large accounts) the replacement of SIMs might be needed to ensure that all 5G security capabilities are realised.

5.4.4 Additional Comments

For more details about the capabilities of IMSI/SUPI encryption in the 5G SIM or in the device see a comparison in the report "Protecting Subscriber Privacy in 5G" by the Trusted Connectivity Alliance [103].

From a security perspective, there is no difference between option 2 and option 3. The risk only applies to the location in the UE where the calculation is performed as the SUPI needs to be available outside the SIM for a key calculation. In the case of a compromised device, it is likely the attacker also has access to the voice and data APIs.

In 4G, the temporary identifiers may be visible. Malicious base stations may force the UE to connect, and as a result, the SUPI will be visible. With the use of rotating master keys, the impact of this risk can be limited.

An UICC card swap, (commonly referred to as a 'SIM swamp'), involves cost and some degree of service disruption so it may only be offered to customers looking for the enhanced 5G security benefits with integrity protection and the concealment of critical identifiers.

The use of mutual authentication represented a significant security improvement.

5.5 UEs Should Limit Downgrading from 5G to 4G/3G/2G

A need was identified that the UE should include functions to limit downgrading from 5G to 2G in networks with 3G and/or 4G, and the user shall be informed when downgrading to 2G in such situations.

Connecting to 4G and 3G networks provides similar protection with support of the AKA security protocol. However, security in 2G offers less protection and users are more easily traceable.

The issue is recognised as is the need to consider use cases such as:

- Enterprises and governmental agencies – Higher demands for secure communication may require specific policies and restrictions to radio network access.
- Specific Network Situations – To improve the performance of UEs and assist MNOs with switching off legacy radio networks in areas with fragmented network coverage.

GSMA Device Security Group (DSG) advice is that users, and particularly those with heightened security needs, should have the option to choose which radio technologies they wish to access. This capability should be offered and controlled on the device. 3GPP TS 22.101 [51] already allows users and home operators to disable and re-enable a device's individual radio technologies. This capability has been implemented in the Android devices, which allows users to disable 2G at the radio hardware level [145]. These features need to be implemented by device manufacturers more widely, in accordance with the standards, and should be made available to MNOs. DSG recommended that MNOs should offer this configuration flexibility to their customers.

GSMA DSG does not consider it necessary to inform users, by default, when downgrading to earlier radio technologies as to do so could cause confusion or unnecessary worry for most users. Some technically savvy users that have higher security requirements may wish to be informed and they should have visibility provided to them via menu choices on their devices or via their enterprise device management system. This need could be fulfilled through a specific application that uses an API offered by the device Operating System (OS).

Operators in most jurisdictions have a legal and regulatory obligation to allow unfettered calling to emergency services. Because the UE should always be able to access emergency services, regardless of the network connection and network/user decisions regarding which radio technologies should be enabled, it must be possible to override the restriction settings to ensure emergency service access is available. This override capability is provided for and defined in 3GPP TS 22.101 [51].

A ciphering indicator has been defined as a standardised feature in 3GPP TS 22.101 [51] and it detects when radio interface ciphering (user plane) is not switched on and indicates this to the user. This need can also be fulfilled through a specific application that uses an API offered by the device OS.

No specific network functions or provisioning actions are required by the network functions. Device manufacturers are required to implement the requirements defined in 3GPP TS 22.101 [51] and implementations must be adequately secured. Device manufacturers should provide MNOs the ability to provision security conscious users with the features described above.

5.6 WLAN Authentication Using EAP-AKA' with a 5G UICC

This approach enables devices that support Hotspot 2.0 (802.11u/ANQP) to authenticate to participating WLANs using their mobile identity. Privacy is enhanced by using the SUCI as the username when it is available, rather than the IMSI.

However, it should be ensured that the extra length of the SUCI should not cause backward compatibility issues when interworking to older systems such as the Remote Authentication

Dial-In User Service (RADIUS) protocol, where the length of the username is limited to 256 octets.

This 256 octets size issue should not arise with the profiles specified thus far. These profiles have a length less than 256 octets and longer profiles are only foreseen in the future. See TS 33.501 [1] and TS 23.003 [50] for more details.

5.7 Subscription Based 5G Core Selection for Roaming

Steering outbound roamers to a 4G/5G overlay core in the HPMN requires older MMEs to appropriately anchor to the (overlay) SMF+P-GW. This issue is outlined in [105] and will be covered in subsequent versions of the LTE Roaming guidelines in GSMA PRD IR.88 [10] and the 5G Core Network Roaming guidelines in GSMA PRD NG.113 [58].

The steering is based on the HSS returning a R15 indicator to the MME, which then enables the MME to modify the FQDN prior to the Domain Name Server (DNS) query to obtain the address of the P-GW. There is a concern that older MMEs do not understand the new R15 indicator and thus anchor onto the (old) P-GW rather than the (overlay) SMF+P-GW. The proposal in [105] describes the OI Replacement in NG.113 [58] as a basic selection mechanism to guarantee that the mechanism works world-wide for all roaming use cases.

5.8 Wireline Authentication using EAP method

To support Wireless and Wireline Convergence for the 5G system, two new network entities, 5G-RG and FN-RG are introduced.

The 5G-RG acts as a 5G UE and can connect to the 5G Core Network via W-5GAN or via Fixed Wireless Access (FWA).

The FN-RG can connect to the 5G Core Network via W-5GAN. The W-AGF performs the registration procedure on behalf of the FN-RG. It acts as the end point of N1 and provides the NAS signalling connection to the 5GC on behalf of the FN-RG.

A 5G -capable UE can connect to 5GC through an RG that is connected to the 5GC via W-5GAN or NG-RAN. The UE supports untrusted non-3GPP access and/or trusted non-3GPP access.

5.9 Authentication for NPN

For Public Network Integrated NPN (PNI-NPN), the primary authentication shall be performed with the public network. Secondary authentication and slice-specific authentication, discussed further in section 14.2.3 can take place after a successful primary authentication.

For Standalone Non-Public Network (SNPN), an existing primary authentication method can be used. Alternatively, primary authentication with credential holder external entity can also be used. In this case, K_{AUSF} is calculated based on MSK, and the UDM/ARPF is not necessarily involved in the key derivation or distribution.

6 Increased Home Control

6.1 Overview

The 5G authentication and key agreement protocols offer increased home control compared to EPS AKA in EPS. They provide better security to prevent certain types of attacks because the AUSF in the home network obtains confirmation that the UE has been successfully authenticated and is really roaming. As this feature only works between networks that are both 5G, there is the risk that an attacker in a network would utilise 4G messages which would not have this security feature and would enable the 5G increased home control to be bypassed.

The increased home control feature is useful in preventing certain types of fraud but an authentication protocol, by itself, cannot provide protection. The authentication result needs to be linked to subsequent procedures in some way to achieve the desired protection.

“Linking increased home control to subsequent procedures” in TS 33.501 [1] specifies the details of the security enhancement for Home Control.

6.2 GSMA Recommendation

The actions taken by the home network to link authentication confirmation (or the lack thereof) to subsequent procedures are subject to MNO policy and are not standardised. MNOs are advised to implement the following security control actions based on the approaches described in TS 33.501 [1]:

Use of “Approach 2 – visited network in the first category” is advised on the international interfaces between roaming partners. A successful authentication 'immediately preceding' the API of the UDM i.e. Nudm_UECM_Registration Request offers additional protection because the message may be routed via e.g. one or more IPX carrier networks with topology hiding in their edge nodes, through which the home network has no direct visibility of the network sending the Nudm_UECM_Registration Request message.

On the internal interfaces within an MNO group a less stringent regime for Home Control may be followed depending on MNO policies.

“Approach 1” and “Approach 2 – visited network in the second category” are equal in their working.

7 Mission Critical Services and Priority Handling

7.1 ACCOLC/MTPAS Supported in 2G/3G

Access Overload Control (ACCOLC) and its successor Mobile Telecommunication Privileged Access Scheme (MTPAS) are based on what is specified in 3GPP TR 23.898 [15] and offer a procedure for restricting mobile telephone usage in the event of emergencies.

ACCOLC/MTPAS can be applied in specific mobile cell sites prioritising access to mobile networks for privileged persons (typically members of emergency services that are designated at a local level). This allows/restricts devices of entitled users to gain priority access to these cell sites. This only applies to the mobile devices of entitled users (e.g.

Police/Fire Services) that are equipped with a special SIM provisioned with specific Access Class levels.

As ACCOLC/MTPAS is not supported in LTE, MNOs currently rely on the 2G/3G functionality by disabling 4G in sites with privileged service access for emergency services.

7.2 Multimedia Priority Service in LTE/VoLTE

ACCOLC/MTPAS is currently a UK specific procedure although some MNOs may have similar control options in their 2G/3G/4G networks. In addition, the Multimedia Priority Service (MPS), see 3GPP TS 22.153 [65], with privileged access features are fully supported and implemented in LTE/VoLTE in the USA.

For 5G, the privileged access barring exceptions for MPS and Mission Critical Services (MCS) are covered in the Unified Access Control (UAC) sections of 3GPP TS 24.501 [26] and 3GPP TS 38.331 [34].

Further enhancements are expected in 3GPP Release 16.

7.3 Mission Critical Services in LTE and 5G

The requirements for the Mission Critical (MC) services are contained in 3GPP TS 22.280 [106] that are common across two or more MCS:

- MCPTT: the Mission Critical Push to Talk as defined in 3GPP TS 22.179 [107].
- MCVideo: the Mission Critical Video services as defined in 3GPP TS 22.281 [108].
- MCData: the Mission Critical Data services as defined in 3GPP TS 22.282 [109].

Initially specified for LTE, these services have been further extended with additional features and access capabilities in 5G. The MCS are typically developed for public safety applications (police, fire and medical services), maritime safety applications and also for general commercial applications (e.g., utility companies, railways and maritime usage).

7.4 Priority Scheme for Roaming Traffic

Multiple services are supported behind the roaming traffic with IoT and other emerging applications. This may include critical services e.g., for healthcare or for emergency services with either permanent roaming users like static devices or temporary visiting roamers within cars or health care devices of travelers.

As a consequence, it may be necessary to have different priorities distinguished between the roaming traffic on the interconnects between roaming partners by use of different QoS slices or via other means that need further consideration by the GSMA NG 5GJA group.

Although roaming signaling traffic should be transferred in a network slice with high priority and high quality of service with assured content security, as specified in GSMA PRD FS.37 [64] , there may be an additional need to differentiate between various types of roaming traffic, especially since operators use partners' networks for M2M and IoT services frequently. This may include services with very critical service characteristics that may require specific treatment to ensure the roaming traffic is rerouted via other resources.

8 Innovations in 5G Core

8.1 Overview

5G core brought significant changes to the mobile core architecture. Those include and are not limited to the introduction of SBA CP, which consists of many NFs covered throughout this document, micro-segmentation, end-to-end network slicing, and more. For more details see the 5G architecture specification 3GPP TS 23.501 [31]. The implementation of 5G NFs may be in the form of Physical Network Functions (PNFs). Virtual Network Functions (VNFs), or Container Network Functions (CNFs), as addressed by ETSI ISG NFV specifications.

[1]5G changes extend to communications protocols also. Those include the following:

- [1]HTTP/2 (see IETF RFC 7540 [2]) as the application layer protocol.
- TLS (see IETF RFC 5216 [13]) to secure the communication between all NF inside a PLMN.
- TCP (see IETF RFC 793 [3]) as the transport layer protocol for HTTP/2, as defined in [2].
- JSON (see IETF RFC 7159 [4]) as the serialisation protocol.
- RESTful framework for the APIs design whenever possible and use custom methods otherwise.
- Support notification with two HTTP client-server pairs.
- OpenAPI 3.0.0 as the Interface Definition Language.

The secured communication between all NFs inside a PLMN is based on TLS with:

- Confidentiality protection by encryption.
- Integrity protection by hash validation.
- Authentication by certificates.

The details on the protocols assessment and conclusions can be found in the latest versions of the 3GPP TS 23.501 [31] and 3GPP TS 33.501 [1].

As these protocols are used in the wider IT industry, it will likely lead to a shorter vulnerability to exploitation timeline, and higher impact of vulnerabilities within these protocols with the need for increased security patching, see also section 9. On the other hand, the use of these well-known protocols expands out the potential pool of attackers. 4G and especially 3G CNs benefit from attackers having little experience with the proprietary standards used within them.

Vulnerability reporting schemes, such as the GSMA Coordinated Vulnerability Disclosure (CVD) programme [156], will have to manage the increased scope of these protocols.

Once in-field vulnerabilities are discovered, the time to patch for relevant vulnerabilities should be short. It is recommended to ensure that workloads of NFs are validated continuously.

8.2 Intra-PLMN Signalling Message Flow within the SBA between NFs

As the SBA introduces TLS and APIs for inter-connectivity between the SBA functions, it requires certificates to support TLS. The certificate allows for both (1) transport encryption and (2) identity authentication.

The functions within the SBA can be created dynamically with virtualisation and resource management tools. Hence the SBA is a dynamic environment, with functions that may come in and out of existence and will need to be available to other functions in the SBA over these encrypted channels. As a result, certificates (keys) need to be created dynamically and managed through their lifecycle, including archival storage.

As this is a difficult challenge, vendors are not proposing key management solutions for the intra-PLMN SBA and instead are proposing solutions that include a single (or few) certificate that have wildcard identities. This allows the certificate to be used on any NF and reduces the management overhead.

Although this simplified approach supports transport encryption between NFs, it is not able to validate the legitimacy of an endpoint. This is a problem as MNO threat models are more concerned with the ability for an attacker to create false functions (in this virtualised core) than it is about having an attacker eavesdrop on data over transport.

To provide identity authentication between the NFs within an SBA, it is advised that the MNO reuses, for this situation, the same key management procedure as specified for inter-PLMN in FS.34 [53], see also the following section 8.3.

8.3 Inter-PLMN Signalling Message Flow Over N32

To allow for 5G Interconnect Security over the N32 interface between 5GCs the SEPP is introduced as a new protection element into the 5G network architecture, as depicted in Figure 19. IPX Providers do not have a N32 interface, or SEPPs (formally).

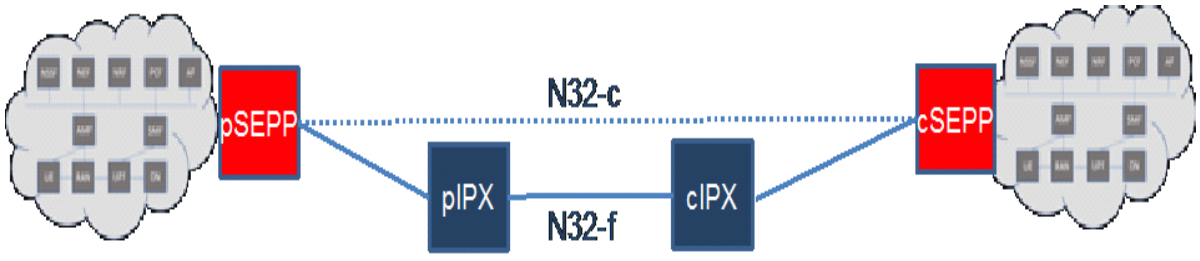

Figure 19 – Overview of N32-c and N32-f interfaces high level (IPX is used illustrative to address any roaming intermediary in transit)

The SEPP takes care of routing signalling messages over the N32 interface. It is validating certificates as part of a N32-c TLS security setup including cross-checks with PLMN ID lists, i.e. to ensure that information in certificates match with the information in service requests. The SEPP has also filtered tasks as described in FS.36 [56].

SEPPs enforce inter-PLMN security on the N32 interface as specified in 3GPP TS 33.501 [1]. N32-c is used for the security capability exchange to negotiate the security method (TLS

or PRINS) to be used for N32-f and, if ALS (PRINS) is the selected security method, then N32-c is also used to negotiate the protection and modification policies for service messages exchanged.

N32-f is used for exchanging service messages between NFs located in the different PMNs in a e2e secured way. The security protocol used for N32-f between the two SEPPs of PMNs is either TLS or PRINS.

TLS is selected when roaming intermediaries are only used for transport. PRINS is selected when roaming intermediaries in transit need to have visibility to some IEs and are allowed to modify with attributability selected IEs. Attributability means that it is possible to prove which roaming intermediary has done which modification by verifying the signature. For the ALS protocol PRINS the underlying transport protocol is TLS, by which all links between hops are protected. N32-f PRINS is using JWE – JSON web encryption & JWS for signatures. SEPP is responsible to provide the following:

- Encryption
- Integrity
- Authentication.

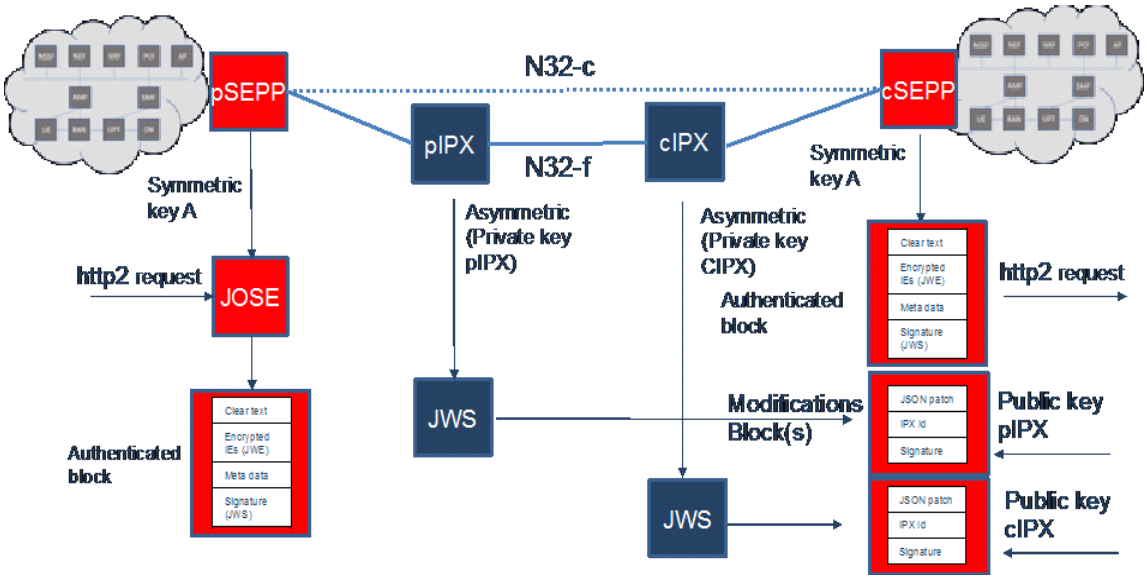

Figure 20 - Message flow over N32-c and N32-f interfaces

The common application errors are defined in 3GPP TS 29.573 [86] and 3GPP TS 29.500 [85].

The specific set of GSMA guidelines for 5G Interconnect Security over the N32 interface is contained in FS.36 [52] and the SEPP related aspects in FS.21 [17].

8.4 Application Layer Security (ALS)

Communication between SBA's NFs happen through RESTful APIs using well-known protocols – HTTP/2 and TLS. The guidelines for 5G ALS with HTTP/2 and JSON can be found in GSMA PRD FS.36 "5G Interconnect Security" [52] together with the embedded 5G Risk Matrix.

This also requires the implementation of the key management procedures as specified in FS.34 [53]. This key management solution is generic for both LTE and 5G inter-PLMN security.

Please refer to section 11.2 for inter-PLMN security details in interworking situations with both Diameter and Signalling System Number 7 (SS7):

The security enhancements for LTE with Diameter are specified in FS.19 [9] and in FS.21 [17].

Diameter and SS7 Security are addressed in Section 12 Legacy Signalling Technologies.

APIs should also be secured via standard means, i.e. OAuth.2.0 and TLS 1.3.

8.5 Lower Layer Security and Monitoring

The mandatory use of TLS between all NFs inside a PLMN implies that communications over the SBA will be encrypted. This has an impact on how network monitoring for service assurance and other network supervisory systems can be accomplished, such as:

- The use of passive network taps or other means to retrieve a copy of the encrypted signalling traffic will require that the monitoring system needs to be integrated with the key management for the active elements on the SBA network.
- The active elements on the SBA network support of a data streaming facility to send a copy of the signalling traffic to the monitoring system. This provides a cost-efficient solution without the extra installation and operation costs for a separate tap network. This simplified deployment model can be implemented either via network taps integrated within the active elements on the SBA network or sending a copy of the signalling traffic in a normalised data format as a feed to the monitoring system via a standard API.

Alternative solutions were also considered but come with their specific limitations and risks as follows:

- Use of Enterprise TLS configured as a Man-In-The-Middle (MITM) TLS proxy acting both as front-end TLS server to a requesting NF client and as front-end TLS client to the remote NF server. TLS proxies introduce intrusion opportunities and vulnerabilities for attackers and that any vulnerability in such a front-end MITM TLS proxy can significantly downgrade network security [14].

- Use of Call Detail Records (CDR) generated by the active elements on the SBA network. However, with CDRs, the visibility of the network actions becomes reactive because the results normally are available after the call is released and only for answered calls. This doesn’t work in real-time and essential details may be lost as not all of the signalling details are recorded in a CDR.

8.6 Transfer of Executable Code via JSON

The filtering rules of signalling firewalls are typically designed to offer protection against the risks implied by the vulnerabilities of the signalling protocols. However, JSON objects may

also be abused for the transfer of executable code similar to the risks with e.g. imperfections of legacy ASN.1 (Abstract Syntax Notation) parsers in SS7 protocol stacks.

Protection against these types of vulnerabilities, as well as evolving 5G vulnerabilities described in FS.36 [52], should be taken into account as part of the future work on guidelines for signalling firewalls for the 5GC protocols.

8.7 Load Distribution, Redundancy and Failover

Refer to the 5G Roaming Guidelines in GSMA PRD NG.113 [58] where implementation scenarios and guidelines are described for load sharing, redundancy and failover across multiple SEPPs.

Note: The 3GPP standards only specify the working between single SEPP pairs and don't cover network situations with multiple SEPPs that will require operational settings between roaming partners for the traffic distributed across their edge nodes. This has a relationship with the key management procedures in FS.34 [53] because use of a single key introduces the risk that all interconnect points could be compromised if this key is stolen. Alternatively, if every pair of SEPPs needs to be allocated a unique set of keys that would introduce a cumbersome key management process.

8.8 Sharing Threat Intelligence Information between MNOs

Similar to SS7 and Diameter as specified in FS.21 [17], the same principles can be applied as an inter-operator framework for sharing HTTP/S and JSON threat intelligence information.

Sharing of threat intelligence between MNOs aligns with the recommendations suggested by EU ENISA and USA FCC in their reports [11] and [12], respectively.

In addition, this framework as defined in FS.21 [17] contains details on how information could be shared, including via:

- Exchanges of threat information at a high-level within the GSMA.
- Specific GSMA services, such as the GSMA Telecommunication Information Sharing & Analysis Centre (T-ISAC) [18] supported by Malware Information Sharing Platform (MISP) for information sharing.
- Other methods, including bilateral exchanges between members, within specific groups or via other threat sharing services/centres.

Threat intelligence integration is essential for the roll-out of 5GCs. Therefore, rapid integration of countermeasures against all attack scenarios, based on latest threat intelligence, deploying AI with ML, is important to avoid having outdated security protection and giving a false sense of security. Cyber threat intelligence integration should include intelligence gathering, analyses, curation based on established frameworks, such as MITRE ATT&CK, MITRE FiGHT, and GSMA MOTIF [79]. Intelligence sharing can be achieved using current GSMA MISP alerts or a system design for M2M communication.

8.9 Additional Security Considerations

The security architecture of 5GS networks is hierarchical and classified by domain during their design. It is advisable to consider the following additional security guidelines.

8.9.1 Zero Trust Methodology

Zero Trust is a methodology which encompasses many aspects of security, including and not limited to cryptography, user validation and authentication, as Figure 21 illustrates.

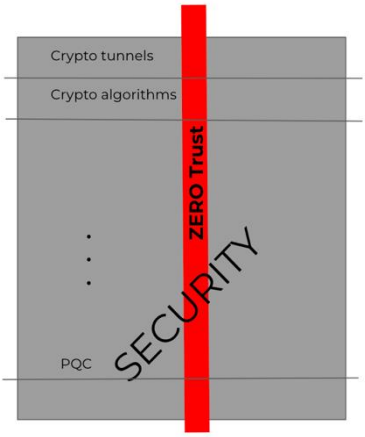

Figure 21 - Meaning of Zero Trust

Zero Trust results in Zero Trust Architecture (ZTA), which prevents breaches from happening by eliminating trust in the digital world, while consistently verifying all users, devices, and applications across all locations.

NIST SP 800-207 [138] document addresses Zero Trust Architecture (ZTA) for enterprises, including and not limited to all enterprise assets and subjects. ETSI GR ETI 002 [135] document extends the ZTA concept to a public telecommunications infrastructure. As mentioned in the document, "... there should be no assumptions as to what happens before or after each hop in and across the infrastructure, starting with the source and ending with the destination of particular data flow at all layers of OSI." (ETSI GR ETI 002).

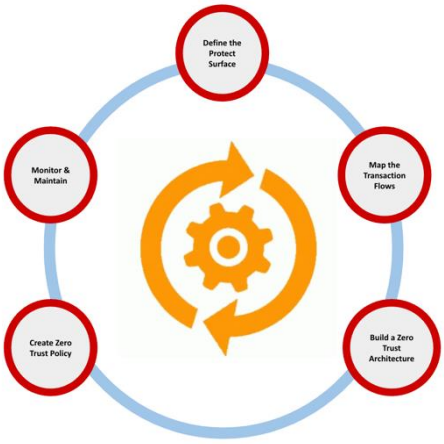

Figure 22 - Zero Trust Methodology

Zero Trust methodology consists of five (5) steps, identified in Figure 22, which are repeated continuously throughout the lifetime of the protected surface. Those steps are:

1. Define the protect surface.
2. Map the transaction flows.

3. Build a Zero Trust Architecture (ZTA).
4. Create Zero Trust security policy.
5. Monitor and maintain.

Figure 23 summarizes the questions a Zero Trust security policy should address.

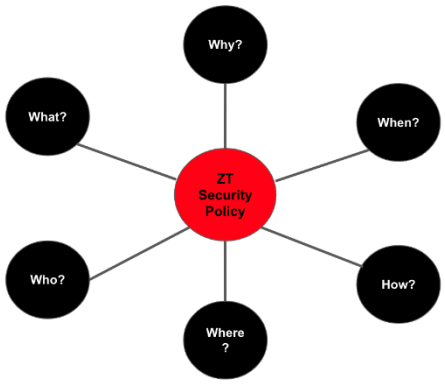

Figure 23 - Method Used to Define ZTA Security Policy

The following are some examples of the questions which could be applied to 5G infrastructures when defining such a security policy:

- What? Identify/validate signaling and user plane traffic - what applications are being used?
- Why? Identify legitimate flows for signaling and user planes - why is the packet trying to access a resource?
- When? Predictable signaling/user plane traffic behaviors - when is the resource being accessed?
- How? Visibility into signaling and user planes - how does the packet access the protected surface throughout this communication?
- Where? Specify source and destination - where is the traffic source and destination?
- Who? Validate unique subscriber and/or device IDs - who can connect?

Zero Trust mechanisms, include the following:

- Micro segmentation as a solution for enforcing isolation between virtual payloads and hosts.
- SBA workloads and API security will be checked continuously, assuring SBA proper functionality and its protection from signaling storms.
- Improve trusted host environment by using technologies such as secure-boot of telco-cloud infrastructure (including host firmware, OS and hypervisor). This mechanism may require continued attestation and validation of the security posture.
- Integrity checking of virtual payloads before execution based on ISO19790 [146] or FIPS 140-2 Level 3 Cryptographic security solution.
- Protect and encrypt data at rest. For example encryption of VNF volume/swap areas, as recommended by ENISA [129]. The best practice to secure the VNF volumes is by encrypting them and storing the cryptographic keys at safe locations.
- Achieve User Plane GTP-U Security as addressed by FS.37 [64].

8.9.2 SBA API Security

When deploying 5G Core SBA it is recommended to make the list of the deployed APIs first. Next, the following recommendations apply:

- Mutual authentication for SBA APIs using both client and server-side certificates.
- Use of OAuth for SBA API request authorisation and Logging of SBA API requests.
- Use of load balancing and monitoring capabilities for SBA API requests.
- Monitor SBA API data communications.
- Observe variability at the network layer.
- Validate API information.

8.9.3 Transport Security

While building the transport security policies, it is recommended to gather security requirements from the RAN, Core and hosting teams. Those recommendations should include the following:

- Use of certificates for IPsec to secure transport traffic.
- Hardening of transport network elements (e.g. optical devices).
- Optical-layer encryption.
- Optical-layer intrusion detection.
- Traffic inspection. For example, support of stateful SCTP inspection to remediate vulnerabilities identified in RFC 5062 [136].

For enhanced transport security in the non-interworking or private usage, it may be considered to activate advanced cipher suites within products or protocols. These advancements can be used as an alternative to, or in conjunction with, standard's based solutions, depending on the specific security needs and operational context. This approach ensures a higher level of data protection/integrity/authenticity, especially in scenarios requiring stringent security measures.

8.9.4 Management and Orchestration

- Use of cryptography on all management interfaces for confidentiality, integrity and replay protection.
- Use of certificate-based authentication on all management interfaces.
- Use of Software Defined Networks (SDN) flow analytics capabilities in SDN controllers.
- Integration of all management systems with centralized AAA/IAM for authentication and authorisation of administrative users.

8.9.5 [146][129][143]Additions to Security for End-User Devices

- Use of certificate-based authentication of IoT devices.
- Monitoring of device communications and use of network security analytics solutions to detect device security issues. Some suggestions are provided in the GSMA PRD FS.37 [64].
- In addition, proactive threat hunting practices should be considered for all domains. More elaborated descriptions of these additional security guidelines will be provided in a future update of this document.

9 Increased Security Patching

9.1 Introduction

With the use of Internet protocols, and because governmental organisations perceive 5G as a critical network and step change in national security risks due to increasing reliance on mobile networks to support essential services, basic security weaknesses can no longer be accepted.

Hence, there is an increased demand and need for security patching following the practices and technologies applied for critical applications like banking with the use of Internet protocols. This specifically applies to the security patching of containers as this is very different from the existing practices in 4G.

GSMA could be a conduit for equipment vendors to communicate the need for critical patch updates to MNOs as general concerns persist about security patching with the IT protocol stack and technology layering that is associated with virtualisation.

Note: For previous generation mobile systems, IR.77 [59] already includes in Binding Security Requirement (BSR) 17 requirements in “Secure Configuration of Network Elements, Network Services and IPX Services”.

9.1.1 Mobile Device Software Security Updates

FS.25 [97] establishes high level requirements for security updates for cellular-connected device software, with a particular focus on critical security updates which need to be deployed widely and quickly due to a major security incident of some kind. The software on devices has historically been, and is often still, referred to as firmware. This includes the baseband software, drivers, OS, communications stacks and application framework. It also includes manufacturer supplied, pre-installed applications such as browser updates which are also controlled and deployed by the manufacturer, rather than through an “app store.”

The requirements in FS.25 [97] acknowledge changes to the global device landscape and that increasingly varied hardware is making use of cellular connectivity. As a result, many of the principles and methods outlined in this current version will be applicable to IoT and Machine-to-Machine (M2M) devices.

9.1.2 Security of IoT devices

Based on practical experience in MNO networks, the following items are considered highly relevant for managing the security of IoT devices:

- End-to-end security for “constrained devices” (e.g. battery-powered ones): Industry will only support BEST, if operators can demonstrate a convincing business case and MNOs jointly pushing in the same direction would be useful in this regard.
- Validation that the IoTs have not been compromised and that the traffic behaviour is as expected, adhering to Zero Trust principles, which are discussed in the Section 8.9.1 (Zero Trust Methodology) of this document.
- Unified certification of IoT device chipsets, e.g. following GSMA SGP.25 and other PRDs.

- Definition of a bootstrap procedure for key material for devices which are not pre-provisioned during manufacturing.

- Appropriate management of firmware vulnerabilities in IoT devices by manufacturers, including pre-existing patch procedures, where the manufacturers must be willing to maintain their software/firmware and provide patches. Furthermore, instructions on how to deploy patches, identified by devices' types must be defined. Critical decision points include the following questions:

    - Is distribution Over the Air (OTA) possible?
    - Does bandwidth support that distribution?
    - Does battery consumption of constraint devices allow that distribution to be successful?

9.2 5G Core and RAN Elements Patching

The importance of software updates and patching for 5G core and network systems cannot be overstated. These updates and patches are crucial for maintaining the security, performance, and reliability of the network. They often include fixes for vulnerabilities that could be exploited by malicious actors, improvements to the system's functionality, and enhancements to its performance. In the rapidly evolving world of 5G technology, staying up to date with the latest software updates and patches is essential to ensure the network can support the advanced services and communication that 5G promises. Moreover, it's critical to not only consider the network functions but also its supporting systems. These supporting systems may include DNS, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), firewalls, security scanners, Identity providers, secret stores, and Continuous Integration/Continuous Deployment (CI/CD) tools. 5G network functions may be supplied by open source or vendors deployed on servers, VM or container engine orchestrated by Kubernetes or similar orchestrator. Patching underlying infrastructure is as important as NF application itself. These components play a vital role in the overall security and performance of the 5G network. They need to be regularly updated and patched to protect against potential threats, ensure they can effectively support the network's operations, and enable them to take advantage of new features and improvements. Ignoring these supporting systems in the update and patching process leads to weaknesses that could be exploited, impacting the network's performance and security.

A malfunctioning Core or RAN NF can have a serious impact to 5G service for its consumers and in some cases regulatory consequences of the down time. All patches must be tested in lab, alpha or beta networks before deployment to understand the system behaviour before and after the upgrades. Patches can be small and large in scope of changes included in the updated software. It is critical to understand and plan for default SW configuration and behaviour changes that may be inadvertently changed in the updated software by developers. Part of network operations should include a plan to monitor and assess the expected improvement the patch is supposed to provide, and also include a roll back plan.

Core elements workloads must be secured continuously due to fluency of containerized 5G environments. All CNF workloads must be validated continuously, as addressed in ETSI NFV SEC 023 [147] or NIST SP 800-190 document [144] - Application Container Security Guide.

10 Messaging and Voice

10.1 Short Message Service (SMS)

The following sections apply to 5GS SMS in Release 15, 16 and 17. It is noted that the Releases 15, 16 and 17 continue to support the legacy MAP/SS7 and Diameter interfaces for SMS Roaming and SMS Interconnect.

The Release 17 SMS_SBI work item is now published and specifies the support for SMS over the Service Based Interface (SBI), hence is understood to support SMS Roaming and SMS Interconnect. These are described in 3GPP TR 29.829 [74] and specified in 3GPP TS 23.540 [121], TS 29.577 [122], TS 29.578 [123] and TS 29.579 [124].

[The GSMA 5GMRR task force is addressing the challenges for SMS_SBI Interworking for 5G SA Interconnections. This includes SMS Bilateral for national and international networks, and SMS Hubbing over SBI [126].]

10.1.1 SMS Roaming

The roaming architecture for SMS over NAS (SMSoNAS) is described in 3GPP TS 23.501 [31]. As shown in Figure 24Figure 24, 5GC signalling for the outbound roaming subscriber between the Visited PLMN and Home PLMN is protected by the SEPP interworking over the N32 interface.

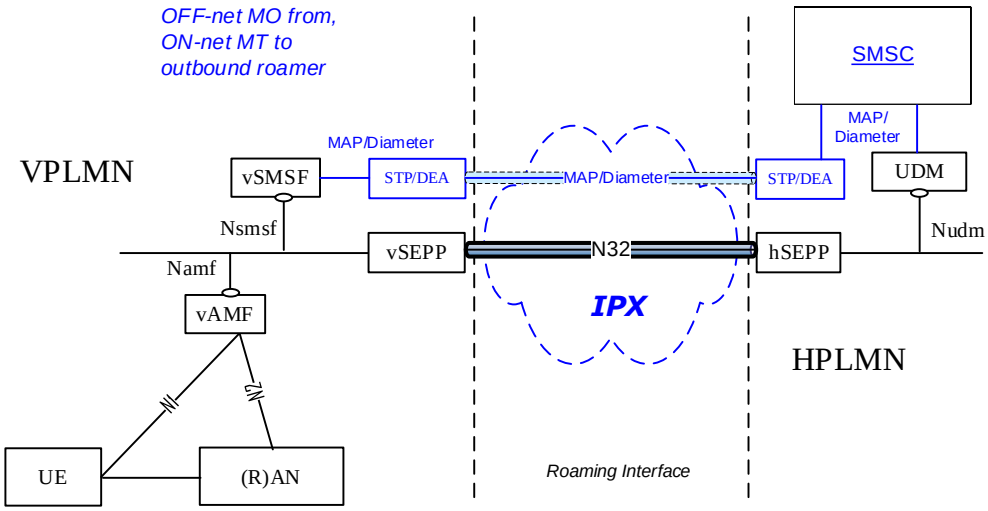

Figure 24 - SMSoNAS Roaming

However, subsequent SMS operations e.g. Mobile-Originated SMS by the roaming subscriber, are transported over the legacy SS7 or Diameter interface between the VPLMN and HPLMN. As these SMS operations are not supported over the 5GC Service-Based interface, they are not protected by the SEPP interworking.

If the roaming interface is supported over Diameter End-to-End Security (DESS) [9], then SMS roaming will be protected with integrity and confidentiality protection.

However, if the roaming interface is supported over Message Application Part (MAP)/SS7, integrity or confidentiality protection will not be supported.

In the case of SMS over IP (SMSoIP) roaming in 5GS, for as long as the outbound roamer continues to roam on IP Multimedia Subsystem (IMS), the SMS messaging shall be protected over the UPF N9 Home-Routed connection between the VPLMN and HPLMN, as shown in [22]. Otherwise, the roamer's SMS may fallback to SMSoNAS.

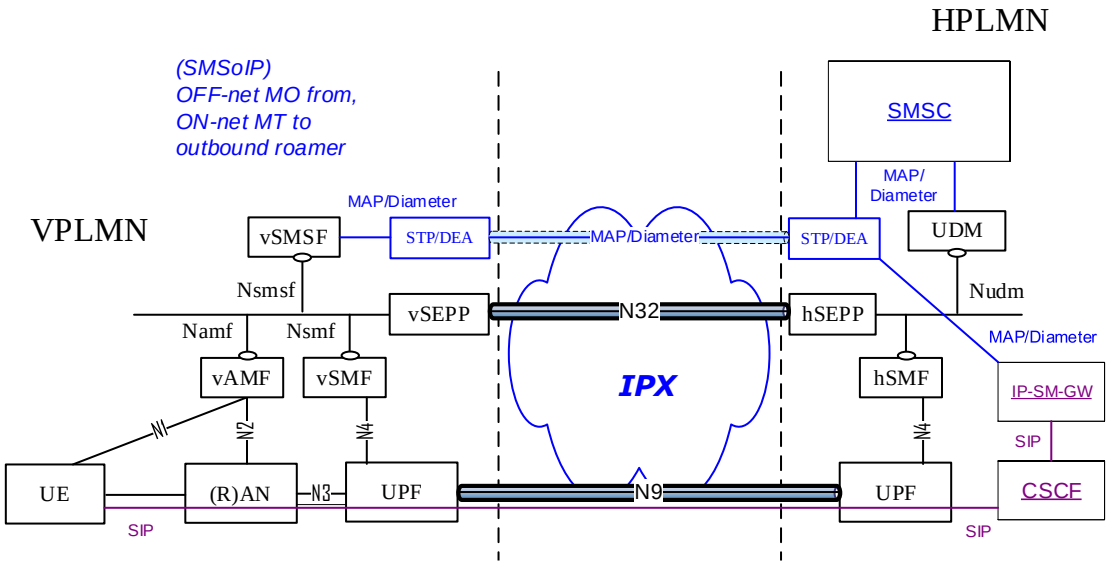

Figure 25 - SMSoIP Roaming

With the specification of SMS over Service Based Interface in Release 17, SMS roaming in 5GS is understood to be included within the scope of the SEPP protection over the N32 interface, as described in 3GPP TS 23.540 [121]. With reference to 3GPP TS 29.573 [86], SMS Roaming may be supported on the N32 links established with the specified purpose for "ROAMING".

As shown in Figure 26, besides the 5GC signalling for the outbound roaming subscriber between the Visited PLMN and Home PLMN, the subsequent SMS operations e.g. Mobile-Originated SMS by the roaming subscriber are transported over the N32 interface between the VPLMN and HPLMN. Therefore, these SBI operations are protected by the SEPP interworking over the N32 interface.

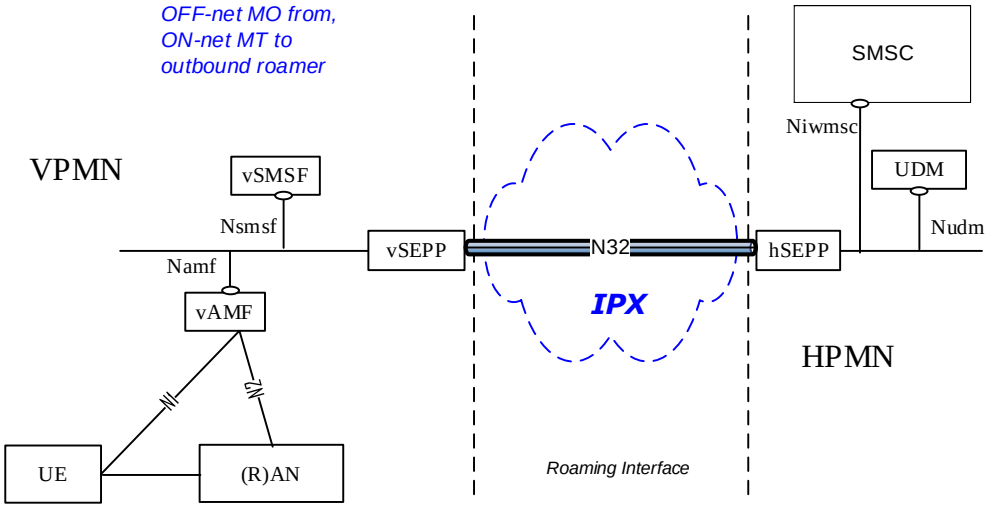

Figure 26 - SMS over SBI Roaming

The relevant NF support for SMS over SBI shall be indicated within the NF discovery phase. Therefore, if the concerned NFs do not support SMS over SBI e.g. in the VPLMN or HPLMN, SMS roaming may fallback to SMSoNAS over the legacy interfaces.

10.1.2 SMS Interconnect

Based on the description in 3GPP TS 23.501 [31] on the SMS architecture over NAS, the non-roaming and roaming interfaces shall also apply for inter-operator SMS. Therefore, we can expand on the following inter-workings for inter-operator SMS (with or without the IPX) as depicted in Figure 27:

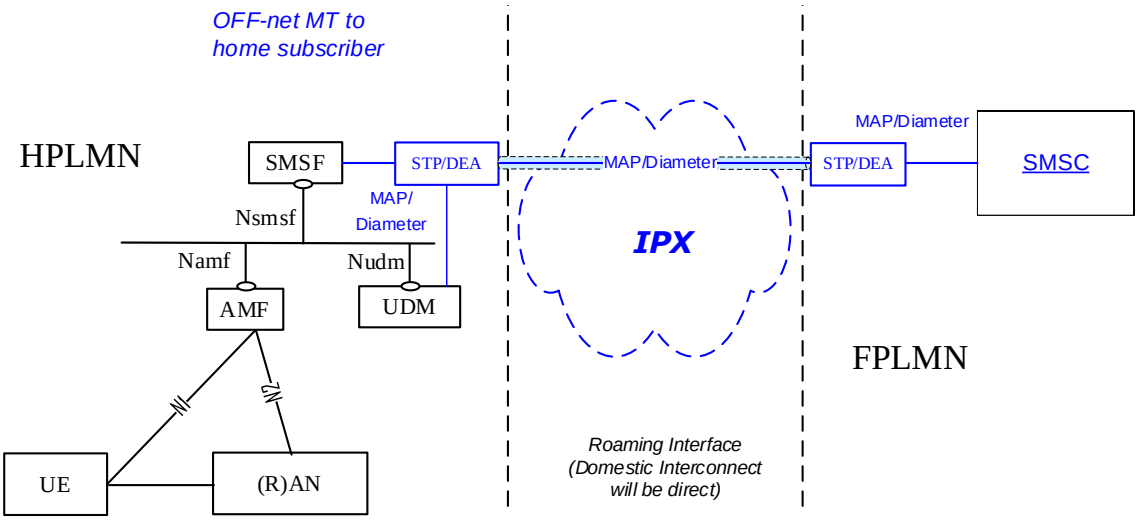

Figure 27 - Inter-operator SMS for Domestic (direct) and International (direct or via IPX) interworking

Based on the SMSoNAS architecture, inter-operator SMS in 5GS is supported over the legacy MAP/SS7 or Diameter interface for SMS interworking.

If SMS interworking is supported over Diameter End-to-End Security (DESS) [9], then such inter-operator SMS shall be protected with integrity and confidentiality protection.

However, if SMS interworking is supported over Message Application Part (MAP), which is part of the SS7 protocol stack, no such integrity or confidentiality protection can be offered to protect the privacy of the 5G subscriber.

With the specification of SMS over Service Based Interface in Release 17, SMS interworking in 5GS is understood to be included within the scope of the SEPP protection over the N32 interface, as described in 3GPP TS 23.540 [121]. With reference to 3GPP TS 29.573 [86], SMS Interworking may be supported on the N32 links established with the specified purpose for “SMS_INTERCONNECT”.

As shown in Figure 28, the SMS operations e.g. Mobile-Terminated SMS by the foreign SMSC to the home subscriber are transported over the N32 interface between the Foreign PLMN and HPLMN. Therefore, these SBI operations are protected by the SEPP interworking over the N32 interface.

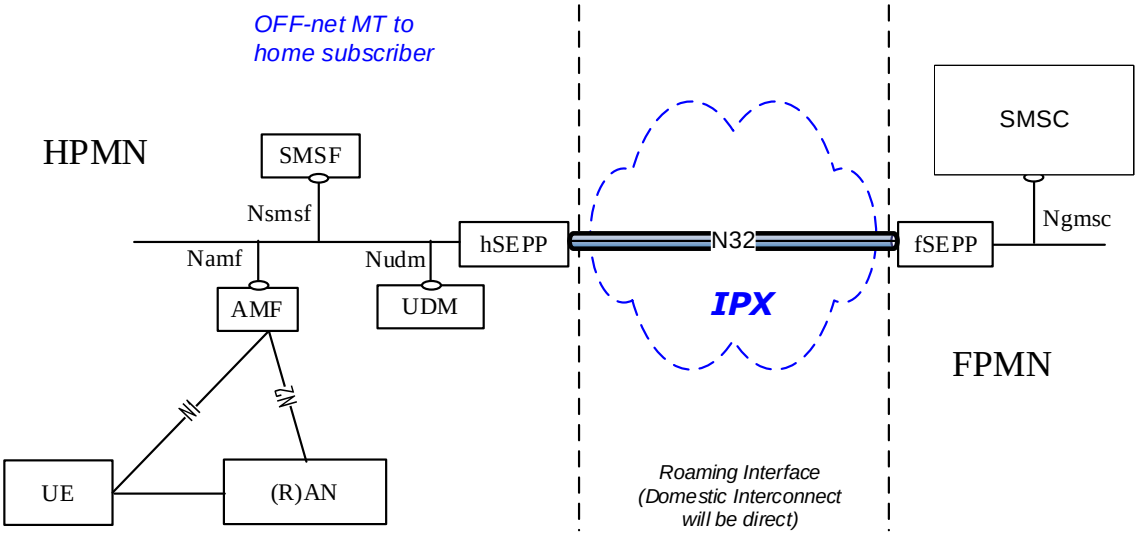

Figure 28 - Inter-operator SMS over SBI for Domestic (direct) and International (direct or via IPX) interworking

The relevant NF support for SMS over SBI shall be indicated in the NF discovery response. Therefore, if the concerned NFs do not support SMS over SBI e.g. in the HPLMN, SMS interconnect may fallback to SMSoNAS over the legacy interfaces.

10.1.3 SMS filtering

The Binary SMS Filtering Guidelines GSMA FS.42 [142] shall apply in the 5G SMS architecture.

10.2 Rich Communication Services (RCS)

RCS Interworking is described in IR.90 [57] and IR.65 [56] based on the RCS Technical Architecture as shown in Figure 29.

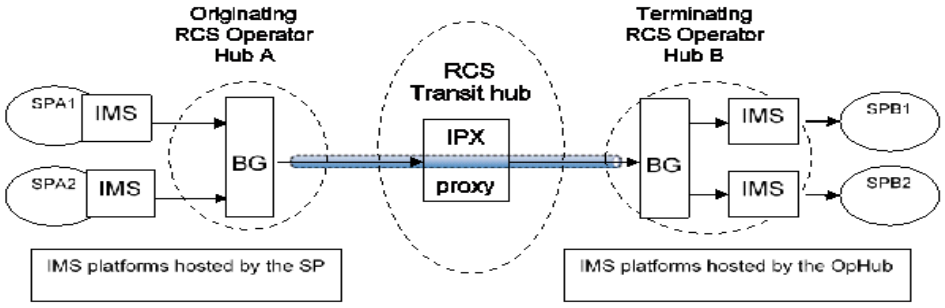

Figure 29 - RCS Technical Architecture, from Figure 5-5 in IR.65 [56]

Specifically in IR.65 [56], the originating and terminating service provider identities for RCS interworking are described in the Session Initiation Protocol (SIP) headers. However, there is currently no Inter-PLMN security specified for RCS interworking to support authentication, integrity and confidentiality protection, similar to DESS or SEPP interworking. Therefore, inter-operator RCS may be exposed to spoofing and the lack of privacy protection for 5G networks and subscribers.

Ideally, inter-operator RCS messaging should also be included within the scope of 5G inter-PLMN security. This may be supported via the 5GS interface for IMS interconnection and interworking. Otherwise, similar protection to DESS may need to be defined.

In the FS.41 RCS fraud and security assessment [75], hop-by-hop hub authentication has been recommended for the originating party to protect against spoofing. Additional security design considerations shall be required to support integrity and confidentiality protection.

In addition, a side channel vulnerability that attackers may exploit for sending spoofed RCS messages to targeted users is described in section 20.17.

10.3 Voice Service over 5G Network

Voice quality gained significant ground with Voice over LTE (VoLTE) with the deployment of 4G LTE networks. Voice over 5G, called Voice over New Radio (VoNR) service is built on continuous mobile networks advancements. Those advancements include evolved voice systems combined with 5G core network elements, (IMS), VoLTE enhancements, 5G NSA and other 5G New Radio (5GNR) radio access networks.

There are two ways for operators to leverage voice in 5G:

1. VoLTE: When no 5G Core is deployed, the operator can rely on the underlying VoLTE network including LTE Radio, EPC Core and IMS to deliver Voice for 5G users while the 5G eMBB services are delivered through 5G Radio and the enhanced LTE/EPC.
2. VoNR: When 5G Core is deployed, voice is delivered using the 5G Core functions and IMS while the 5G use cases are delivered by the NR and the 5G Core.

Advantages of VoNR include ultra-high-definition voice/audio for both voice-only calls as well as integration with applications and content such as announcements, music, conferencing, and more. VoNR will also provide enhanced support for real-time communications including Rich Communications Services (RCS) integration.

VoNR is anticipated to become increasingly more valuable to enterprise and consumer segments in parallel with the growth of next-generation applications, especially those involving immersive technologies such as augmented, virtual, and mixed reality. Anytime, anywhere telepresence, holographic communications, and telepresence robotics are some of the key solution areas that will leverage VoNR.

Voice services must be secured. This is achieved through securing all elements of the 5G network, which this document addresses.

11 User Plane Data Transfer with GTP-U

11.1 Overview

GTP-U is used in EPC for the bearer context establishment, modification and termination. These bearers carry voice, data and value-added services content. Use of GTP-U is inherited in 5G architecture.

To secure the GTP-U traffic at the PLMN perimeter, the use of TLS, IPSec or similar is recommended on the connections as well as adherence to the GTP-U security guidelines described in GSMA PRD FS.20 [62] and GSMA PRD FS.37 [64],[64]

For the user data traffic on the N6 interface to public network or private networks security according to GSMA PRD FS.37 [64] is recommended. Likewise, the recommendations to follow GSMA PRD FS.37 [64] guidelines for the user traffic extend to the N3 interface, which is between the RAN and 5G UPF.

11.2 Inter-PLMN User Plane Security (IPUPS) N9 Border Security Function

3GPP Release 15 introduced the SBA for the mobile packet core with CP and UP separation natively designed within the SBA. The SEPP enables an MNO to secure the perimeter protection for the CP of the 5GC. The equivalent perimeter protection for the UP, however, is achieved by a functionality referred to as IPUPS introduced in 3GPP Release 16 in the UPF itself, and not by a separate network function. It is applicable to home routed scenarios in the roaming architecture. It addresses the 3GPP Release 15 capability gap of UP protection on the inter-PLMN N9 interface and bolsters overall N9 protection acting at an application layer. In addition, the transport layer security control recommended at the inter-PLMN border is NDS/IP by means of IPSec with peering partners. It is recommended to secure N9 interface traffic with adherence to GSMA PRD FS.37 [64]

The IPUPS functionality as shown at the network borders on the N9 interface in Figure 30is based on a principle of detect, correlate and filter incoming GTP-U UP packets.

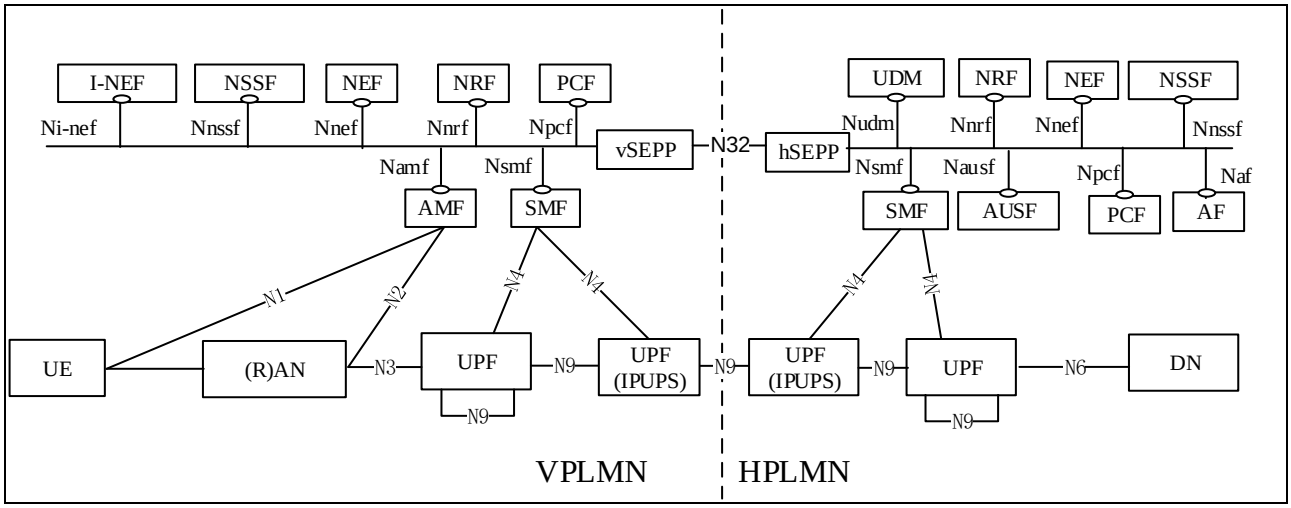

Figure 30 - IPUPS for UP protection on the inter-PLMN N9 interface

The SMF controls the packet processing in UPF by establishing, modifying and deleting Packet Forwarding Control Protocol (PFCP) session context on the N4 interface and provisioning of various rules. As a result, the protection mechanism on N9 is controlled and managed by the N4 interface between SMF and UPF. Three deployment models arise due to the introduction of IPUPS functionality within UPF:

1. A MNO could deploy a UPF with IPUPS.
2. A MNO could deploy a UPF without IPUPS.
3. A MNO could deploy IPUPS only, without regular UPF.

11.3 Packet Forwarding Model for PFCP Session Context Lookup

If a UPF is enabled for IPUPS, at the time of PFCP association on N4, the UPF sets the flag UUPSI (UPF configured for IPUPS) to Boolean value 1 informing SMF that IPUPS functionality within UPF is enabled.

The UPF allocates and stores a local F-TEID during the PFCP association procedure on the N4 interface per PDU session. This local F-TEID is the identifier for the UP tunnel that is unique per subscriber session. If the incoming GTP-U is destined for one of these tunnels identified by F-TEID, it is a valid packet. This detection mechanism relies on the packet forwarding model defined in 3GPP TS 29.244 [83].

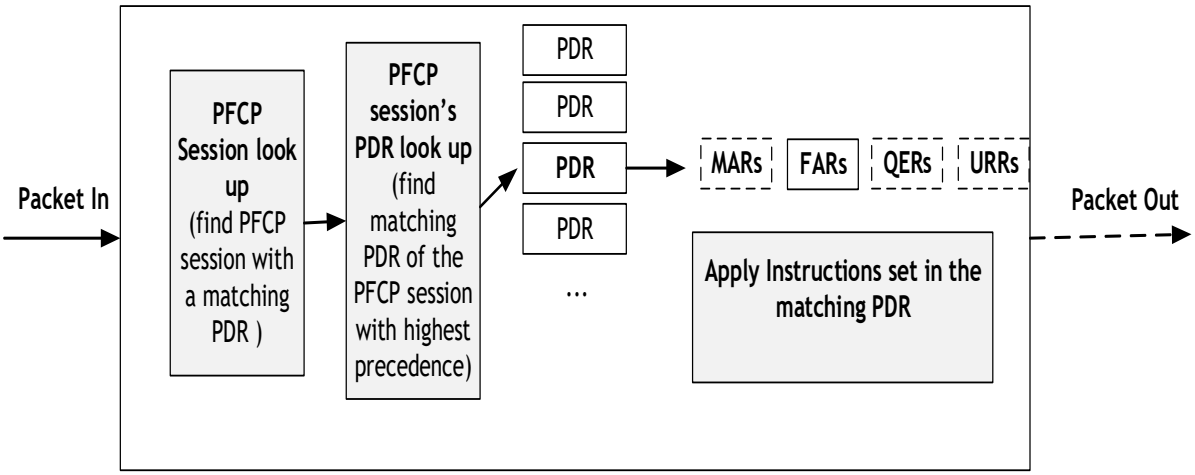

Figure 31 - Packet forwarding model for PFCP session context lookup

The packet forwarding model performs PFCP session context lookup as outlined in Figure 31.

- Each PFCP session context has a number of Packet Detection Rule (PDR).
- Once the matching PFCP session context is found, the corresponding PDR is looked up.
- Each PDR has one or more identifiers to match against. F-TEID forms one of these identifiers for outer IP packet matching for the incoming GTP-U packets.

The PDR screening stops screening as soon as the first matched highest precedence PDR is found. If the incoming GTP-U packets are received at the PLMN for the existing and allocated F-TEID matched by the PDR, then GTP-U packets are permitted. Otherwise, they are dropped. The IPUPS functionality is defined in 3GPP TS 23.501 [31] and 3GPP TS 33.501 [1] and GSMA PRD FS.37 [64] describes the implementation in MNO networks, also referenced in GSMA PRD NG.113 [58].

12 Legacy Signalling Technologies

12.1 Current Situation

Operators still mainly use SS7 on inter-connect to support international roaming services. The security vulnerabilities and the security measures applicable to SS7 are described in GSMA PRDs FS.07 [6], FS.11 [7] and IR.82 [8].

Diameter is positioned as a successor to SS7. Similar security risks apply to Diameter as for SS7 as well as the end-to-end security risks due to topology hiding with the hop-by-hop routing in Diameter Edge Agents (DEAs). The security vulnerabilities and the security measures with Diameter are described in GSMA PRDs FS.19 [9] and IR.88 [10].

The combination of SS7 and Diameter requires special attention for the protection against multi-domain attacks. This situation will be further complicated with the use of HTTP2 and JSON for 5G. See FS.36 [52] for further details.

This is especially the case when, in early Non-Stand Alone (NSA) deployments, there will be a 5G NR combined with existing 4G CN deployments like:

- When a 5G RAN is deployed with an existing 4G CN, security operates according to the LTE principles because the SIM interacts with the MME in the 4G CN. The 5G security concept of SUPI and SUCI doesn't work in such implementation situations.
- In roaming situations where the combination of technology in the VPLMN and that in the HPLMN influence the security offered to the UE as further detailed by the 5GC roaming guidelines in NG.113 [58].

The risks from interworking with different technology generations and signalling protocols are outlined in detail in FS.21 [17] and NG.113 [58].

12.2 Coexistence of Signalling Protocol Suites

The co-existence of multiple generations protocol suites and technologies offers an excellent opportunity for hackers to exploit weaknesses of all deployed signalling protocols. . Multi-Protocol filtering logic, based on protocols' behaviours, is essential because the roaming actions are protocol agnostic and multi-protocol attack vectors can be foreseen. Attackers are often not interested in a particular technology but are hired to perform certain tasks e.g. location tracking, DoS or eavesdropping. Due to the migration from 4G to 5G, and the continued support of interfaces for legacy partners, it is assumed that different generations of signalling protocols will coexist in many networks.

In addition, for verticals which connect to 5G at the User Plane Function (UPF) or at the Network Exposure Function (NEF) one has to consider the local service execution with SDN and Multi-access Edge Computing (MEC), which will require a flexible and distributed security architecture and detailed information element grained filtering.

As a result, all 5G SA and 5G Non-Standalone (5G NSA) scenarios should be protected. Figure 32 sketches the multi-domain signalling coexistence assuming SS7 is interworked to HTTP2 via Diameter, and reverse.

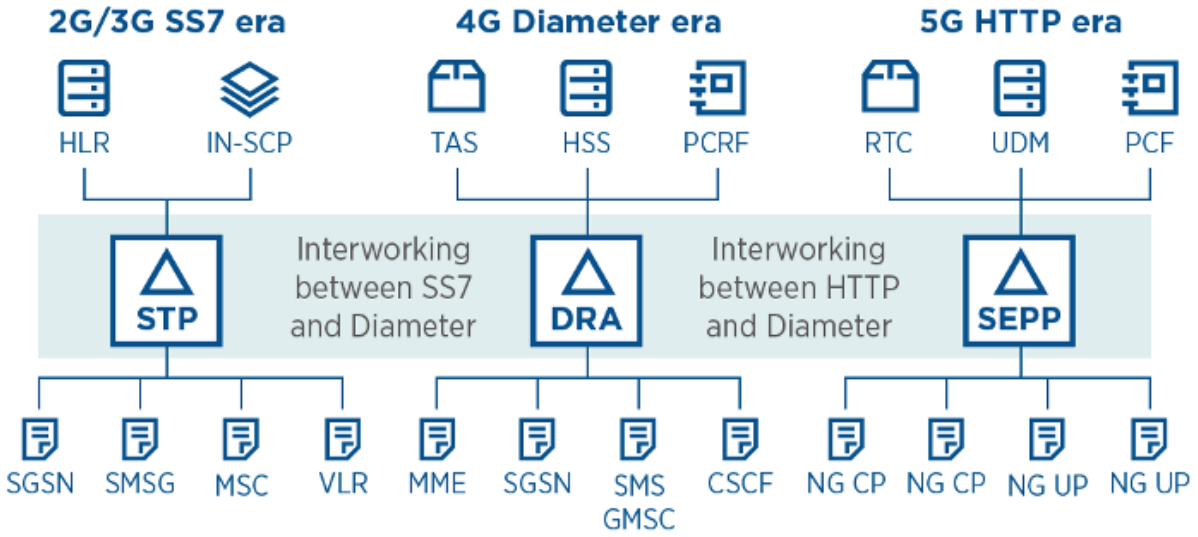

Figure 32 - Multi-domain signaling scenario between different technologies

Figure 33 sketches the protection capabilities with the various combinations of signalling technologies.

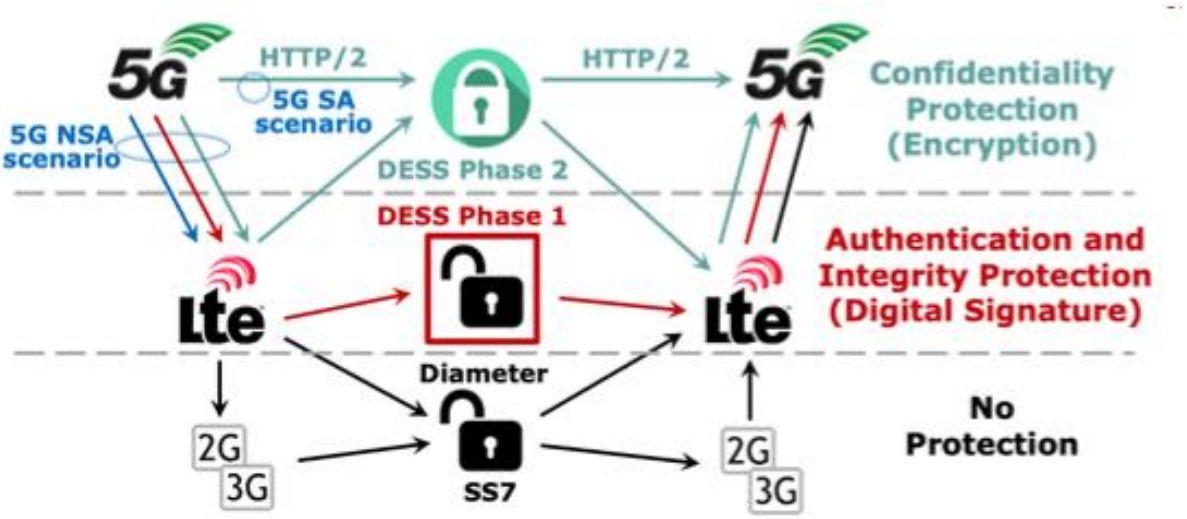

Figure 33 - Protection capabilities for multi-domain signaling between different technologies

The following protection capabilities are provided as part of the signalling protocol stacks for the different roaming scenarios with the use of different signalling technologies:

SS7 provides no protection capabilities and use of screening functions in Signalling Transfer Points (STPs) and SS7 firewalls are needed to secure the SS7 signalling traffic between roaming partners. For further details see FS.11 [7].

A similar lack of protection applies to Diameter but with the implementation of DESS Phase1 the end-to-end security of the Diameter messages significantly enhanced by the addition of a signature for Integrity Protection. This offers MNOs the capability to detect any manipulation of a message according to FS.19 [9], FS.21 [17], IR.88 [10] and FS.34 [53].

With the support of DESS Phase 2, the privacy sensitive user content and specific network identifiers within the Diameter messages are also secured by the additional Confidentiality Protection capability.

In the SA-based deployment scenarios, i.e. 5G RAN and 5G Core, the N32 interface between SEPPs of 5GCs will provide confidentiality protection for the signalling messages between roaming partners. See for further details TS 33.501 [1].

As an illustration, Figure 34 shows in more detail the SA-based mobile roaming scenarios with the best protection capability. This is with end-to-end supported confidentiality protection (on top of authentication and integrity protection) by means of either a Digital Signature (DESS Phase 2) or HTTP/2 per security perimeter segment. The diagram shows that confidentiality protection can only be supported for a 5G UE when the device is end-to-end controlled either by:

The 5G SA scenario with end-to-end HTTP/2 signalling support between SEPPs via the N32 interface as specified in GSMA PRD FS.36 [52].

The 5G NSA scenario with end-to-end DESS Phase 2 enhanced Diameter signalling support between the DEA/SigFW border elements of the EPC networks as specified in GSMA PRD FS.19 [9].

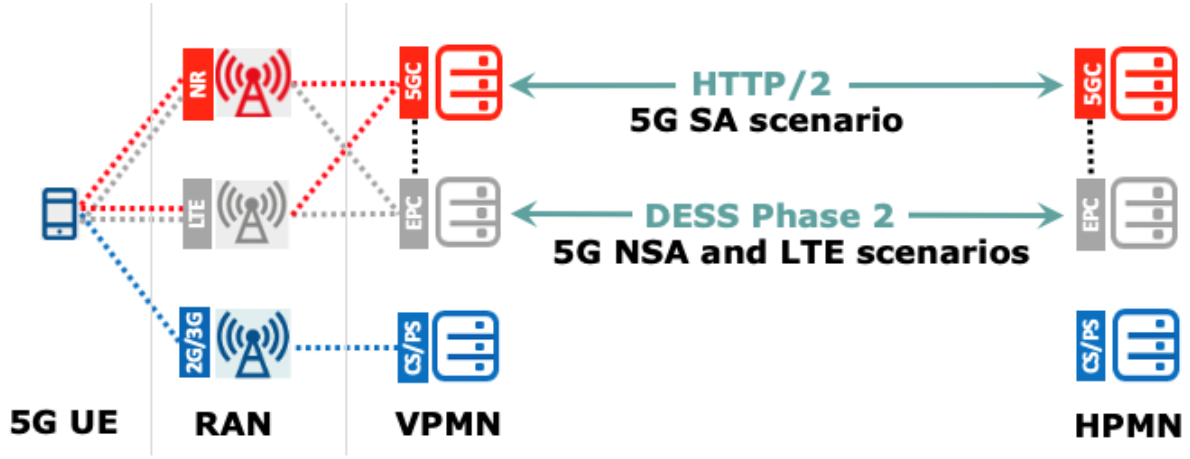

Figure 34 - Confidentiality Protected Roaming Traffic Scenarios

It is important to note that the aforementioned confidentiality protection can be offered assuming that the corresponding UEs have not been compromised.

The 5G signalling security enhancement is impacted in the scenarios, where legacy networks are deployed, For example, in the legacy roaming scenarios when the roaming signalling traffic is exchanged via either the standard Diameter signalling (without the DESS enhancements) or via SS7 signalling, the 5G signalling security enhancements don't apply. This is illustrated in Figure 35, and applies for the following roaming scenarios with a 5G UE:

The 5G NSA scenario with the standard Diameter support between the DEA/SigFW border elements of the EPC networks as specified in GSMA PRD FS.19 or by means of the SS7 signalling as specified in GSMA PRD FS.11 [7].

When the 5G UE is paging in 2G or 3G because then the roaming is being supported via SS7 signalling as specified in GSMA PRD FS.11 [7].

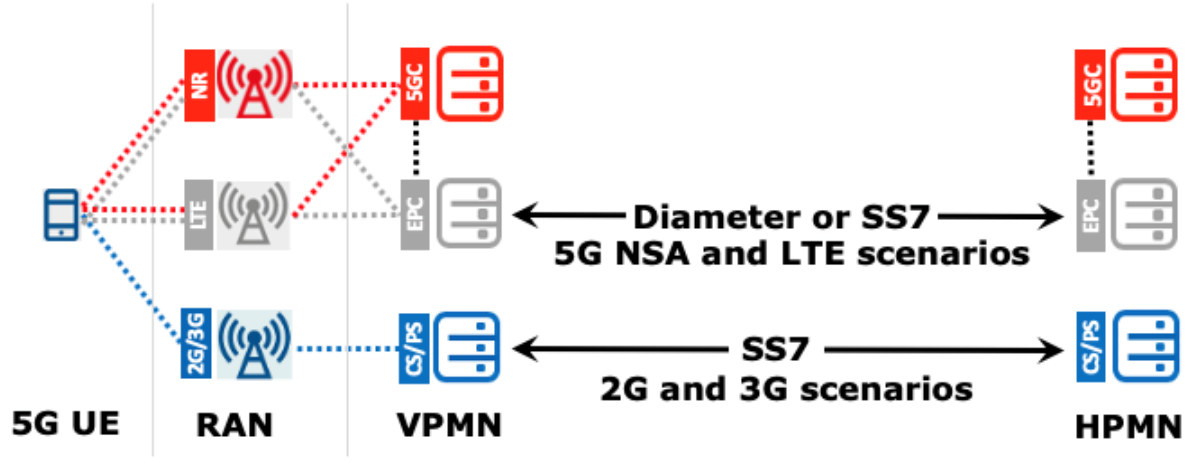

Figure 35 – Least Protected Roaming Traffic Scenarios

Note: Typically, SS7 is used for the 2G and 3G roaming scenarios. However, for 3G PS Diameter may also be used via the S6d interface.

GSMA PRD FS.21 [17] contains a complete overview of the other scenarios and the security impact that is exposed via the network signalling with the existence of legacy technologies like 2G, 3G, 4G and 5G in combination with the coexistence of SS7, Diameter and HTTP/2 signalling protocol suites.

In addition, these threats are extensively addressed in the report “ENISA Threat Landscape for 5G Networks – Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)” [60].

On the signalling firewall side, the SEPP has to work with 2G, 3G, 4G signalling firewalls as the existence of legacy protocol suites and technologies offers an excellent opportunity for hackers to build attack vectors with access via different signalling connections.

For 5G deployments with the NSA-based architecture, roaming traffic is handled between 4G CNs with the result that the security of the roaming traffic is via SS7 and/or Diameter and, therefore, needs additional protection by screening functions and firewalls.

To support end-to-end roaming between 5G Core SA-based networks, it is assumed that roaming will depend on the new authentication procedures with SUPI/SUCI and require N32 support end-to-end as a prerequisite.

12.3 Parallel Roaming Security Risks

According to NG.113 v2.0 Section 5.2, “it is anticipated that both 5GS roaming and LTE roaming using EPC as well as 3G/2G roaming using a circuit switched and mobile packet core will be provided at the same time between two MNOs“. It is expected that operators may support at the same time:

- REST API / HTTP2.
- GTP-C.
- Diameter.
- SS7.

The degree of support for legacy protocols depends on many factors:

- Migration and extension strategy for core and radio network.
- Support of roaming partners and ecosystem partners with legacy infrastructure.
- Support of services running using legacy protocols.
- Support of devices without feature support e.g. SMSoNAS instead of RCS.

Whenever such a multi-protocol agreement is in place, it may be possible for a misbehaving roaming partner or IPX ecosystem partner to attack targeted victims using less secure signalling channels. This kind of behaviour where attackers change the attack vector has been observed, when operators started rolling out SS7 firewalls, when attackers started using binary SMS for location tracking. For example, in an 5G attack scenario, an attacker could issue fraudulent or otherwise abnormal “location updates“ over SS7, pretending that an otherwise 5G-enabled customer (whose phone is switched off) currently roams using 2G.

The roaming partner may even be tricked into initiating such signalling by an external attacker.

This effectively negates the security benefits of 5G signalling security and provides a legacy attack vector, including 5G authentication confirmation, in which the home operator obtains strong cryptographic evidence that its customer is indeed roaming with the visited network as the incoming signalling suggests.

In order to increase the level of security in situations where networks have SEPP, Diameter, GPRS Tunnelling Protocol – Control (GTP-C) and/or SS7 signalling links in parallel, it is appropriate for the home operator to ask the question “is it reasonable that signalling for this customer arrives over this channel from this partner?“. “Did we see an invalid request for another protocol for this customer?”

In this context, the home operator should be able to block incoming signalling on the basis of the channel on which it arrives in combination with context information from other channels. If, for example, a customer is 5G-roaming in B’s network for some time (business trip), then the home network should be rejecting SS7 signalling from B for that customer – even if that signalling appears to be legitimate with all other fraud detection systems in place.

There are certain trade-offs between security, efficiency and connectivity. For example, some geographic areas may only have 2G coverage by an otherwise 5G operator. In such cases the home operator must be able to not cause connectivity issues for its customers. The creation of false positives needs to be minimised and key security issues clearly identifiable in a multi-protocol protection to avoid overloading the security team.

Certain user groups may have more strict security requirements and may be happy to lose connectivity if the signalling security level is too low. The subscription profile today allows fine tuning of security e.g. Subscription-Data-Flags to push the security level higher for sensitive customer groups. Another approach can be taken via the Policy Control Function (PCF), but this is more in terms of QoS. The SEPP can in cooperation (to avoid bypassing) with other signalling traffic filtering engines enforce user, user group or slice specific attack countermeasures. In addition, the network itself needs to have sufficient support of the security features offered by 5G e.g. deploying a real key for SUPI concealment.

13 Impact of Cloud on 5G Security

13.1 Overview

Three separate technology trends have major impact on 5G rollout:

- For some operators may choose to deploy 5G Core and RAN network functions as cloud-native containerised applications in contrast to the traditional physical and VM-based developments, many open-source tools are now mature enough to be bundled into a product that can easily build an infrastructure for these cloud-native network functions. Such implementations are considered to run Containers as a Service.
- Major public cloud providers are extending their reach from a limited number of data centres in a limited number of cities, to much more points of presence across the world by both developing products that can work outside their data centres and also

building a global network infrastructure that makes it possible to build reliable and available connections to them from most of the world.

- SDN in the form of overlay network fabrics that are readily available to implement without the need for extra development and maintenance by service providers. These can easily extend inside service provider data centres as well as into the public cloud landing zone.

All these, plus the desire to build services customised to enterprise needs over an edge compute environment, have built the momentum to build the 5G Core and RAN environments using Containerised Network Functions (CNF) rather than Virtualised Network Functions (VNF).

Securing these cloud-native networks has its own advantages and challenges that are completely different from the traditional VM-based and physical networks.

Securing the environment in the network layer is no longer efficient, using traditional firewalling for example. Firewalls to be used for these environments need to be cloud-native themselves. This is partly because of the nature of cloud applications that are short-lived, assume a dynamic IP address whenever there is a change and may even move between different computers and data centres based on the logic that is built into the Kubernetes.

Patching, and generally lifecycle management, is very different from traditional network functions. A containerised network function is, by definition, an immutable block that can't be modified e.g. patched. Every new version of the network function will simply be run and replace the old container instantly. This is a significant advantage because updating and addressing security issues can be done much faster and with automation.

Network function implementation, configuration and operation are now all automated using a CI/CD pipeline. The pipeline receives the container, verifies it, reads the configuration from a git repo and runs the function as expected. Security considerations must have been considered in all these artefacts. As mentioned in Section 9.2 (Core and RAN Elements Patching), core elements workloads must be secured continuously due to fluency of the containerized 5G environment. All CNF workloads must be validated continuously, as addressed in ETSI NFV SEC [147] or NIST SP 800-190 document [144] - Application Container Security Guide.

13.2 Multi-Cloud Ecosystem

A multi-cloud ecosystem has emerged to support 5G technologies, devices (e.g., IoT) and different application use cases. There are multiple public and private network environments that are at the customer site, carrier network edge, carrier core network, and partner networks. Cloud computing exists to address the scaling of storage and computing resources. Disaggregated functional architectures and the associated virtualised platforms and open software frameworks reside in these environments.

With different network domains, products and business partnerships, the responsibility for managing these different cloud environments falls to different organisations including carriers, internet and cloud service providers, suppliers, and enterprises. For different cloud service architectures (e.g., PaaS, IaaS), the shared operations responsibility model can create additional security challenges.

As cloud infrastructures become a key element in the 5G ecosystem, cloud-focused threats and associated Tactics, Techniques and Procedures (TTPs) are part of the attack surface landscape. The emerging threat frameworks MITRE FiGHT, GSMA MOTIF, CSA Cloud Adversarial Vectors, Exploits, and Threats (CAVEaT™) and the Cloud matrix of the MITRE ATT&CK® Framework [79] provide a systematic approach to capture adversarial behaviour targeting cloud environments.

Examples of cloud associated adversarial behaviours include the following:

- **Initial Access –** compromising user administration accounts that are not protected by multi-factor authentication.
- **Evasion –** modifying cloud compute instances in the production environment by modifying virtual instances for attack staging.
- **Discovery –** using open-source tools to discover what cloud services are operating and then disabling them in a later stage to avoid detection.
- **Data Exfiltration –** moving data from the customer's production databases to the hacker's cloud service account or transferring the data out of the Communication Service Provider (CSP) to the attacker's private network.
- **Service Impact –** creating denial-of-service availability issues by modifying Web Application Firewall (WAF) rules and compromising APIs and web-based GUIs.

13.2.1 Cloud Infrastructure Reference Model (CIRM)

The CIRM in GSMA PRD NG.126 [80] is defined by the GSMA Open Infrastructure Task Force (OITF) in a joint initiative with the Linux Foundation in the joint Cloud infrastructure Telecom Taskforce project (CNTT).

This PRD specifies a virtualisation technology agnostic (VM-based and container-based) cloud infrastructure abstraction and acts as a "catalogue" of the exposed infrastructure capabilities, resources, and interfaces required by the workloads.

The document includes an extensive security chapter that examines multiple aspects of security related to a single cloud infrastructure and security aspects for workloads. Future work will address multi-cloud architectures.

In addition to describing high level security attack vectors, the document recommends cloud infrastructure security requirements. Specifications and documents covering security requirements and best practices published by standards organisations are also listed in a dedicated section.

The document concludes with a consolidated set of essential and desired recommendations. Operators are advised to carefully evaluate the recommendations for possible implementation.

13.2.2 Multi-Cloud Security Considerations

With multiple cloud environments, technologies and administrative entities, there are additional security principles to be considered:

- **Policy synchronization –** there should be consistency in applying the right security policies across environments, services, interfaces and configured resources.

- **Visibility –** a common data model approach should be developed to capture events and behaviours across all of the key compute, storage, network, and applications resources, environments, virtualised platforms, containers and interfaces.
- **Monitoring –** the approach should entail centralisation, correlation and visualisation of security information across the different cloud environments to provide an end-to-end view and enable timely response to attacks. A single pane of glass to control and monitor data security, including key management and encryption based on ISO 19790 [146] or FIPS 140-2 Level 3 HSM is recommended.
- **Automation –** there are critical activities that should be automated including cloud security posture management, continuous security assessments, compliance monitoring, detection of misconfigurations and identification and remediation of risks.
- **Access Management –** the wide array of users including administrators, testers, DevOps, and developers and customers should be organised into security groups with privileges appropriate to different resources and environments.
- **Security Solutions –** besides using the security services provided by cloud service providers, the use of vetted third-party tools and services should be incorporated into the overall security operations model.

13.2.3 Secure Public Clouds for Telcos

The ETSI standard TS 103 457 “Interface to offload sensitive functions to a trusted domain” [35] provides extra security requirements for public clouds to offer telcos the option of running public telecom network functions in public clouds.

The standard provides extra security for sensitive functions down to individual Virtual Machines. It introduces a trust hierarchy onto the flat admin architecture of public clouds so that only a subset of telco engineers or processes can access these sensitive functions.

See for further explanation “ETSI Secure Public Clouds for Telcos” [36].

In addition, considerations of data sovereignty and compliance with national regulations become increasingly relevant, particularly in the context of public telecom network functions operated in public clouds. This is where BYOK (Bring Your Own Key), HYOK (Hold Your Own Key), and BYOE (Bring Your Own Encryption) strategies play a critical role.

These approaches allow telecom operators to maintain control over encryption keys and encryption processes, aligning with specific national regulatory requirements and data sovereignty concerns. BYOK and HYOK enable operators to manage their encryption keys according to their policies, either by bringing them into the cloud environment or holding them in their own secure premises. BYOE takes this a step further by allowing operators to use their own encryption algorithms and processes, ensuring that sensitive functions and data are handled in strict compliance with local laws and standards.

Public commercial cloud also introduces their account identities and credentials in addition to identities and tokens used for applications running on the cloud. These identities and accesses must also be secured, as cloud master accounts have full privileges and can also create and revoke any associated identities and access rights for entire tenant cloud services.

These practices not only fortify the security of virtual machines running sensitive functions but also provide a framework for telecom operators to exercise greater control and compliance over their data in public cloud environments.

13.3 Impact of 5G Functions' Virtualisation on Security

In the virtualised world the threats can be more devastating than in the physical world. While left undetected, those threats could propagate to other VNFs/CNFs, all located within one physical entity or in separate ones. Typical implementations of VNFs/CNFs come with a lack of visibility from host OS to guest virtual machines or containers resulting in several potential vulnerabilities to the overall network infrastructure.

5G network must be designed to ensure its security, its users and their traffic against cyber-attacks, regardless of it using NFV/SDN principles. Appropriate flexible security mechanisms should be considered and applied. Those security mechanisms should include and be not limited to containers' workloads security assurance, API security, deployed protocols' validation at Layer 7 of the OSI reference model, threat detection and mitigation between VNFs/CNFs, including protection of the interfaces external to SBA.

Ensuring the security of data stored by telcos, whether in storages, databases, or file shares, demands meticulous attention. It is advised to employ robust encryption and key management solutions, consistently maintaining sensitive data in encrypted form. It is advisable for the operators to be cognitive of the latest developments in the Post-Quantum world security principles, including and not limited to hybrid environments.

With 5G networks implemented based on cloud technology, attention needs to be paid to network design principles in the context of security in 5G e.g.:

- Less visibility from OS to the guest Virtual Machines (VM) / Containers with the Virtualisation or Containerisation.
- Its design shall secure the network, the users and traffic with flexible security mechanisms.

13.3.1 Cloud Native Applications and Containerisation Security

Containerisation is an OS level virtualisation technology. Containers are packages that rely on virtual isolation to deploy and run applications that access a shared OS kernel without the need for virtual machines (VMs). Containers hold the components necessary to run desired software. These components include files, environment variables, dependencies and libraries. The host OS constrains the container's access to physical resources, such as CPU, storage and memory, so a single container cannot consume all of a host's physical resources. Containers are well-adapted to work with microservices, as each service that makes up the application is packaged in an independently scalable container. For example, a microservices application and supporting infrastructure can be composed of containerised services that generate alerts, log data, handle user identification, authentication and authorisation, routing and provide many other services. Each service operates on the same OS while staying individually isolated. Each service can scale up and down to respond to demand. Cloud infrastructure is designed for this kind of elastic, unlimited scaling. Some service mesh implementations are based on OSS components that need to be managed properly. The NIST publication NIST SP 800-204B entitled "Attribute -based Access Control

for microservices-based applications using a service mesh [114] provides additional guidance.

The cloud native concept is first introduced to Service-Based Architecture networks and characteristics such as finetuning, service customisation, high throughput are key enablers for 5G, which will see more effective execution, higher deployment density and second-level scalability. ETSI's defined NFV architecture, Network Function Virtualisation Infrastructure (NFVI), supports 6 types of virtualisation technologies, the foundations of which are VMs and containers. Containers and microservices are the evolution of NFV cloud native and security is a significant consideration for their rollout. For example, host OS security is a typical container security threat as the lack of isolation from the host OS may be a potential risk. Because containers share a host OS, the obvious security threat is that the entire system can be more easily accessed and attacked when compared with hypervisor-based virtualisation. There are also container attack tools (e.g., Rhino Cloud Container Attack Tool) that facilitate different types of attacks. The container security threats also include aspects such as compromised container image file and registries, container management and orchestration functions, container lifecycle management patches and updates, and container run-time security, etc. In order to facilitate the rollout of 5G networks and services, security technologies to address these threats need to be considered in a timely manner.

For managing containers and microservices, Kubernetes and its associated infrastructure is becoming a popular choice, and it is also being integrated with the Continuous Integration/Continuous Delivery (CI/CD) tooling and processes for deploying applications and updates. There are many components of a Kubernetes infrastructure such as an API server, Kube scheduler, and Kubernetes controller manager that need to be hardened. In addition, Kubernetes functions need to be configured to restrict access to container image repositories and clusters, enforce runtime policies (e.g., applications should not run as root), and control ingress and egress communications to containers and microservices.

ETSI NFV SEC 023 [147] and NIST SP 800-190 document [144] give guidelines on applying container security.

13.3.2 Safeguarding Containers in Multi-Tenant Cloud Environments

The NIST Internal Report (NISTIR) 8320A "Hardware-Enabled Security: Container Platform Security Prototype" [98] explains an approach based on hardware-enabled security techniques and technologies for safeguarding container deployments in multi-tenant cloud environments. It also describes a proof-of-concept implementation of the approach - a prototype - that is intended to be a blueprint or template for the general security community.

13.3.3 Security Guidelines for Storage of UICC Credentials

GSMA PRD FS.43 [90] provides security guidelines for the protection of UICC credentials stored within an MNO. Use of a HSM is needed to ensure that the credentials are never exposed and potentially intercepted when stored in the memory of functional elements like the UDM. With the virtualisation of service logic multiple new intrusion points are introduced that potentially imply security risks like:

- The OS, like Linux, via which access is given to application elements like UDM.
- The OS that is supporting the hypervisor.

- Hardware maintenance interfaces.

This is an unsolved technical issue not reflected in ETSI NFV standards or the 3GPP standards. As a result, key material should be kept in a separate non-virtualised box.

For the storing of the authentication credentials encrypted in a secure hardware component as in TS 33.501 [1], the HSM should be based on the following principles as in FS.43 “Security Guidelines for Storage of UICC Credentials” [90] like:

- Unencrypted Ki must never exist outside of an HSM, neither for storage nor for processing.
- A unique storage key must exist inside the HSM which will not be used for any purpose other than encryption/decryption of Ki used by the Authentication Centre.
- EKi(store) to 5G vector calculation must take place inside an HSM.

Additionally, the support for multiple simultaneous algorithms in ETSI TS 103 457 “Trusted Cross-Domain Interface: Interface to offload sensitive functions to a trusted domain” [35] like:

- Milenage with Encrypted Ki in external databases, operational OP code in HSM.
- Calculation of 5G vectors 5G AV (RAND, AUTN, HXRES*, KSEAF*).

Security principles for Authentication in the HSM in ETSI TS 103 457 [35] like:

- Ki must not be visible to the HSS/AUSF.
- Provisioning / transport / storage encryption keys must not be visible to the HSS/AUSF.
- Authentication algorithms must not be visible to the HSS/AUSF.
- Keys and codes (such as OP code) must not be visible to the HSS/AUSF.
- Provisioning of HSM must be possible from a dedicated key management server.
- RAND calculation should take place using HSM random number generators.
- Rate limitation: possibility to limit the number of queries per IMSI to N/minute.
- Algorithm enforcement: HSM should not deliver COMP-128 vectors for a 3G/4G IMSI.

The need for implementation of a HSM in a virtualised software environment has been affirmed by GSMA FASG. This is aligned with the guidelines in FS.43 “Security Guidelines for Storage of UICC Credentials” [90].

In this context, ETSI TS 103 457 “Trusted Cross-Domain Interface: Interface to offload sensitive functions to a trusted domain” [44] tackles the challenge of secure storage – where organisations want to protect customer data whilst still using a cloud that is not under their direct control.

Many organisations need to protect this data, but when it is held in a virtual network or cloud, the organisation often doesn’t have control of this storage solution. TS 103 457 solves this problem, by standardising an interface between a “secure vault” like HSM that is trusted and a cloud that could be anywhere, where such sensitive data is stored in the vault. This allows a sensitive function to exist in a lower security environment, with data held securely.

This new specification offers multiple use cases. For instance, this interface can be used with new NFV technology to allow secure authentication of users for billing purposes.

Virtualisation means that processing can happen anywhere and might be untrusted, therefore these secure vaults are needed to protect sensitive functions and data. This is more common as NFV technology becomes widespread.

The interface can also be used to search databases that hold private data. Another feature defined in the specification is a logging function that allows queries of customer data to be audited, making it easier to detect data breaches, which in turn deters malicious activity.

This ETSI standard proposes a new interoperable interface, so that an organisation may change “vault” or cloud provider and still achieve the same functionality, which is vital in a world of evolving technology.

14 Network Slicing

14.1 Overview

Network slicing is defined in GSMA’s Future Networks document “An Introduction to Network Slicing” [110] as “the embodiment of the concept of running multiple logical networks as virtually independent business operations on a common physical infrastructure in an efficient and economical way. This is a radical change of paradigm compared to current implementations. With network slicing the 5G network is able to adapt to the external environment rather than the other way around”.

A Network Slice incorporates multiple components defined by 3GPP and beyond.

Within a 3GPP system, TS 23.501 [31] and TS 28.530 [111] define the functions involved in a Network Slice in a PLMN and shall include:

- The 5G Core Network CP and UP Network Functions.

In the serving PLMN, at least one of the following is included:

- The NG-RAN.
- The N3IWF or TNGF for non-3GPP Access.
- The Trusted WLAN Interworking Function (TWIF) for trusted WLAN in the case of support of N5CW devices.
- W-AGF for Wireline Access Network.

There are several key 5G Core functions that manage UE access to a network slice.

- The Network Slice Selection Function (NSSF):
    - Selects the set of Network Slice instances (NSI) serving the UE.
    - Determines the Allowed/Configured NSSAI and maps to Subscribed S-NSSAIs.
    - Determines the AMF Set to be used to serve the UE.
- The Network Slice Specific Authentication and Authorisation Function (NSSAAF):
    - Supports Network Slice-Specific Authentication and Authorisation with a AAA Server (AAA-S).

- The UICC can be involved in the NSSAA procedure:
    - The specific SSIM application [132] is used for authentication and slice credential management in the UE side.

5G introduced Charging Function (CHF) to collects charging-related information from various network elements and functions, aggregates it, and provides it to the charging system for billing purposes. It ensures accurate accounting of resource usage and service consumption. CHF is an integral entity in CCS (Converged Charging System) which provides an Account Balance Management function, Rating Function, and Charging Gateway Function. If compared with 4G EPC, CHF combines the functionality of OCF (Online Charging Function) and CDF (Charging Data Function). CHF plays a critical role in network slicing when creating slices based on differentiated services. A future version of this document will provide more details on the CHF.

14.1.1 Understanding S-NSSAI

The S-NSSAI - identifies a Network Slice, which is comprised of Slice/Service type (SST) and an optional Slice Differentiator (SD) and a NSSAI is a collection of S-NSSAIs. The NSSAI is used by the RAN for AMF selection.

A NSI can be associated with one or more S-NSSAIs, and an S-NSSAI can be associated with one or more NSI and Multiple NSI associated with the same S-NSSAI may be deployed in the same or in different Tracking Areas.

The operator can deploy multiple Network Slices delivering exactly the same features but for different groups of UEs, and the network may serve a single UE with one or more NSI simultaneously.

A Network Slice access can be subject to specific authentication, the NSSAA procedure, independent to the primary authentication.

14.1.2 Network Slicing In Roaming

Network Slicing can also be supported in Roaming scenarios. The NSSF in the VPLMN determines the Allowed NSSAI without interacting with the HPLMN.

The Network Slice specific functions in the HPLMN are selected by the VPLMN via support from the HPLMN NRF by using the related S-NSSAI.

14.1.3 Interworking with EPC

A 5GSA operating a network slice may need to interwork with the EPC in its PLMN or in other PLMNs. Mobility between 5GC to EPC does not guarantee that all active PDU Session(s) can be transferred to the EPC.

When the UE moves from EPC to 5GSA, the UE includes the S-NSSAIs associated with the established PDN. The UE provides the AMF the S-NSSAIs values for the Serving PLMN using the latest information from EPC and 5GSA.

In the home-routed roaming scenario, the AMF selects the default V-SMFs. The PGW-C+SMF sends PDU Session IDs and related S-NSSAIs to AMF.

14.1.4 Network Slice as a Service

A Network Slice as a Service (NSaaS) can be offered by an operator to its Communication Service Consumer (CSC) in the form of a service. This allows CSC to use the network slice either as the end user or to operate the network slice as manager. CSC can in turn play the role of CSP offering its own services e.g. OTA service on top of the network slice obtained from the operator.

The NSaaS offered by the operator can be characterized by certain properties e.g. radio access technology, bandwidth, end-to-end latency, reliability, guaranteed / non-guaranteed QoS, security level, etc.

Figure 36 illustrates some examples of how network slices can be utilised to deliver communication services, including NSaaS.

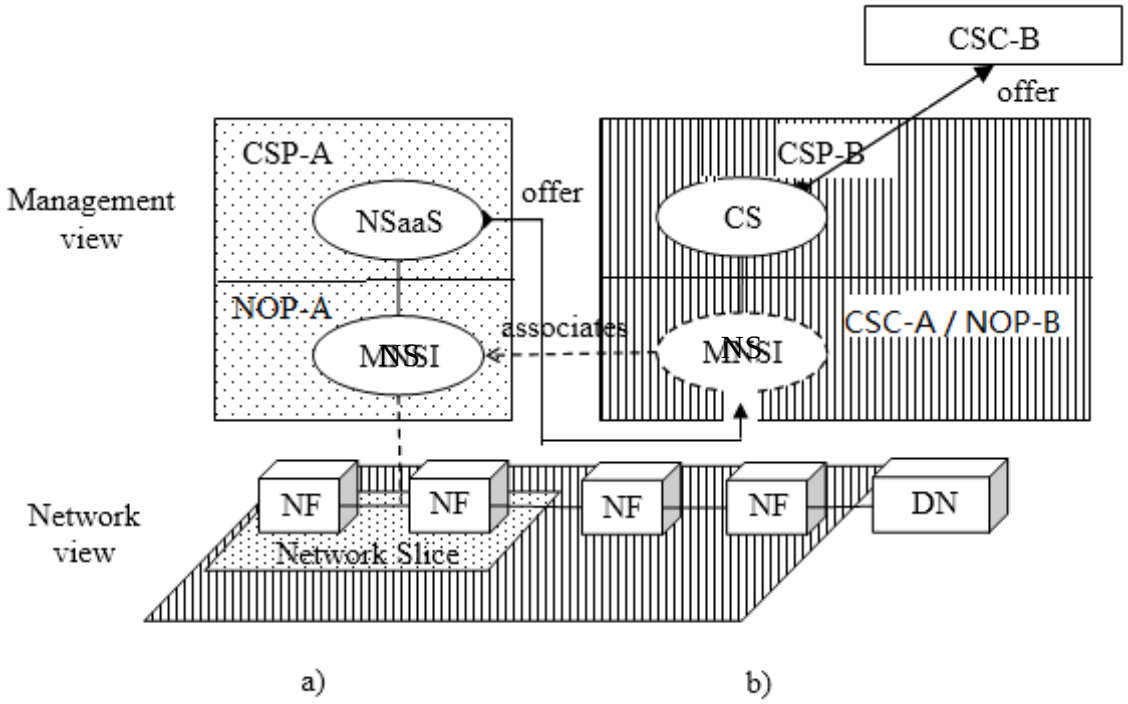

Figure 36 – Examples of Network Slice as a Service (NSaaS), 3GPP TS 28.530 [111]

NSaaS may impact the operator's trust model and operational security. NSaaS may result in reduced operational control and visibility. Operators should evaluate the risks resulting from adopting this mode of operation and establish a clear shared responsibility model for the services being offered in a similar manner to those offered by cloud service providers.

14.2 Standardised Security Features

14.2.1 Configuration of Network Slice availability in a PLMN

A Network Slice may be configured by the operator to be available in the whole PLMN or in one or more Tracking Areas of the PLMN.

The NSSF may be configured with policies specifying conditions that would allow operators to restrict S-NSSAIs per TA and per HPLMN of the UE.

14.2.2 Operator-controlled inclusion of NSSAI in AS Connection Establishment

The Serving PLMN can control per Access Type if a UE includes its NSSAI in the Access Stratum request when establishing a connection caused by Service Request, Periodic Registration Update or Registration procedure.

In addition, the Home and Visited PLMNs can instruct the UE to never include the NSSAI in the Access Stratum i.e. to always enable privacy for the NSSAI.

During the Registration procedure, the AMF may provide a NSSAI Inclusion Mode parameter, indicating whether and when the UE shall include NSSAI information in the Access Stratum Connection Establishment.

14.2.3 Network Slice-Specific Authentication and Authorisation

In general, a UE requires authorisation from a home/serving PLMN in order to gain access to a network slice. An authorised/allowed S-NSSAI is granted to a UE only after the UE has successfully completed primary authentication.

The network operator can define some S-NSSAIs that would require additional Network Slice Specific Authentication and Authorisation (NSSAA). The Network Slice-Specific Authentication and Authorisation allows operators to further control access to a specific slice.

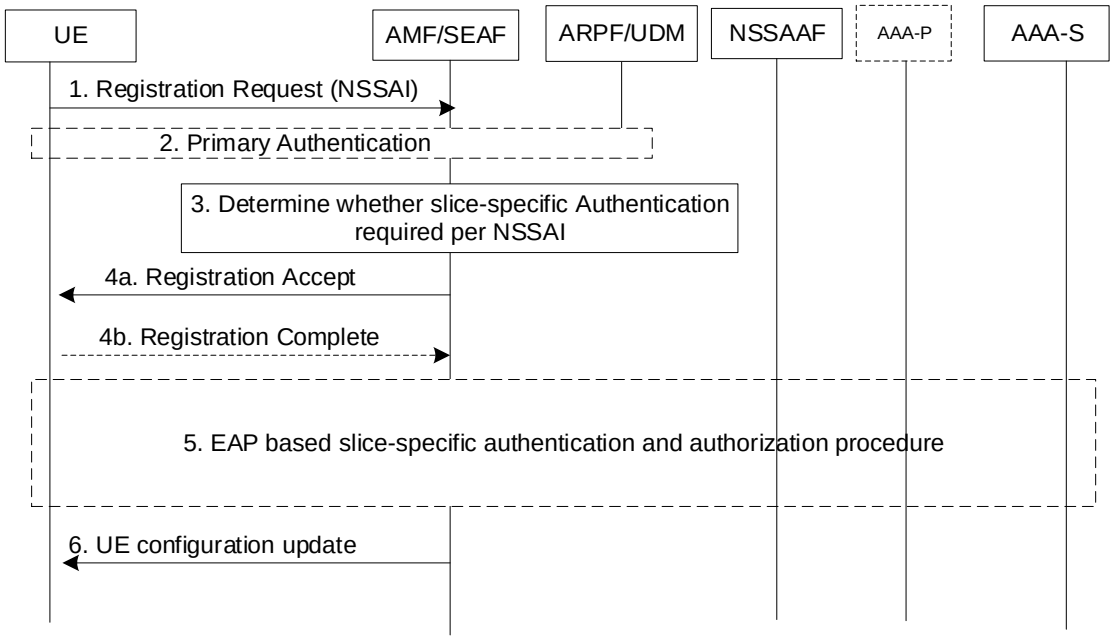

Figure 37 – Relationship between primary authentication and NSSAA TS 33.501 [1]

The AMF invokes an EAP- based Network Slice-Specific authorisation procedure. This procedure can be invoked for a supporting UE by an AMF at any time.

The SEAF/AMF performs the role of the EAP Authenticator and communicates with the AAA-S via the NSSAAF. Multiple EAP methods are possible for NSSAA. A privacy-

protection capable EAP method is recommended, to protect the privacy of the EAP ID. The AAA server can trigger Slice-Specific Re-authentication, Re-authorisation and Revocation procedures as specified in TS 33.501 [1] providing continuous control over UE access to specific authenticated and authorised slices. These can be used to prevent a compromised UE from gaining further access to the slice.

3GPP recommends that at least one of the Subscribed S-NSSAIs marked as default S-NSSAI should not require Slice-specific Authentication and Authorisation, in order to ensure access to services even when Network Slice-specific Authentication and Authorisation fails.

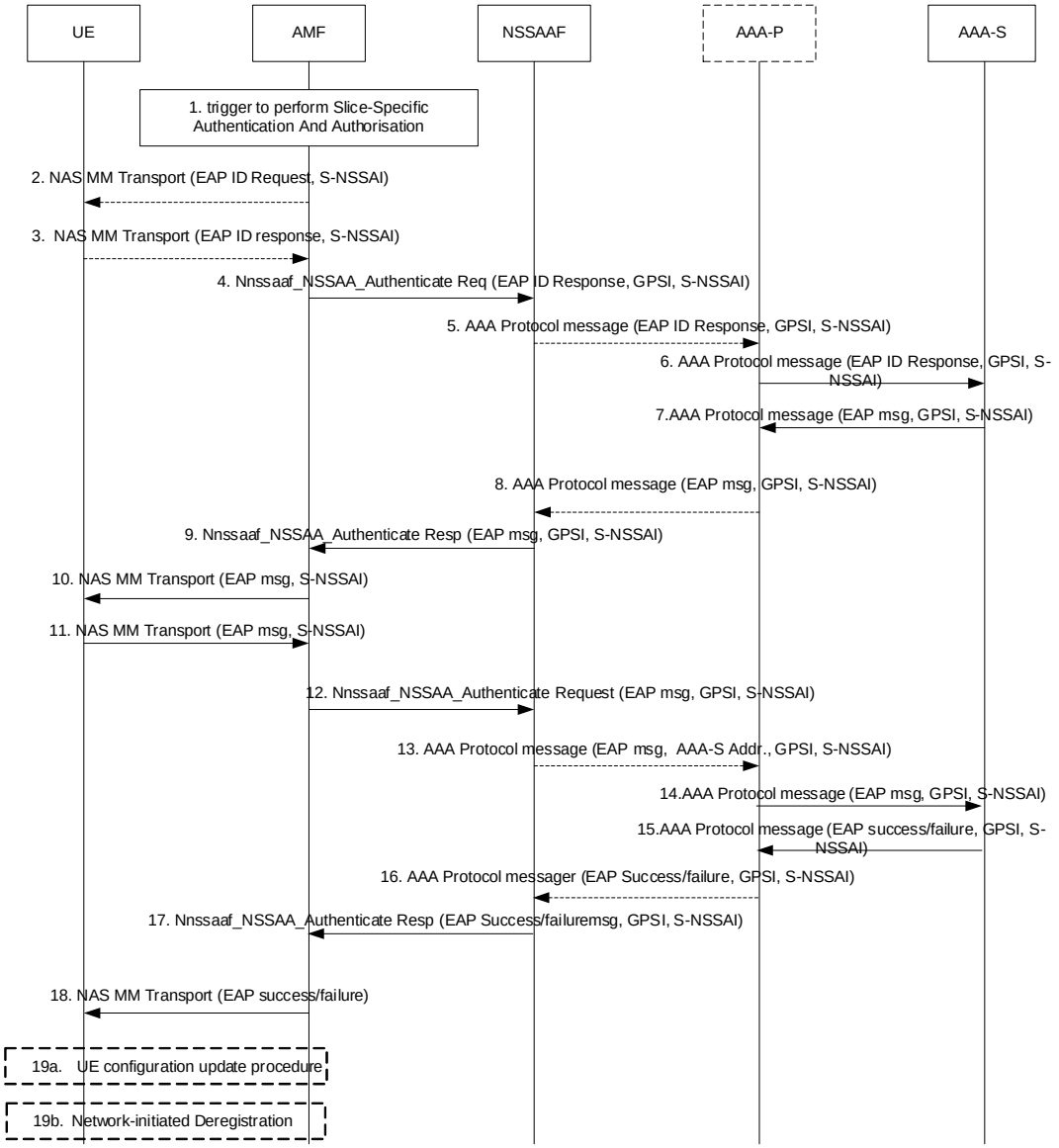

Figure 38 – Network Slice-Specific Authentication and Authorisation procedure TS 23.502 [112]

The UICC can be involved in NSSAA procedure through the SSIM application [132].

14.3 Slice Security Isolation Models

The various isolation types for the control of the independent slices must be integrated in a coherent defence mechanism. The presentation “Security for E2E 5G network slice isolation” [43] provides an overview of the different isolation components that need to be combined to achieve E2E isolation for 5G network slices:

- Isolation in the Radio Access Network (RAN).
- Isolation in the Transmission Network (TN).
- Isolation in the Core Network (CN).

Network slices are logically independent dedicated networks that share a common network infrastructure. To achieve high security and availability, 5G shall support isolation between network slices by using physical and logical isolation methods. Figure 39 elucidates the end-to-end isolation of the network slices in a 5G network.

OBJ

Figure 39 – End-to-end isolation in RAN, TN, and CN of slices in a 5G network

In this context, GSMA has defined security controls for network slicing in GSMA PRD FS.31 [63].

Figure 40 provides a high-level overview of different isolation models, which operators may use to satisfy the different requirements of vertical industries. Dedicated network components may provide stronger isolation assurances at the expense of additional complexity and cost while partly shared network components virtually isolated may satisfy the majority of vertical industry use cases.

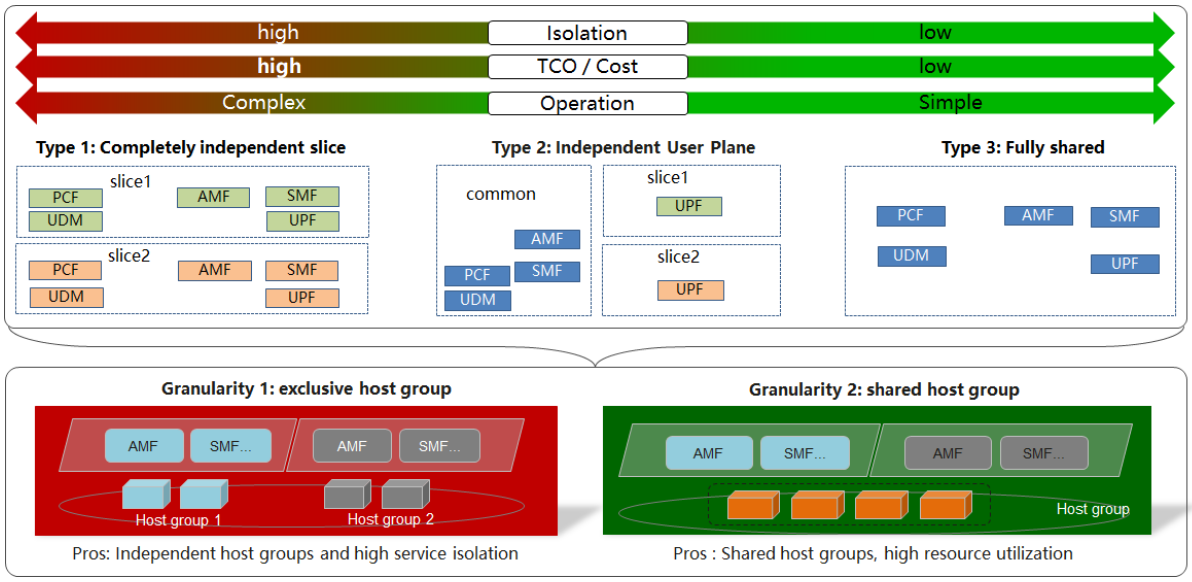

Figure 40 – Slice Security Isolation Models

Figure 41 below depicts possible interactions of various CSP’s with different network slices. As highlighted in Figure 40 (above), a CSP slice may have parts of its network slice subnets with distinct sets of AN, TN or CN NFs or a mixture of shared and dedicated AN, TN and CN

NFs. As mentioned in Section 2.20 of this document, for data in transit, Network Slice must always be re-affirmed to avoid slice hijacking.

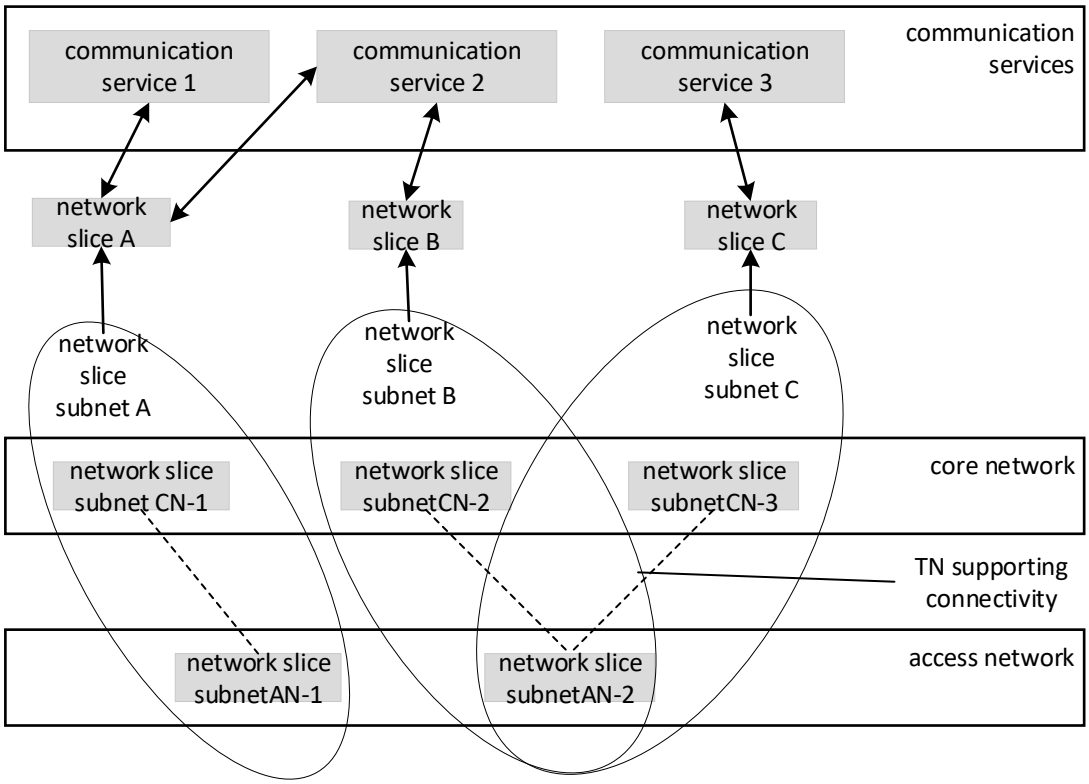

Figure 41 – Communication services provided by multiple network slices, TS 28.530 [111]

14.4 Slice Lifecycle Management

The lifecycle management of network slicing can be described by four phases – Preparation, Commissioning, Operation and Decommissioning, as shown in Figure 42 below.

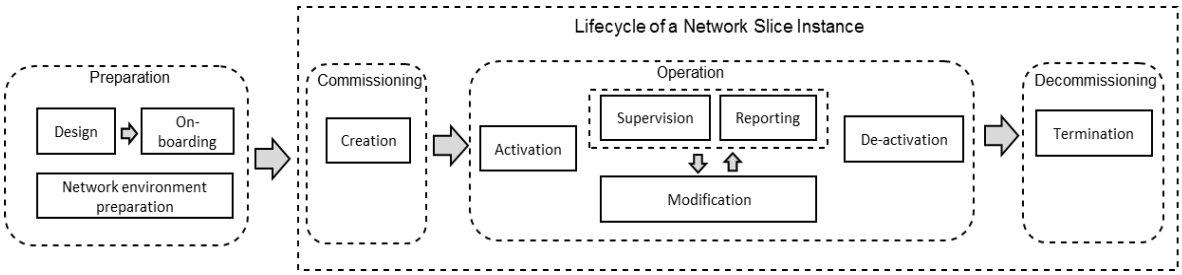

Figure 42 – Management aspects of network slicing, TS 28.530 [111]

A network slice may include non-3GPP parts e.g. data centre network (DCN), transport network, etc. The 3GPP management system has to coordinate with the non-3GPP management system parts (e.g. MANO system) when preparing a network slice, as illustrated in Figure 43below.

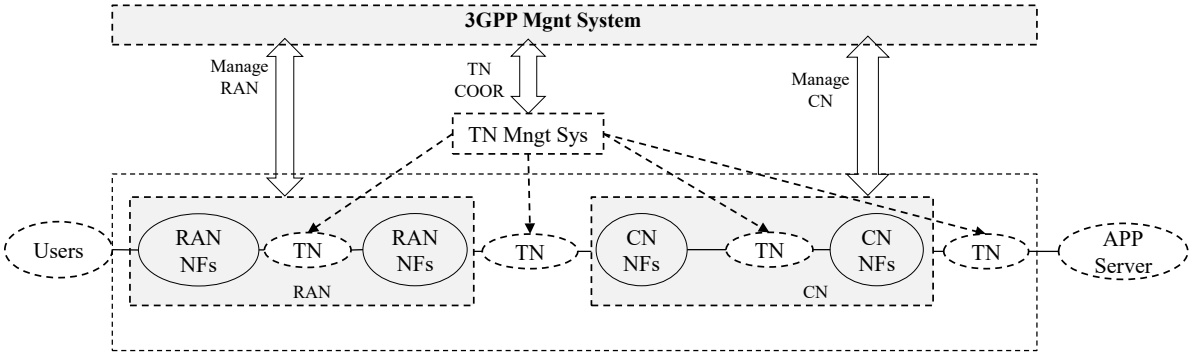

Figure 43 – An example of coordination between 3GPP and Non-3GPP management systems TS 28.530 [111]

14.4.1 Functional Management Architecture

The management services for a mobile network including network slicing may be produced by a set of functional blocks. 3GPP TS 28.530 [111] provides an example of such a deployment scenario with functional blocks such as NSMF, NSSMF, NFMF and CSMF.

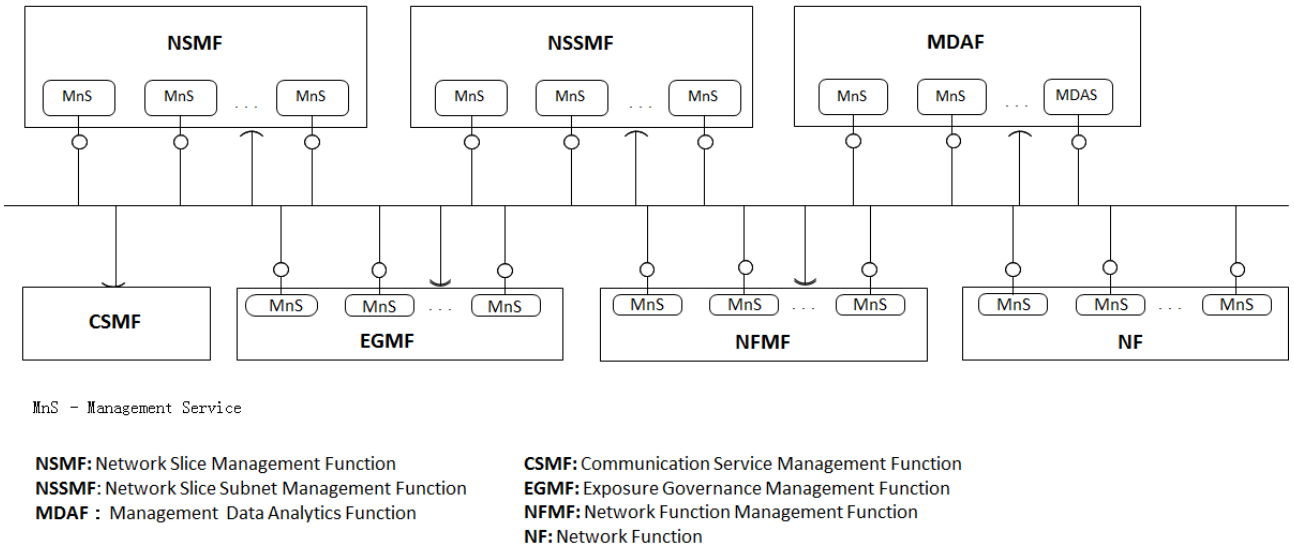

Figure 44 – Example of functional management architecture, TS 28.530 [111]

In this deployment example:

- NSSMF provides the management services for one or more network slice subnets.
- NSMF provides the management services for one or more network slices.
- MDAF provides the Management Data Analytics Service for one or more NF, network slice subnet and/or network slice.

14.4.2 Example deployment scenario for network and network slice

3GPP TS 28.530 [111] provides an example of a possible deployment scenario for mobile network slicing management as shown in Figure 45.

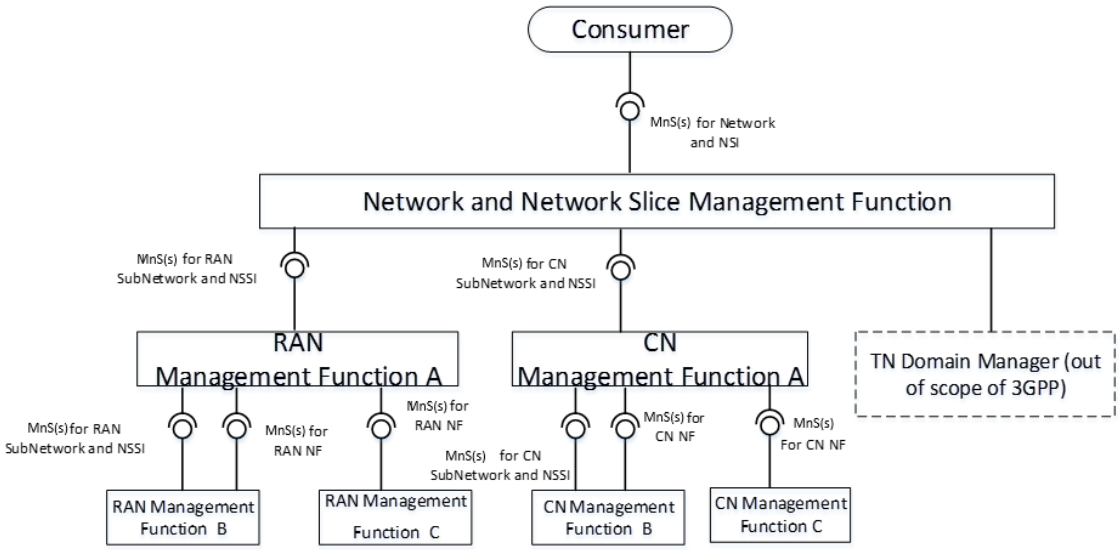

Figure 45 – Example management of a mobile network including network slicing

As each stage of slice lifecycle management may involve multiple 3GPP and non-3GPP functions, operators should conduct detailed risk analysis and deploy adequate security controls through the different network slice lifecycle phases. GSMA has developed content in two of its PRDs FS.30 [113] and FS.31 [63] that can assist operators identify relevant threats and recommended security and privacy controls.

14.4.3 Management security for network slices

The creation, modification, and termination of a NSI is part of the Management Services provided by the 5G management systems. These services are securely protected through mutual authentication and authorisation as described below.

14.4.3.1 Mutual authentication

If a management service consumer resides outside the 3GPP operator's trust domain, mutual authentication of the service consumer and producer using TLS 1.2 or 1.3 based on either client and server certificates or pre-shared keys.

14.4.3.2 Service consumer and service producer management traffic protection

TLS 1.2 or above provides integrity protection, replay protection and confidentiality protection for the interface between the management service producer and the management service consumer residing outside the 3GPP operator's trust domain.

14.4.3.3 Authorisation of management service consumer's requests

After mutual authentication, the management service producer determines, based on either OAuth token authorisation mechanism or local policy, whether the management service consumer is authorised to send requests to the management service producer.

15 Software Defined Network (SDN) Security Monitoring in 5G

15.1 SDN Architecture

SDNs are considered as a key technology to design the core part of a 5G network and are well regarded in terms of network flexibility and programmability. Separation of the data plane from the CP and facilitates the network management through the abstraction of network control functionalities.

SDN will help mobile operators shorten time-to-market for the new services hence introducing a new business model to cater for the service requirements known as Network as a Service (NaaS).

The concept can also be used in the RAN where the SDN controller could control and schedule the radio resources for base stations, thus improving spectrum efficiency as well as mobility management.

There are still many challenges with SDN that need to be addressed including the following:

1. The scalability problem due to the centralisation of network intelligence.
2. Latency sensitivity between devices and the SDN controller.
3. Addressing security challenges for the communication between the control and data planes.
4. Adoption of SDN into mobile networks, such as placement problem of SDN controller, and mobility management.
5. The most important of all is the SDN Security monitoring in 5G Networks.

15.2 OpenFlow tiered SDN Architecture

The SDN architecture is separated into three functional layers with interfaces between the layers. OpenFlow based SDN follows a tiered architecture with OpenFlow applications, OpenFlow controllers and OpenFlow switches, see Figure 46.

- **Application plane:** consists of applications for various network functions such as network management, QoS management and security services, etc.
- **Control plane:** the logically centralised network control platform having a global view of the network resources and stats and provides hardware abstractions to the applications in the application plane.
- **Infrastructure plane:** also called the data plane that consists of the data forwarding elements that act on the instructions of the CP for dealing with the data packets or traffic flows.

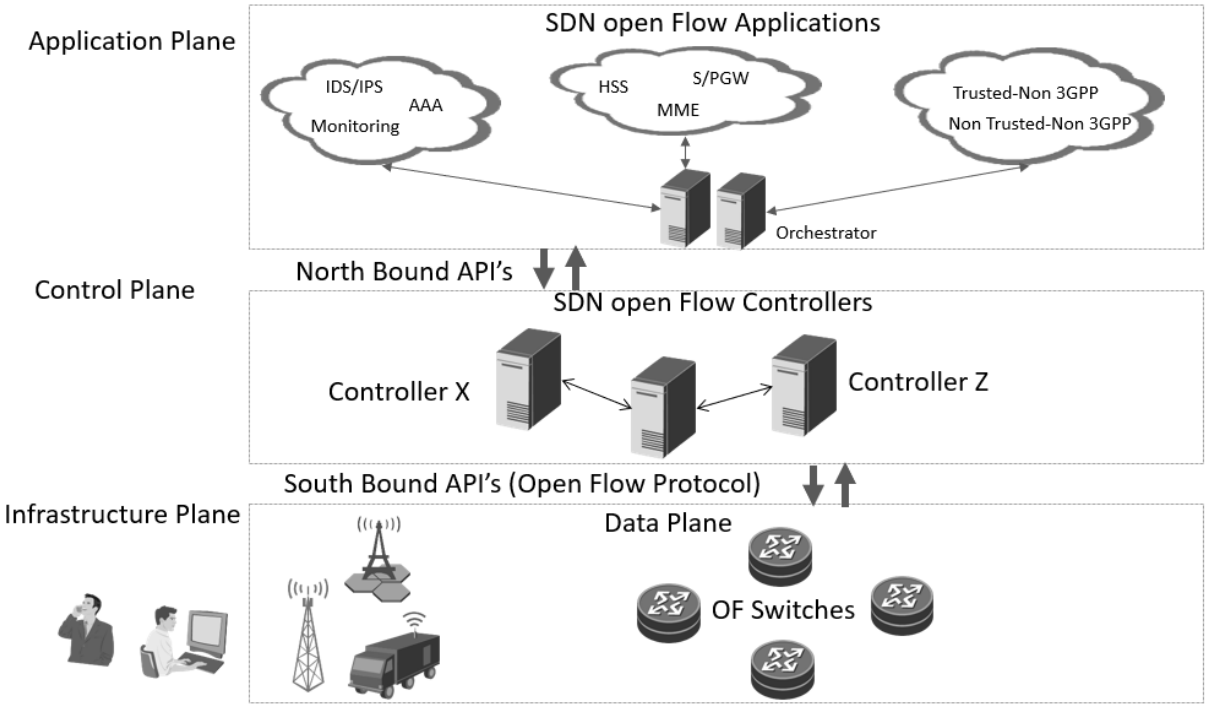

Figure 46 – OpenFlow tiered SDN Architecture

15.3 SDN Security Monitoring for 5G

Security monitoring solutions for 5G networks should offer a capability to monitor and inspect both signalling and data traffic at multiple network points, starting from the UE to RAN and all the way to 5G core network components. The solution should inspect the IPv4 and IPv6 traffic at Level 3 of the OSI Reference Model. Further, the solution should offer Application, which is Layer 7 of the OSI Reference Model, visibility and Layer 7 threat inspection. 5G networks could also leverage SDN control and data plane separation and perform centralised network flow traffic monitoring for a deeper visibility and correlation of traffic traversing inside the network AKA "Flow based network visibility".

The lack of visibility and controls on internal virtual networks coupled with the heterogeneity of used devices make many Security Information and Event Management (SIEM) applications ineffective, if the security elements are not integrated into virtual networks. Existing SIEM solutions were mostly adapted and designed for physical systems and boundaries. Security monitoring systems in 5G networks need to consider integration with legacy networks monitoring systems.

15.4 SDN Security Monitoring Architecture

The Software Defined Monitoring (SDM) architecture is an extension of the OpenFlow type interface, referred to as the SDN/SDM Control Interface and allows the packet and flow data and meta-data needed by the security applications (Monitoring and Security) to be obtained from either the OpenFlow switches or the probes.

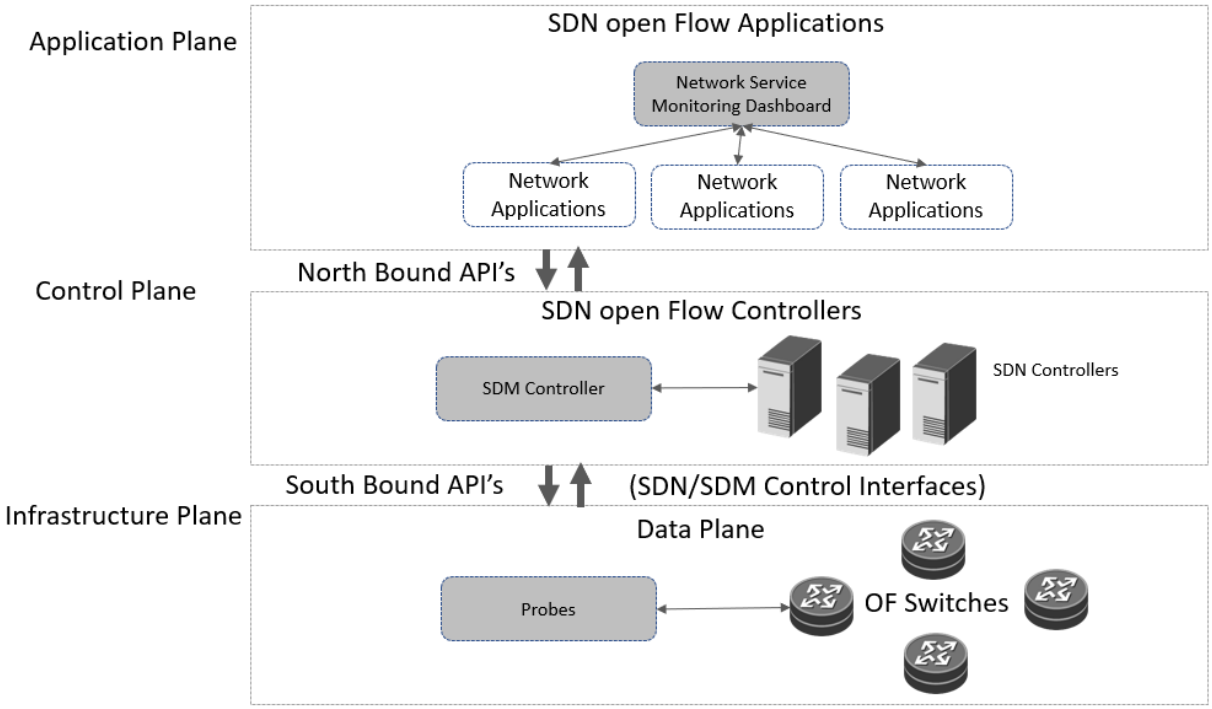

Figure 47 – SDN monitoring architecture for 5G Networks

A control layer based on SDN/SDM is inserted between the application and network infrastructure layers. At the network infrastructure layer, an SDN protocol, such as OpenFlow, is used as an interface.

SDN controller directs the network traffic to be analysed to the monitoring and Security function. Such deployed rules on the security application will allow the identification of anomalous traffic flows and the performance properties of the connection to provide "flow-based visibility".

See section 15.4.1, section 15.4.2 and Figure 48 for the added Modules and Interfaces of the SDM architecture.

15.4.1 Modules

- **Security Sensor:** an active monitoring probe for the detection of security and behaviour related information (e.g. security properties and attacks) and mitigation (e.g. filtering). It can be installed on the Network Elements on the application layer or in network taps (passive network observation points) on the network infrastructure layer.
- **SDM controller:** a new module or extension of SDN controller to allow the control of the monitoring function (i.e. management of network monitoring appliances, traffic mirroring, traffic load balancing and aggregation) and accept requests from network functions and applications.
- **Monitoring and analysis Application:** A monitoring function (i.e. part of the traffic analysis)
- **Traffic Mirroring:** a passive traffic monitoring device utilised by different network functions.

15.4.2 Interfaces

- **SDN/SDM Control Interface:** an interface that facilitates control the use of the monitoring resources or metadata for analysis. It allows monitoring requests to be performed and the status of the network links to be obtained. In this way, applications and network functions can send requests.

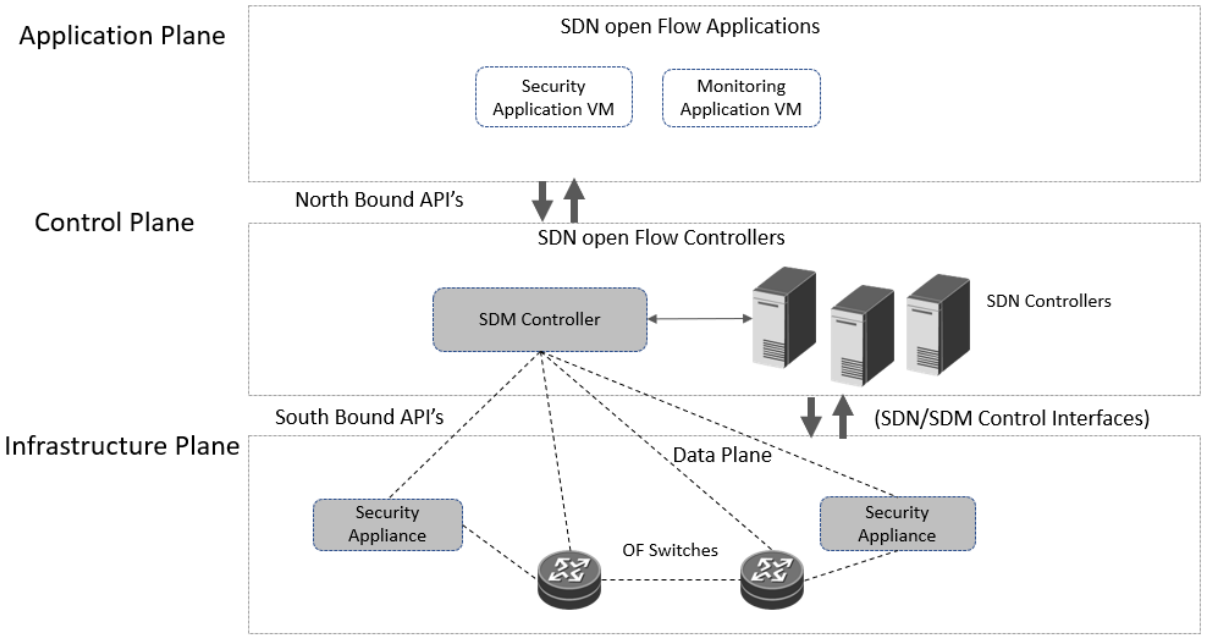

Figure 48 – SDM Controller components and Interfaces

16 O-RAN Security

16.1 Overview

O-RAN is a paradigm shift in RAN architecture and deployment leveraging SDN and NFV, virtualisation and containerization by disaggregating traditional RAN functions to create a more open and interoperable network environment. It is implemented in software, deployed on independent cloud infrastructures, and connected via standardised interfaces. It is important to understand some terms that has been used in literature and specification:

- Open RAN: An industry term for open radio access network architecture. It is a RAN that includes open interoperable interfaces and virtualization and is big data and AI-enabled.
- O-RAN: Refers to the O-RAN Alliance developed standards based on 3GPP RAN specifications. O-RAN is also used to describe a network that complies with O-RAN Alliance Standards. O-RAN Standards define architecture for disaggregated deployments for virtual and physical network functions as well as introduced new APIs, Interfaces and processes for full lifecycle management of the RAN.
- OpenRAN: Refers to initiatives driven by Telephony Infrastructure Project's (TIP) OpenRAN project group.
- vRAN: 5G becoming software-defined and programmable, generating additional RAN architecture flexibility, platform harmonization and simplification.

- Cloud RAN: Cloud RAN is a virtualized RAN that is designed to be cloud native, built on future proof architectures and incorporating key elements such as microservices, CI/CD and containerization.

This section describes some concepts based on O-RAN highlighting cloudification, virtualization and open interfaces where applicable. The O-RAN logical architecture is shown in Figure 49.

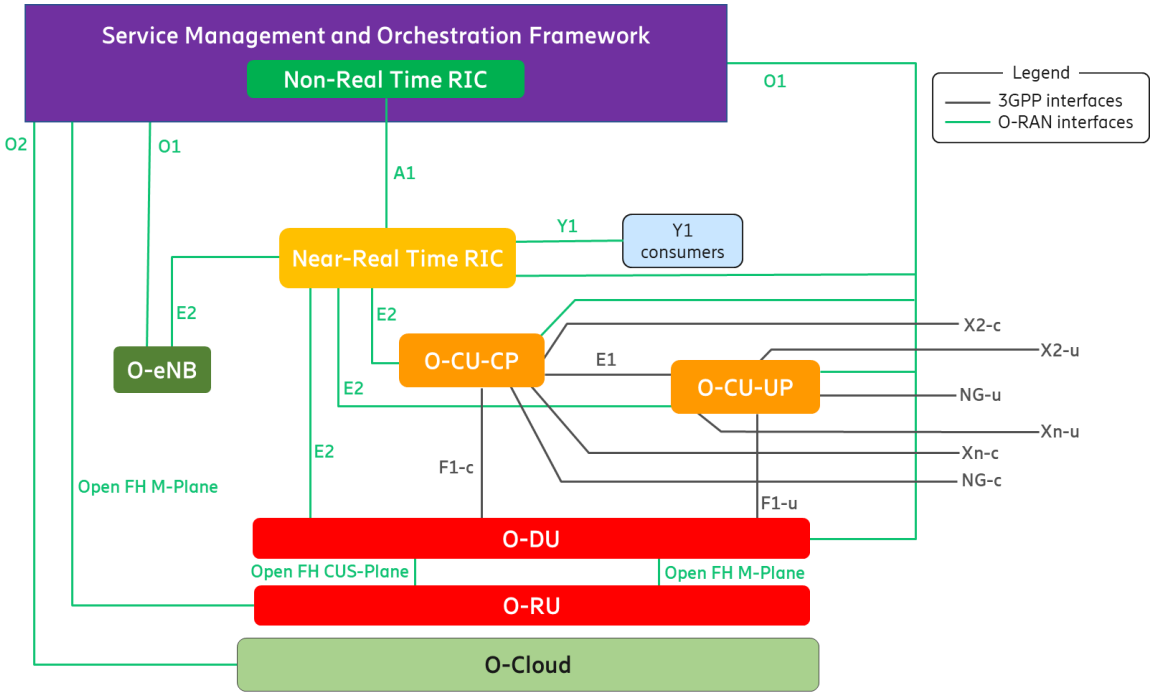

Figure 49 – O-RAN Logical Architecture

16.2 Security Challenges

O-RAN faces similar security challenges as other virtualised and open architectures, as follows:

- Disaggregation of functions increases the RAN threat surface by inheriting threats present in underlying infrastructure and network (Network DOS, NF DOS, MiTM, Network Sniffing).
- New challenges arise pertaining to monitoring and troubleshooting security issues in a disaggregated multi-vendor, multi-domain (physical, virtual, multi-cloud) RAN architecture.
- The strict latency requirements (network hops, network and processing delays) on RAN need to be considered when implementing security controls, such as encryption, on the Open Fronthaul Interface.
- ORAN encourages open-source capabilities, since increased reliance on open-source software increases the O-RAN dependence on secure development practices within open-source communities.
- Use of AI in the RAN may lead to unanticipated consequences as it has in other domains (e.g. racially biased facial recognition).

- The dramatic growth in the number of resource constrained IoT devices requires all RAN deployments to protect against the increasing likelihood of attacks by compromised devices.

O-RAN Alliance's Work Groups publish architecture, threat analysis, and mitigation in many specification documents available at the alliance website. [127]

16.3 O-RAN Security Features

O-RAN key security features are:

- **Enhanced supply chain security**: By diversifying the supply chain through a multi-vendor approach, O-RAN reduces reliance on single suppliers, thereby reducing the risk of relying on a single vendor. It might result in somewhat enhanced security and resilience of the network infrastructure.
- **ZTA approach in O-RAN**: O-RAN embraces some concepts of Zero Trust methodology (discussed in section 8.9.1), implementing stringent access controls and network segmentation based on the principle of least privilege. This approach ensures that access to network resources and functions is strictly limited to entities that are explicitly authorised, effectively adopting a "never trust, always verify" stance. Alongside secure authentication protocols and ensuring that access to network resources is granted only to authenticated and authorised devices, users, and services, O-RAN employs secure communication channels. These channels are encrypted and continuously monitored to prevent interception or tampering, ensuring the integrity and confidentiality of data as it traverses the network. Further, adhering to the ZTA approach, security elements may be added to some interfaces within O-RAN architecture, assuring legitimacy of the protocols deployed.
- **AI/ML-enhanced security and resilience in O-RAN**: Leveraging advanced AI and ML algorithms, O-RAN systems, with Radio Intelligent Controller (RIC) and added security elements, can continuously monitor network patterns to identify and respond to anomalies, threats, and vulnerabilities in real-time. This capability can significantly enhance the network's security posture. Concurrently, AI/ML enables the development of self-healing networks in O-RAN, allowing for the automatic detection and rectification of network failures or performance issues. This dual approach can ensure not only a proactive stance against security threats, but can also minimize downtime and improve overall network reliability and performance.

16.4 O-RAN Security Specifications

The Security Working Group (WG11) of the O-RAN Alliance is dedicated to advancing the security of the RAN ecosystem through a risk-based specification process. This approach is grounded in the principles of Zero Trust Architecture (ZTA), ensuring a comprehensive assessment of both internal and external threats.

O-RAN security is evolving to adopt modern security best practices. Table 2 provides a view of the existing security controls and their corresponding protocols for the different O-RAN interfaces as specified by O-RAN Alliance:

Security Control	A1	O1	O2	Y1	E2	Open Fronthaul			
						C-plane	U-plane	S-plane	M-plane
Authenticity	mTLS	mTLS	mTLS	mTLS	IPsec	IEEE 802.1X	IEEE 802.1X	IEEE 802.1X	mTLS/SSH/ IEEE 802.1X
Confidentiality	TLS	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH
Integrity	TLS	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH
Authorisation	OAuth	NACM	OAuth	OAuth		IEEE 802.1X	IEEE 802.1X	IEEE 802.1X	NACM/ IEEE 802.1X
Replay Prevention	TLS	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH

Table 2 - O-RAN interface security controls

Authorisation for the E2 interface is being developed in collaboration with the Near-Real Time RIC and E2 interface work group. Confidentiality and integrity protection on the Open Fronthaul C-Plane and authenticity protection on the Open Fronthaul S-Plane are being developed in collaboration with the Open Fronthaul and Transport working groups. PDCP requirements are specified by 3GPP in TS 33.501.

The following is a focused overview of the O-RAN Requirements and Controls Specification which presents an analysis of the various components within the O-RAN architecture, each accompanied by its specific set of requirements and controls.

For SMO, the specification emphasizes stringent authentication and authorisation measures for both internal SMO functions and external systems, ensuring secure communications and operations. Specific requirements include resilience against volumetric Distributed Denial of Service (DDoS) attacks, secure handling of internal and external communications with confidentiality, integrity, replay protection, and mutual authentication. The security of event logs is also addressed, with specifications for secure forwarding, storage, access, and integrity. Additionally, the requirements extend to the Network Function Orchestrator (NFO) and Function Orchestrator Component Manager (FOCOM), mandating secure user access and communications, as well as resource limits and auto-scaling thresholds for microservices. Security controls include the support for OAuth 2.0, mutual authentication using mTLS with Public Key Infrastructure (PKI) X.509v3 certificates, and TLS protocol for data protection in various SMO communications and interfaces.

For Non-RT RIC and rApps, the specification stipulates robust authorisation mechanisms to ensure secure interactions as both resource owners/servers and clients. They must be capable of withstanding volumetric DDoS attacks across specified interfaces, underlining the importance of resilience against cyber threats. A crucial aspect of these security measures is the requirement for uniquely generated rAppIDs using strong randomization methods. The

Non-RT RIC and SMO/Non-RT RIC Framework are tasked with the authentication and authorisation of API Producers and Consumers, especially when using Kafka based protocols for data streaming. The adoption of TLS for secure communications further fortifies the framework. The document mandates the support of OAuth 2.0 for various interfaces, aligning with the O-RAN Security Protocols to ensure standardized security practices.

The requirements for Near-RT RIC and xApps include adhering to specific security requirements such as unique and authenticated xApp identifiers. The Near-RT RIC is accountable for authenticating xApp access to its databases and providing authorised access. It is also required to support mutual authentication in communications with xApps and establish a robust authorisation framework that considers operator policies. The Near-RT RIC must exhibit resilience against volumetric DDoS attacks and be capable of defending against content-related attacks, including injection and buffer overflow attacks, across various interfaces. For API security, mutual TLS authentication, OAuth 2.0 authorisation, and IPsec are mandatory for different types of APIs. These security controls also encompass message confidentiality and integrity. The Near-RT RIC, in its roles defined in OAuth 2.0, must validate and log policies and data received through various interfaces, ensuring they adhere to predefined criteria. In the xApp registration security procedure, xApps acquire credentials from a provisioning system, establish secure TLS communication with the Near-RT RIC, and are assigned unique xApp IDs. These IDs, embedded in x.509 certificates, are crucial for authentication and authorisation in API requests. The xApp ID, defined as a UUID, ensures unique identification. The Near-RT RIC is responsible for verifying and logging any inconsistencies or failures in data validation received through its interfaces, thus enhancing the overall security of the system.

For both O-CU-CP (Control Plane) and O-CU-UP (User Plane), compliance with the security requirements specified for gNB-CU-CP and gNB-CU-UP in TS 33.501 is mandatory. This compliance includes supporting the same security controls for these elements as detailed in the specification.

Similarly, the O-RAN Distributed Unit (O-DU) must conform to the security requirements and controls set for the gNB-DU, as per TS 33.501.

The O-RAN Radio Unit (O-RU) must adhere to established security standards for gNB setup, configuration, and environment as per TS 33.501, and follow detailed security controls for the Open Fronthaul Interface as outlined in Table 5.

The Shared O-RU is mandated to support mutual authentication with an O-RU Controller, provide least privilege access based on the sro-id of each Secondary Radio Operator (SRO), and ensure data protection, both at rest and in transit, for the Host MNO and each SRO. It is also required to support Multi-Factor Authentication (MFA) for human user logins, implement access controls for human users, be resilient against volumetric DDoS attacks, and support event logging with tenant awareness. Security controls for the Shared O-RU include supporting mTLS 1.2 or higher for mutual authentication with an O-RU Controller, not using password-based authentication with an O-RU Controller, supporting Network Access Control Models (NACM) for access control to an SRO, and supporting TLS 1.2 or higher for data protection in transit.

The O-Cloud encompasses a wide range of security aspects, from user access management and software integrity to data protection and hardware security. User management involves authentication and authorisation of users, implementation of isolation mechanisms, and recommendation of Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA). Software package protection entails authenticating and verifying application packages, ensuring integrity, and supporting code signing and encryption/decryption processes. Virtualization and isolation requirements include preventing privilege escalation by applications, authenticated and authorised communication between applications, and strict data isolation. Secure updates, secure storage of cryptographic keys and sensitive data, a chain of trust, and security requirements for Acceleration Abstraction Layer (AAL) components are also part of the O-Cloud specifications. Additionally, mutual authentication, authorisation, and secure connections for O2dms/O2ims/O-Cloud Notification APIs are mandated. Physical access restrictions for O-Cloud hardware and unique, protected, and audited O-Cloud instance IDs are also required. Time synchronization and consistency across the O-Cloud infrastructure are essential for ensuring uniform time references.

The document also provides guidelines for the generation, delivery, and usage of a Software Bill of Materials (SBOM) in the context of O-RAN software development. An SBOM is crucial for secure software development, aiding in the understanding of the software supply chain and effective vulnerability management. It includes both proprietary and third-party software, commercial or open-source. Key requirements for O-RAN SBOMs include providing an SBOM with every software delivery package, specifying minimum data fields, excluding vulnerabilities to avoid a static view, defining SBOM depth, protecting the SBOM for authenticity and integrity, controlling access and maintaining confidentiality, and providing the SBOM in recognized formats like SPDX, CycloneDX, or SWID. Security controls for SBOMs include using a hash for SBOM integrity and providing a digital signature for SBOM authenticity.

The document outlines various transversal requirements for O-RAN components, focusing on areas such as application lifecycle management, software package protection, secure update processes, and security in API usage. These include certified and signed application packages, secure update requirements against downgrade attacks and vulnerabilities, security descriptors for group rules and SAL requirements, guidelines for securely sanitizing unwanted application data, generating comprehensive post-decommission reports, documenting supported network protocols and services, ensuring robustness of common transport protocols and resilience against volumetric DDoS attacks, identifying known vulnerabilities in OS and applications, adhering to best practices for password-based authentication, and outlining requirements for generating, transmitting, storing, and analysing security log data. Additionally, the document specifies support for the CMPv2 protocol for certificate management, details security requirements and controls for securing APIs and provides guidelines for Trust Anchor provisioning.

The O-RAN security specifications are found in [127], under WG11.

17 Security of Open-Source Software

17.1 Overview

A large portion of the software capabilities being produced use open-source software components. There are many 5G network components already using open-source components in vendor supplied solutions [157].

Open-source software is about the accessibility and freedom to modify the source code of the software, while open interfaces are about the ability for different software systems to interact and communicate with each other. As an example, O-RAN Alliance specified open interfaces for O-RAN compliant RAN, whereas an open-source community – ORAN-SC-- convened to build O-RAN based RAN NFs.

Generally, open-source software refers to a type of software whose source code is released under a license that allows anyone to view, modify, and distribute the software for any purpose. This means that anyone can contribute to the development and improvement of the software. Examples of open-source software include Linux, Kubernetes, Mozilla Firefox, and WordPress. Open interfaces, also known as open APIs (Application Programming Interfaces), are sets of rules and protocols that specify how software components should interact. They allow different software applications to communicate with each other. An open interface is publicly available for other developers to use and integrate into their own software applications. They do not necessarily provide access to the source code of the software, but rather provide a method for different software systems to interact. Examples of open API/Interfaces are O-RAN interfaces A1, O1, O2, E2 etc. A GSMA whitepaper [99] explains the differences between open interfaces and open source. Open-source software packages and Vendor provided licensed applications may use open-source software libraries, an example is java-based applications using log4J open-source library.

The Enterprise (or software vendor) that uses open-source software in its solutions is responsible for maintenance and updates of the software libraries and patching vulnerabilities. This may pose a challenge when the software being used in production environment does not contain the latest open-source libraries with vulnerability patches. An organization must have a holistic approach to their enterprise security that incorporates threat informed defences and continuous assessment.

17.2 Deployment scenarios

A variety of deployment scenarios is explored within virtualised mobile networks that include various types of open-source software - from new proprietary code developments in commercially supported software packages that include significant portions of open-source code on open-source community-supported software packages, such as:

- VNF on top of Cloud /NFVI.
- Component within a disaggregated solution.
- Component of Software as a Service (SaaS), e.g. as part of an O-RAN solution.
- Middleware abstraction between the Commercial Off The Shelf (COTS) compute layer and applications layer sitting on the top.
- Part of a vendor executable code with the executable code difficult to inspect.

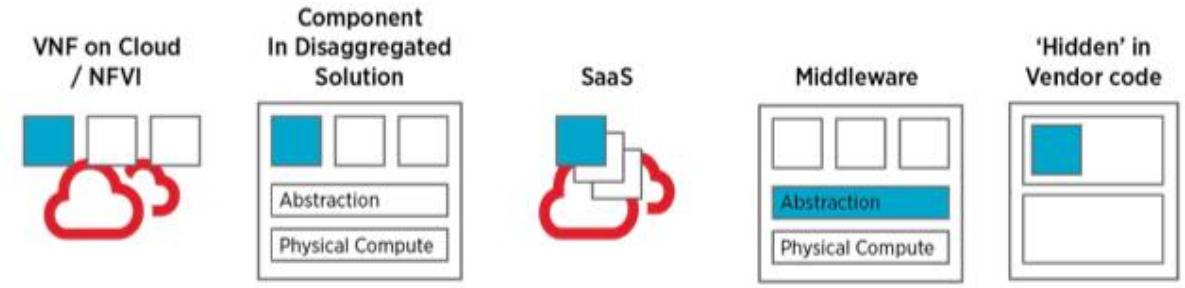

Figure 50 - Open-Source Software (OSS) deployment arrangements

17.3 Guidelines for Security

The following guidelines are provided herein for a secure deployment of OSS solutions:

- Incorporate the use of a SBOM to ensure full visibility of the deployed open-source software code in use.
- Incorporate software identification: Code hashing and applying digital signature as a well-used method to uniquely identify code, packages and their release versions. Signature verification verifies that a software package is a genuine artifact.
- Encourage vendors to promptly update or patch open-source components integrated within their software code or included in a full stack supply. This can be achieved by either facilitating swift upstream updates or empowering operators to take direct action.
- Use asset and inventory management - by tracking all open-source assets in organizational use. Maintaining an analysed and tested software library within an organization can improve the security of the production environment. Maintaining visibility of all software in repositories and run time environment helps with this goal.
- Leverage the advantages of open-source transparency by conducting code inspection, engaging in Source Code Analysis (especially for generating and validating an SBOM), employing dynamic application security testing, promoting adherence to coding standards in both vendor Software Development Life Cycles and Enterprise Infrastructure Lifecycles (example-Linux Foundation projects sign their code and many started to provide SBOMs).
- Where infrastructure virtualisation is provided through open-source-code-derived software packages, employ scanning tools to detect obsolete, end-of-life and vulnerable products. Advocate for supply arrangements that enforce the capability to update outdated components within a stack within a reasonable timeframe.
- Ensure that all open-source components can be supported by the community, industry groups and/or the supplier for all OSS components included in all products.
- Ensure supplier management best practices are used. This is a means to assess the health and performance of the OSS community, including their secure software development practices (Example OpenSSF Badging, CNCF certification for CNFs)
- For infrastructure virtualisation, consider proving and re-using deployments with established industry benchmarks and common security-proven builds that have been extensively defined, tested and maintained. The CNTT has undertaken work in this area.
- Incorporate proven security methods that deliver ‘Bottom to top’ security to preserve the root of trust for the solution as a whole. Current equipment is often supplied from

a single vendor, but open networking is changing this and may mean there are different vendors involved in each layer.

- Follow the O-RAN Alliance Security Working Group defined security requirements when evaluating and building RAN solutions.
- Account for the overall operating environment in which open-source code is deployed, ensuring holistic security considerations are applied across both new and existing infrastructures.
- When developing a software or solution, utilise a lifecycle approach, such that security is baked in the architecture, design, and deployment processes, comprehensively tested, securely deployed and validated, and operated to maintain and optimise this security; there is a vibrant community providing guidance and tools on DevSecOps.
- Most open-source software communities have a bug reporting process; participate in bug reporting to ensure vulnerabilities are caught, evaluated, and patched sooner for the entire ecosystem.

18 Security Assurance for 5G

18.1 Network Equipment Security Assurance Scheme (NESAS)

GSMA's NESAS [16], is an important development that provides an assurance scheme which covers assessment of the vendor development and product lifecycle processes, test laboratory accreditation, and security evaluation of network equipment products. Both approaches – assessment and evaluation by testing – significantly help the MNO to determine the achieved level of security of a network product.

NESAS provides "out of the box" security assurance to MNOs and vendors, ensuring a common baseline security level for the industry. In addition, NESAS can help vendors avert fragmented regulatory and MNO customer requirements and give their networks a robust security baseline. The security provided by NESAS can then be enhanced according to the regional risk requirements and operator specific security needs e.g. due to high-risk customer base, sensitive verticals or regulator requests.

Figure 51 illustrates the collaborative roles of 3GPP and GSMA within the scheme.

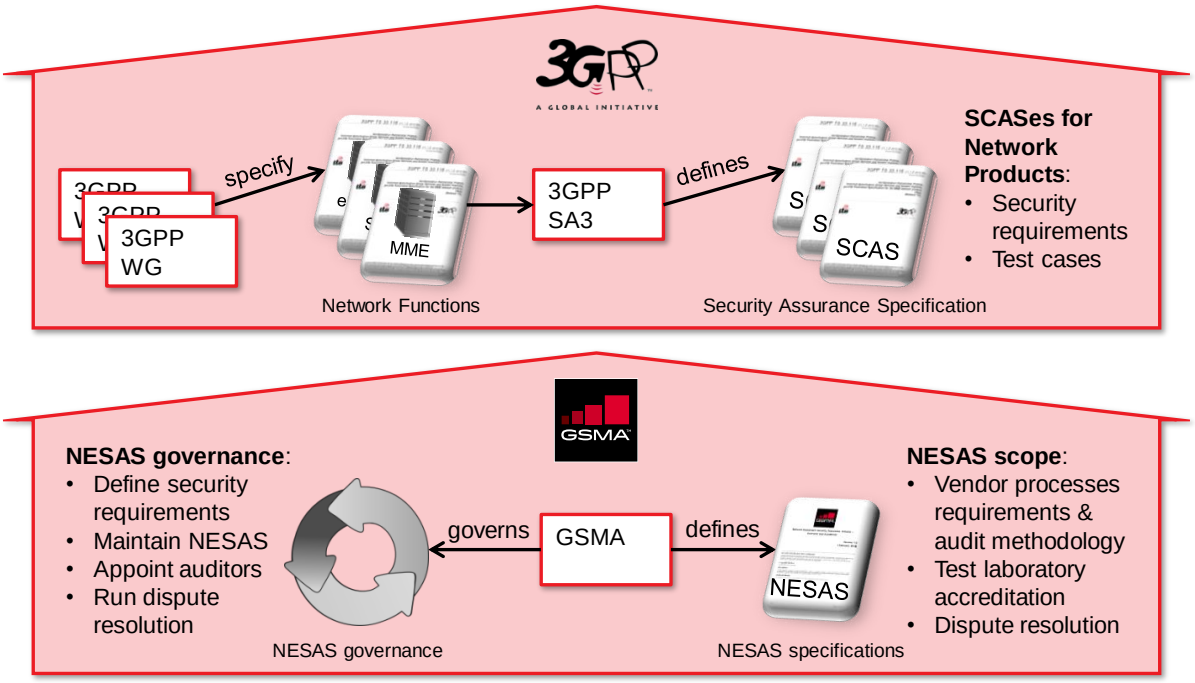

Figure 51 – Roles of 3GPP and GSMA in NESAS

The focus of NESAS is on equipment assurance. Although GSMA and 3GPP work on security assurance in the wider sense, NESAS, does not address the following aspects:

- Risk from legacy interworking, third party interworking or external systems (e.g. fixed networks)
- Security deployments (e.g. configuration, monitoring of traffic)
- Operational security (e.g. threat analysis and threat intelligence feeds, penetration testing of network, fraud protection)
- Cloud security aspects (e.g. virtualisation and hosting security)
- Operator organisational aspects (e.g. ISO 27 related aspects)

For many of these topics GSMA has created specifications and guidelines but they are not part of the assurance program and need to be tailored to the individual operator ecosystem and architecture.

18.2 Security Assurance Specifications (SCAS)

3GPP produces the Security Assurance Specifications (SCASs) that define the security requirements for each network product class. 3GPP TS 33.117 [82] provides a catalogue of general security assurance requirements with objectives, requirements and test cases that apply to several network product classes as many share very similar, if not identical, security requirements that are catalogued in this generic SCAS.

In addition to the generic SCAS, requirements specific to different network product classes are captured in separate documents and the following link provides a reference to the list of 3GPP specifications for the respective 5G network functions (AMF, UPF, UDM, SMF, AUSF, SEPP, etc.) : https://www.gsma.com/security/nesas-security-assurance-specifications/

18.3 Security Assurance Considerations for the Software Supply Chain

As a supplement of GSMA NESAS and 3GPP SCASs, supply chain integrity and risk management will extend to vendors' E2E supply chain management activities with security, availability, processing integrity, confidentiality and privacy protection key considerations. Also essential will be compliance with industry standards and best practises e.g. ISO 28000, BSIMM. The 5G Americas white paper [84] refers to GSMA's NESAS as a framework for the delivery of compliance reports. Incorporating NESAS auditing by the OEMs via an independent, reputable, 3rd party auditor could ensure that the OEMs follow best practices for secure software development to secure the end-to-end supply chain.

19 Regulatory Aspects and Industry Papers

19.1 Overview

A number of governments and agencies across the globe have focussed attention on the need for enhanced security levels for 5G networks and related technologies due to the critical nature of some services that will be delivered by 5G. A range of initiatives and publications have emerged in several countries and regions, some of which may influence the evolution of 5G security features and requirements. Although the primary purpose of this document is to provide technical information, it was considered useful by GSMA's 5G Security Task Force to include an overview of some of the policy related initiatives to provide a flavour of how government and national authorities are thinking about 5G security. A selection of regulations and publications, and excerpts from them, are presented below and, although subjective and not exhaustive, they are intended to inform the reader about some of the publicly announced 5G security policy initiatives.

19.2 National and Regional Regulations

19.2.1 EU Level Regulations and Position Papers on 5G

19.2.1.1 ENISA's view on 5G Security

The following main findings on 5G security are contained in the ENISA report "Signalling Security in Telecom SS7/Diameter/5G – EU level assessment of the current situation" and many of which have implemented since the roll out of the report [11].

19.2.1.2 Considerations on 5G security

IPX security aspects, such as IPX service provider usage and hop-by-hop routing and security, might become part of later 3GPP releases. Concern was expressed that 5G signalling will incorporate the same vulnerabilities as Diameter (used in 4G) and the need for a new signalling architecture was noted.

5G will inevitably increase the attack surface resulting in an evolved threat landscape and new technologies, such as NFV, are expected to bring new security concerns.

SIP signalling has some known vulnerabilities that are potentially easier to exploit than SS7 and Diameter.

5G will see a break out from Diameter to use HTTP/2 as a base applicative layer and that will increase the number of interconnects, something attackers may use to their advantage to slow down attack detection. Each interconnection must be properly monitored.

5G uses common “Internet” protocols like HTTP, TLS, and Representational State Transfer (REST) API for which known vulnerabilities exist and these are often more quickly discovered and exploited than was the case with older protocols.

19.2.1.3 Technical recommendations

The initial design of interconnect protocols has made security hard to implement but an end-to-end security solution, providing both confidentiality and integrity is desirable.

GSMA is studying ways to implement end-to-end interconnect security for LTE and 5G networks and to address operator concerns about interconnect security and the need to eliminate legacy vulnerabilities. Simply upgrading network infrastructure is not a solution to the problem.

19.2.1.4 ENISA implementation guide European Electronic Communications Code EECC and 5G Supplement

The European Electronic Communications Code (EECC) is an EU Directive that regulates electronic communications networks and services in EU member states. EECC was adopted in December 2018 and consolidated and reformed the existing regulation framework.

In its report “Guideline on Security Measures under the EECC” [88], ENISA provides guidance (“the framework”) to EU national authorities on the technical details of implementing Articles 40 and 41 of the EECC.

This is accompanied by the “5G Supplement to the Guideline on Security Measures under the EECC” [94] that contains a 5G technology profile which supplements the technology-neutral Guideline on Security Measures under the EECC.

The following diagram shows the relationship between both guidelines and their relationship to the EECC and the EU Toolbox on 5G Security.

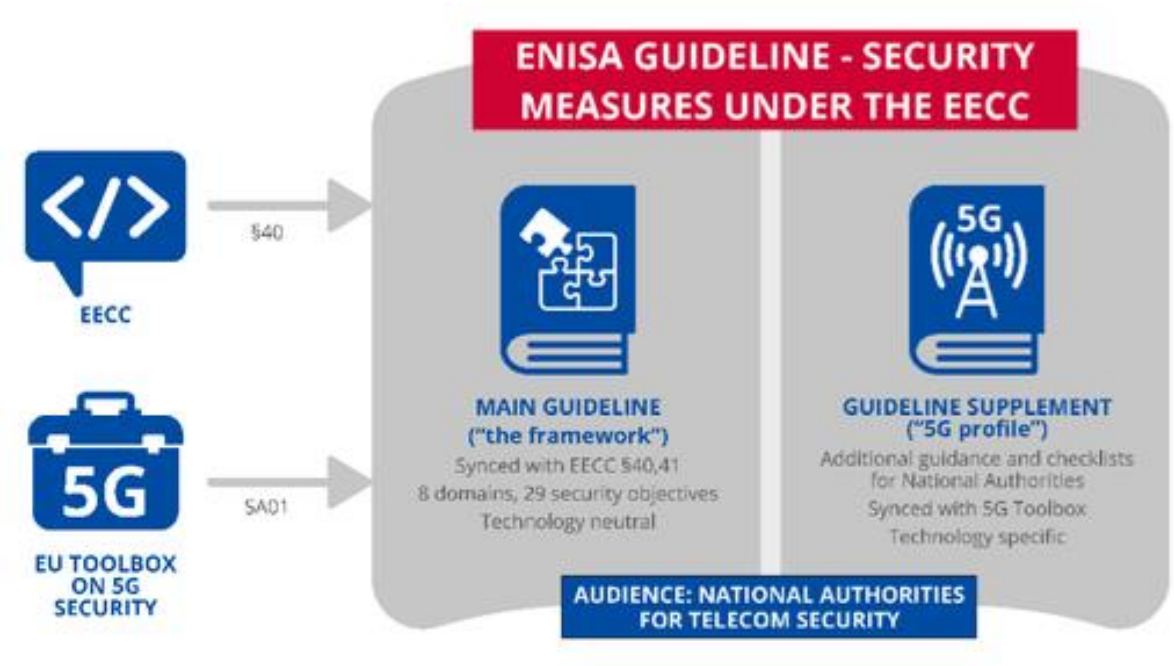

Figure 52 – Structure of the ENISA Guideline on Security Measures under the EECC

A cybersecurity certification scheme for 5G will be developed in line with a February 2021 request by the European Commission to ENISA. The new cybersecurity certification scheme follows on from the EU toolbox for 5G security to further enhance the cybersecurity of 5G networks as it contributes to addressing certain risks, as part of a broader risk mitigation strategy. The 5G scheme will be based on existing cybersecurity certification schemes as well as experience already acquired by ENISA on cybersecurity certification.

19.2.1.5 Guideline on Security Measures under the EECC

Most notably in this report are the Security Objectives (SO) on Encryption and Data Protection:

- **SO 13: Use of encryption:** Ensure adequate use of cryptographic controls for data encryption to prevent and minimise the impact of security incidents on users and on other networks and services.
- **SO 14: Protection of security critical data:** Ensure that the security critical data is adequately protected.

Hence, these guidelines are in line with the mandated use of encryption of all signalling in the 3GPP standards for 5G and they contain useful insights on the impact on network monitoring and the storage of user credentials in an HSM.

19.2.1.6 5G Supplement to the Guideline on Security Measures under the EECC

This document gives additional guidance to competent national authorities about how to ensure implementation and strengthening of security measures by mobile network operators to mitigate risks to 5G networks. The supplement focuses on the cybersecurity of 5G networks at the policy level relating to the EU 5G toolbox and at the technical level for new technologies, such as virtualisation, slicing and edge computing.

In this document the criticality of the 5G assets is defined with both the Core network functions and the NFV management and network orchestration (MANO) classified as Critical, followed by the RAN classified as High, and the other 5G assets classified as Moderate/High.

The 5G Technology profile gives additional and more specific guidance on 5G by clarifying and refining the security measures for 5G networks and services.

Detailed analysis is made of the security impact of network virtualization, network slicing and Edge computing.

19.2.1.7 The EU's Cybersecurity Strategy for the Digital Decade

The EU's Cybersecurity Strategy for the Digital Decade [101] announces three key strategic measures for achieving secure and reliable digital tools and connectivity in the EU:

1. **Boosting the security of essential services and connected things**

Revised rules on the security of network and information systems

Securing 5G networks and supply chain

High standards of cybersecurity for all connected objects, including future Regulation to ensure an Internet of Secure Things

2. **Strengthening collective capabilities to respond to major cyberattacks**

Support to Member States to defend their citizens and national security interests.

Working together on preventing, discouraging, deterring and responding to cyber threats

The Joint Cyber Unit is a platform that will help to better protect the EU from the most impactful cybersecurity attacks, especially cross-border ones.

3. **Working with partners on international security and stability in cyberspace**

The strategy comes with a continued focus on 5G security and related Toolbox – this has testing and assurance within it.

19.2.2 UK Telecommunications (Security) Bill

Telecom companies in the UK must follow tougher security rules or face fines of up to ten per cent of turnover with the new Telecommunications (Security) Bill 216 [95] and [96].

The Bill 216 strengthens the security framework for technology used in 5G and full fibre networks including the electronic equipment and software at phone mast sites and in telephone exchanges which handle internet traffic and telephone calls.

It provides the Government with new national security powers to issue directions to public telecoms providers in order to manage security risks.

19.2.3 United States Regulatory Environment

The United States regulatory environment is driven by the US Congress that either passes a law or delegates authority to the office of the President, who in turn can issue an executive

order. The primary regulatory agency responsible for telecommunications is the Federal Communications Commission (FCC). Following is a list of some key laws and regulations related to telecommunications in the US:

1. **Telecommunications Act of 1934:** This act established the FCC and laid the groundwork for regulating interstate and international communications by wire and radio.
2. **Communications Assistance for Law Enforcement Act (CALEA):** Enacted in 1994, CALEA requires telecommunications carriers to ensure their equipment can support authorised electronic surveillance by law enforcement agencies.
3. **Telecommunications Act of 1996:** This landmark legislation overhauled the regulatory framework for telecommunications, aiming to promote competition and accelerate the deployment of new technologies. It addressed various aspects such as local and long-distance telephone service, cable TV, and the internet.
4. **Net Neutrality Rules:** The FCC has implemented various rules and regulations to preserve an open internet, preventing internet service providers (ISPs) from blocking, throttling, or prioritizing certain internet traffic. The legal framework for net neutrality has seen several iterations and legal challenges over the years. These rules are scheduled to be updated on April 25th, 2024.
5. **Spectrum Allocation:** The FCC is responsible for allocating and managing radio frequency spectrum for various telecommunications services, including wireless communication, for non-Federal use. The National Telecommunications and Information Administration (NTIA) administers spectrum for Federal use.
6. **Universal Service Fund (USF):** Established under the Telecommunications Act of 1996, the USF aims to ensure that all Americans have access to affordable telecommunications services, including telephone and broadband internet.
7. **Privacy Regulations:** The FCC and other federal agencies have implemented rules to protect consumer privacy in telecommunications, including requirements for the protection of customer data and the disclosure of privacy practices by service providers.
8. **Secure 5G and Beyond Act of 2020:** This bipartisan legislation requires the development of a strategy to secure 5G and future generation telecommunications systems and infrastructure in the United States.
9. **Secure and Trusted Communications Networks Act of 2019:** This law aims to protect the security of U.S. telecommunications networks by prohibiting the use of federal funds to purchase equipment or services from companies that pose a national security risk.
10. **Executive Order on Securing the Information and Communications Technology and Services Supply Chain (EO 13873):** Issued in May 2019, this executive order declares a national emergency with respect to the threats posed by foreign adversaries to the U.S. information and communications technology and services supply chain. It grants the federal government authority to block transactions involving information and communications technology or services that pose an unacceptable risk to national security.

The FCC Communications Security, Reliability and Interoperability Council (CSRIC) provides recommendations to the FCC regarding ways the FCC can help to ensure security, reliability, and interoperability of communications systems. CSRIC's recommendations focus

on a range of public safety and homeland security-related communications matters, including: (1) the reliability of communications systems and infrastructure; (2) 911, Enhanced 911 (E911), and Next Generation 911 (NG911); (3) emergency alerting; and (4) national security/emergency preparedness (NS/EP) communications, including law enforcement access to communications.

Although the FCC plays a central role in enforcing and implementing these regulations, other departments may also have considerable influence on the telecommunication industry: Department of Homeland Security (DHS), Department of Commerce and Department of Defense (DOD). The Department of Commerce acts directly through its National Telecommunications and Information Administration (NTIA) as well as National Institute of Standards and Technology (NIST).

19.2.3.1 The FCC Communications Security, Reliability, and Interoperability Council (CSRIC)- reports

CSRIC sets up term councils – numbered II through IX as of this writing—and they work for a period of about 2 years to produce various recommendations. The latest recommendations available at this time are from CSRIC VIII, which were published from 2021 to 2023. Some reports listed by previous councils may still be relevant.

A full list of FCC reports and practices are available in Communications Security, Reliability and Interoperability Council (CSRIC) VIII [152]. The following is a list of some selected reports and best practices:

- CSRIC VIII Report on Security Vulnerabilities and Mitigations in HTTP2 (June 2023)
- CSRIC VIII Report on Best Practices to Improve Supply Chain Security of Infrastructure and Network Management Systems (June 2023)
- CSRIC VIII Report Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment (December 2022)
- CSRIC VIII Report on How Virtualization Technologies Can be used to Promote 5G Security and Reliability (December 2022)

Some notable reports from previous CSRIC VII are:

- CSRIC VII Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security (March 10, 2021)
- CSRIC VII Report on Review and Recommendations on Optional 3GPP Standards for 5G Non Standalone Architecture. (December 9, 2020)
- CSRIC VII Report on Risks Introduced by 3GPP Releases 15 and 16 5G Standards. (September 16, 2020)
- CSRIC VII Report on Risk to 5G from Legacy Vulnerabilities and Best Practices for Mitigation. (June 10, 2020)

19.2.3.2 US Department of Defense (DoD) - 5G Strategy

The US DoD 5G Strategy [66] requires access to resilient and protected 5G capabilities and spectrum. Therefore, the DoD supports national efforts to:

1. Advance U.S. and partner 5G capabilities,
2. Promote awareness of 5G risks to national security,

3. Develop approaches to protect 5G infrastructure and technologies.

Given the breadth of these challenges, the DoD must collaborate closely with other U.S. Departments and Agencies, industry, academia, Congress, allies, and partners to ensure success.

5G technologies are strategic capabilities that will impact the U.S. economic and national security and those of its allies and partners. The DoD can utilise its unique partnerships, expertise, and resources to accelerate 5G innovation and deployment, including leading edge-millimetre-wave and spectrum sharing technologies in support of DoD's enduring missions. This will help ensure that the U.S. military, the American public, and its allies and partners have access to the best 5G systems, services, and applications in the world.

19.2.3.3 DHS, CISA and S&T – Secure Mobile Network Infrastructure for Government Communications

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and Science and Technology Directorate (S&T) issued a Broad Agency Announcement (BAA) in 2019 that demanded new standards to improve the security and resilience of critical mobile communications networks.

The BAA established a research and development (R&D) project for a Secure and Resilient Mobile Network Infrastructure (SRMNI) through which S&T worked with several performers on innovative approaches to improving protection of the cellular mobile infrastructure against threats. A program guidebook summarizing work undertaken by the performers was published as a result [153].

19.2.3.4 DHS and CISA - Overview of Risks Introduced by 5G Adoption in the United States and 5G Wireless Networks: Market Penetration and Risk Factors

The report "Overview of Risks Introduced by 5G Adoption in the United States" [46] by the Department of Homeland Security (DHS) / Cybersecurity and Infrastructure Security Agency (CISA) assesses that the Fifth Generation Mobile Network (5G) will present opportunities and challenges, and its implementation will introduce vulnerabilities related to supply chains, deployment, network security, and the loss of competition and trusted options:

Use of 5G components manufactured by untrusted companies could expose U.S. entities to risks introduced by malicious software and hardware, counterfeit components, and component flaws caused by poor manufacturing processes and maintenance procedures. 5G hardware, software, and services provided by untrusted entities could increase the risk of compromise to the confidentiality, integrity, and availability of network assets.

5G will use more components than previous generations of wireless networks, and the proliferation of 5G infrastructure may provide malicious actors with more attack vectors. The effectiveness of 5G's security enhancements will, in part, depend on proper implementation and configuration.

The CISA report is accompanied by the "5G Wireless Networks: Market Penetration and Risk Factors" [47] providing an overview of the Mobile Network Equipment Components Market Leaders and the Major Components of 5G Networking for UE, RAN and CN.

Since the initial report, CISA has produced a number of security related recommendations: [154] for example:

- 5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance.
- Potential Threats to 5G Network Slicing.
- Open RAN Security Considerations.
- Security Guidance for 5G Cloud Infrastructures.

19.2.3.5 CISA – Ensuring the Security and Resilience of 5G Infrastructure in Our Nation

In its report "CISA 5G Strategy: Ensuring the Security and Resilience of 5G Infrastructure in Our Nation" [89] the CISA outlines five 5G Strategic Initiatives with respective Spotlights:

1. Support 5G policy and standards development by emphasizing security and resilience with as spotlight the collaborative work between government and the private sector in FCC's CSRIC Working Groups.
2. Expand situational awareness of 5G supply chain risks and promote security measures with as spotlight the Federal Acquisition Security Council (FASC) and implementation of the Federal Acquisition Supply Chain Security Act.
3. Partner with stakeholders to strengthen and secure existing infrastructure to support future 5G deployments with as spotlight the discussions with the rural carriers to discuss 5G innovation, security, and risk mitigation efforts.
4. Encourage innovation in the 5G marketplace to foster trusted 5G vendors.
5. Analyse potential 5G use cases and share information on risk management strategies with as spotlight 5G use cases as the initial 5G applications will be organised by use case type, which are defined by their unique characteristics and services they facilitate.

19.2.3.6 The Enduring Security Framework (ESF)

The Enduring Security Framework (ESF) is a public-private partnership that addresses risks to critical infrastructure and national security systems. It has produced reports on ORAN, OSS supply chain, SBOM, identity and access management, and network slicing security (reference [155].

19.2.4 South Korea Shared 5G Infrastructure

The South Korean government pushed domestic carriers to share a single 5G infrastructure for reasons of cost rather than security. For more details see "South Korean carriers agree to build single 5G network, saving money and time" [117].

19.2.5 5G security policies, standards and practices in China

China actively promotes 5G cyber security, and continuously improves security assurance measures in terms of policies, standards, and technologies, and makes overall planning for 5G security.

19.2.5.1 5G security policies' development

In March 2020, the Ministry of Industry and Information Technology (MIIT) issued the Notice on Accelerating the Development of 5G, aiming to promote industry development. The following are the MIIT provisions:

- Provide instructions on building a 5G security assurance system, while accelerating the construction of new 5G infrastructure and strengthening the research and development of 5G technologies.
- Guide the IMT-2020 (5G) Promotion Group aiding the releases of the 5G Security Report [148],and the 5G cyber security implementation guide.
- Provide technical guidance for 5G Security risks and countermeasures helping all industries understand and respond to 5G security issues objectively.

In addition, in July 2021, MIIT, CAC, National Development and Reform Commission, and other nine departments issued the Action Plan for 5G Application (2021-2023)[149], which pointed out that it is necessary to accelerate the construction of a security assurance system that is compatible with the development of 5G applications.

19.2.5.2 5G security standards framework establishment.

The goal of this framework is to be inline with the progress of international standards, such as 3GPP SA3, and GSMA Industry Guidelines. The following are the goals of the 5G Security standards framework:

- Rely on the security working group of the IMT-2020 (5G) Promotion Group, and actively deploy 5G security standards in Chinese standardization organizations such as TC260, TC485, and CCSA[150].
- Promote the formulation of technical standards for 5G communication security, MEC security, slicing security, and device security assurance in China.
- Release industry standards, such as 5G Mobile Communication Network Security Technical Requirements.
- Establish a sound 5G security standard system.
- Guide the healthy development of 5G security technologies, products, and industries.
- Formulate a series of specifications for the security assurance of 5G mobile communication equipment in China.
- Build a security assessment system covering various security assurance requirements for 5G base stations and core networks.
- Lay the foundation for mutual recognition with international 5G security testing and certification.

19.2.5.3 Build 5G Core Security Evaluation and Testing.

Under the guidance of MIIT, China Academy of Information and Communications Technology (CAICT) set up a 5G security evaluation centre to build a 5G network test bed. The following are the objectives:

- Build detection capabilities, including terminal access security, base station/core network device security, communication protocol security, and network slicing security.
- Work with the organization of operators and equipment vendors to carry out 5G network equipment security evaluation efforts.

In May 2021 5G base station and core network equipment security tests were completed for five mainstream equipment manufacturers - Huawei, ZTE, Ericsson, and Shanghai Nokia

Bell. The test results have been released by the IMT-2020 (5G) Promotion Group and on the GSMA official website[151].

19.2.6 World Economic Forum

The World Economic Forum (WEF) cares about 5G because of the global impact on society and economies [37]. In preparing for future cyber security scenarios, the WEF explores the following three key cybersecurity areas:

- Threat - what will be the biggest changes to the threat landscape as a result of 5G rollout?
    - Emergence of a new generation of threats unique to 5G – impact on signalling, configuration and authentication.
    - Acceleration and modification of existing attack methods.
    - Widening and deepening of the attack surface given to new connected ecosystems.
- Cooperation - who are the new stakeholders MNOs will need to work with in order to secure the rollout and use of future networks?
    - 5G will play a crucial role in the operation of society – far more than 4G has done.
    - New networking and service models will therefore be required, including new trust models.
    - A far wider range of stakeholders will need to consider the security implications of their interfaces.
    - 5G will also pose new concerns around privacy, identity management and interoperability.
- Policies and Incentives - where are there good examples of incentivising the secure rollout of 5G networks?
    - Consensus building will be required across stakeholders in order to develop a robust baseline security level.
    - Implications of 5G networks being considered as critical infrastructure on the supply chain.
    - Streamlining of approaches and global competitiveness.
    - Awareness raising among ‘new’ stakeholders and governments.

19.2.7 EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks

Following the studies by ENISA, the Network and Information Systems (NIS) Directive issued the report “EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks” [48] with the support of the Commission and the European Agency for Cybersecurity.

This is a major step for the implementation of the European Commission Recommendation adopted in March 2019 to ensure a high level of cybersecurity of 5G networks across the EU as 5G networks is the future backbone of our increasingly digitised economies and societies.

The report is based on the results of the national cybersecurity risk assessments by all EU Member States. It identifies the main threats and threat actors, the most sensitive assets, the

main vulnerabilities (including technical ones and other types of vulnerabilities) and a number of strategic risks.

The security challenges are mainly linked to:

- Key innovations in the 5G technology (which will also bring a number of specific security improvements), in particular the important part of software and the wide range of services and applications enabled by 5G;
- The role of suppliers in building and operating 5G networks and the degree of dependency on individual suppliers.

Specifically, the roll-out of 5G networks is expected to have the following effects:

- An increased exposure to attacks and more potential entry points for attackers.
- Certain pieces of network equipment or functions are becoming more sensitive, such as base stations or key technical management functions of the networks.
- An increased exposure to risks related to the reliance of MNOs on suppliers that also will lead to a higher number of attack paths.
- The risk profile of individual suppliers will become particularly important.
- Increased risks from major dependencies on suppliers.
- Threats to availability and integrity of networks will become major security concerns.

Together, these challenges create a new security paradigm, making it necessary to reassess the current policy and security framework applicable to the sector and its ecosystem and essential for Member States to take the necessary mitigating measures.

In addition, the European Agency for Cybersecurity has published the report “ENISA Threat Landscape for 5G Networks – Updated Threat assessment for the fifth generation of mobile telecommunications networks (5G)” [60] that draws an initial threat landscape and presents an overview of the 5G network security challenges. It also, beneficially, creates a comprehensive 5G architecture, identifies important assets (asset diagram), assesses threats affecting 5G (threat taxonomy), identifies asset exposure (threats – assets mapping) and provides an initial assessment of threat agent motives.

In the updated version some additional elements have been taken into account to enlarge the scope of the assessment and include important parts for the enhancement of operational security:

- Implementation/migration options of a gradual migration to 5G from 4G have been taken into account including technical details on IE's, encryption, SEPP and roaming.
- Secondly, security issues of operational processes have been considered. These two changes enlarge the scope of the assessment and include important parts for the enhancement of operational security.
- A vulnerability analysis, which examines the exposure of 5G components and how cyber threats can exploit vulnerabilities and how technical security controls can help mitigate risks.

Following this ENISA report, the toolbox “Cybersecurity of 5G networks EU Toolbox of risk mitigating measures” [61] was agreed by the NIS Cooperation Group. The objectives of this toolbox are to identify a possible common set of measures which are able to mitigate the

main cybersecurity risks of 5G networks and to provide guidance for the selection of measures which should be prioritised in mitigation plans at national and at EU level to create a robust framework of measures with a view to ensure an adequate level of cybersecurity of 5G networks across the EU and coordinated approaches among Member States.

The measures contained in the EU Toolbox are based on the following 9 risks:

- R1: Misconfiguration of networks.
- R2: Lack of access controls.
- R3: Low product quality.
- R4: Dependency on a single supplier.
- R5: State interference through 5G supply.
- R6: Exploitation of 5G networks by organised crime.
- R7: Significant disruption of critical infrastructure.
- R8: Massive failure due to power interruption.
- R9: IoT exploitation.

Subsequently, the Network and Information Systems (NIS) Directive issued the “Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity” [87] that provided an overview of the toolbox implementation process by as of June 2020 focussing on the steps taken by EU Member States at national level.

A large majority of the EU states are in the process of significantly strengthening national regulatory powers to regulate the procurement of network equipment and services by operators, to perform more regular and detailed audits and to request more information from operators about 5G equipment procurement and deployment plans. The implementation of the measures aimed at minimising the exposure to high-risk suppliers as well as to limit the types of activity and conditions under which MNOs are able to outsource particular functions.

19.2.8 ETIS – Telco Security Landscape

The Global IT Association for Telecommunications (ETIS) Information Security Working Group is monitoring together with the Dutch research institute TNO the status of the Telco Security Landscape [49].

This provides an overview of the main Security Threats and Security Opportunities and is being updated during their regular meetings.

19.2.9 5G-ACIA Security Aspects of 5G for Industrial Networks

The 5G Alliance for Connected Industries and Automation (5G-ACIA) White Paper “Security Aspects of 5G for Industrial Networks” [68] concentrates on the security needs of industrial networks by drawing on use cases and network deployment models and focusing on the requirements of operational technology (OT) companies, and on the degree to which these are already fulfilled by existing 5G features, and describes gaps between the two.

In the IEC 62443 standard context, when the 5G network is part of a critical industrial system, the administrators and 5G MNOs must be trusted by the industrial systems operators. When security levels 3 and 4 are needed, higher layer protections (e.g. a secure application layer protocol such as TLS or IPsec) may have to be provided.

The degree of involvement of the PLMN operator in implementation of the OT network plays an important part in determining which security features apply. In an OT 5G Public Network-Integrated Non-Public Network (PNI-NPN), where a PLMN operator provides part of the network infrastructure or services, the PLMN operator is a new entity that the OT operator must trust based on its certification requirements. As in any outsourcing model, visibility and monitoring capabilities become key to establishing trust and verifying compliance. It has been demonstrated that 5G security features form a toolbox that both OT and PLMN operators can use to manage the risks in OT networks.

19.2.10 5GAA Efficient Security Provisioning System

The White Paper “Efficient Security Provisioning System” [69] published by the 5G Automotive Association (5GAA) outlines the properties of the optimised ‘Efficient Security Provisioning System’ (ESPS) that is designed to balance the security and privacy principles of existing region specific systems in USA and Europe that are not fully interoperable due to differing security and privacy requirements.

In this context, it is paramount that the system architecture ensures not only the principles of security and privacy, but also those of deployability and practical operation. It constitutes a call to action for all Vehicle-to-Everything (V2X) communication stakeholders to take these into account when implementing credential management systems for V2X, and to future-proof such systems against threats that may arise as connected cars become ubiquitous.

19.2.11 5G Americas white paper “Security Considerations for the 5G ERA

This white paper [84] examines the security considerations in the 5G ERA of aspects like software, virtualisation, automation and orchestration. Concepts such as zero-trust security are discussed to mitigate the threats, and various recommendations are proposed for security enhancements.

The paper concludes that the new 5G architectures can expose new vulnerabilities. Securing 5G must be designed-in and not be an afterthought. Hence, a careful approach to these new aspects of cloud-native services, open-source software, APIs, SDN and NFV can improve their security. Taking a zero-trust approach, combined with advanced cyber threat intelligence, will further enhance 5G’s security.

Security assurance considerations for the Software Supply Chain are also described in the paper.

19.2.12 5G Standalone core security research

This report from Positive Technologies [102] shows that the technology stack in 5G potentially leaves the door open to attacks on subscribers and the operator's network performed from the international roaming network, the operator's network, or partner networks.

The report outlines attacks based on vulnerabilities in the HTTP/2 protocol and a MITM attack relying on the PFCP. Therefore, also in the 5G network it is vital to ensure comprehensive protection as operators frequently make errors in equipment configurations with consequences for security. The important role played by equipment vendors, which are

responsible for the technical implementation of the architected network protection features, is covered.

Protection of the 5G core must be thorough and far-reaching with additional systems for monitoring, control, and filtering, in addition to regular security audits of the MNO network to identify potential risks.

19.2.13 5G Smart Devices Supporting Network Slicing

The white paper “5G Smart Devices Supporting Network Slicing” by the NGMN Alliance (Next Generation Mobile Networks Alliance) [104] outlines that the design of the Network Slicing function in 5G devices has to rely on 5G device OS as well as the traffic descriptors of the service between the upper layer and the modem, which results in the inability of current 5G devices to support the use of network slicing. The paper provides the reference design of network slicing solutions in 5G devices.

This white paper analyses the unique technical capability and service advantages of network slicing services. Through the research and analysis of the key parameters and signaling messages of network slicing, combined with the actual design capability of the current system, the paper introduces the challenges faced by the characteristics of network slicing in the design and technical implementation of the system. The paper introduces a variety of reference architectures and technical design schemes for network slicing in devices and proposes that 5G devices should support "the target scheme of network slicing in the devices" and "modem centralization scheme", which provides guidance for 5G devices to support network slicing capability.

19.2.14 Protecting Subscriber Privacy in 5G

For more details about the capabilities with IMSI/SUPI encryption in the 5G SIM or in the device see “Protecting Subscriber Privacy in 5G” by the Trusted Connectivity Alliance [103].

The paper explains how 5G subscriber privacy is improved by encrypting the IMSI/SUPI to mitigate the risk of IMSI Catchers. In addition, the capabilities of the options are compared with encryption implemented in the 5G SIM or in the device. The paper also underlines that an important balance is necessary between protecting a citizen’s right to privacy and ensuring that law enforcement agencies can track and monitor criminals.

20 5G Security Research

20.1 Overview

5G security has proven to be an attractive and fertile domain and area of focus for security researchers. Government research agencies and a range of academic research papers and other vulnerability disclosures have been published, revealed at security conferences and otherwise made public.

Some security researchers have chosen to disclose details of 5G security vulnerabilities to GSMA under its CVD programme. A summary of the various disclosures that specifically relate to potential weaknesses in the 5G security standards is provided below.

20.2 A Formal Analysis of 5G Authentication (CVD-2018-0012)

The research paper “A Formal Analysis of 5G Authentication” [19] describes flaws in the 5G standard which could lead to network deployments not fulfilling critical security goals of 5G AKA. The paper describes three vulnerabilities as follows;

1. Due to a lack of channel binding, KSEAF and SUPI could be confused between concurrent sessions between HN (Home Network) and SN (Serving Network) allowing attackers to bill other customers.
2. Attackers could impersonate a serving network towards a subscriber because implicit authentication is deferred to use of keys.
3. Active attackers can trace a subscriber through use of the AKA protocol if the attacker is, and stays, in the physical vicinity of the subscriber.

The first issue no longer exists because the 5G specifications evolved and SUPI and K_SEAF, are now included in the same message. Consequently, confusion is no longer possible, and this vulnerability has been resolved.

The second issue is not considered a security oversight as a conscious decision was taken during the standardisation process to bind the key delivered to the serving network to the serving network identity to simplify the key hierarchy and to ensure legacy compatibility.

The third issue was considered to be only of moderate concern because authentication involving SUPI encryption, with SUCI sent back to the home network decryption, only happened on the rare occasions when a temporary identifier is not available, such as initial attach to a new serving network. This was a design decision for efficiency reasons.

The researchers proposed radical reform of the authentication protocol, which was considered impractical for reasons of backward compatibility. GSMA’s CVD Governance Team encourages operators to continue deploying the AKA protocol in their 5G core. Further analysis of the research is contained in the GSMA’s briefing paper [20]:

20.3 On LTE Network Security Testing and Attack Detection Techniques with Full Baseband Control (CVD-2018-0013)

The research paper “On LTE Network Security Testing and Attack Detection Techniques with Full Baseband Control” [24] describes how insecurely configured LTE networks fail to enforce the mandatory integrity protection on NAS and RRC can allow attackers to launch a range of attacks including billing fraud.

Except for emergency calls, LTE networks must reject peers without integrity protection but open source terminals could allow attackers to request insecure operation and a similar issue exists in 5G. 3GPP TS 24.501 [26] was updated for 5GS NAS handling. Vendors should check how their MME/AMF implementations react when receiving illegal input and apply appropriate error handling. Vendors are also advised to test the behaviour of non-standards compliant devices.

A detailed assessment of the issues and the impact is available in a GSMA briefing paper [25].

20.4 Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information (CVD-2018-0014)

The research paper “Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information” [21] describes an inherent design weakness of the 4G/5G cellular paging protocol which can be exploited to achieve the following outcomes:

1. Determine whether a particular user is in a particular geographical area.
2. Determine a user’s IMSI (or SUPI for 5G) from the MSISDN or other identifiers.

The attacks involve the attacker triggering paging messages to a target subscriber’s phone and if enough are sent in quick succession it could be possible to observe on the radio interface if the number of paging messages in a particular area increase, indicating the presence of the target. The researchers observed that paging messages for any particular device will only happen in specific time slots, on a cycle that the attacker could observe, and patterns could reveal when multiple paging messages are sent to the same device (even if the temporary identifier (TMSI/GUTI) changes every time). A trial-and-error search of encrypted SUPIs, using a false base station to send trial registration requests, possibly over a long period of time that could render the attack impractical, could eventually reveal the IMSI by analysing responses.

The GSMA Governance Team considered the research and concluded it was based on an early version of 3GPP TS 38.304 [23]. The procedures had since been changed so that the calculation of the Paging Frame Index (PFI) is no longer IMSI based but now uses 5G-S-TMSI, which is strictly refreshed in 5G. Therefore, the attacks described in the paper do not work and no remedial action is required.

Full details are available in the GSMA briefing paper [22].

20.5 New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities (CVD-2019-0018)

The research papers “New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities” [41] and “New Vulnerabilities in 5G Networks” [45] describe identification, bidding down and device battery drain attacks by exploiting unprotected device capabilities in 4G and upcoming 5G networks.

The vulnerability arises from current 3GPP RRC specifications allowing the UECapabilityEnquiry procedure to occur before RRC security establishment. This exposes the UE capabilities to tampering by a MITM attacker on the radio interface, which can result in degradation of service e.g. downgrading the UE’s maximum throughput. Since the UE capabilities are persistently stored in the network, the impact of the attack can last for weeks, or until the UE is power cycled. Such attacks can have a particularly high impact on unattended IoT devices. The researchers demonstrated the feasibility of the attack using low-cost equipment.

As there is no legitimate reason to fetch UE radio network capabilities before RRC security establishment, GSMA requested 3GPP to change the specifications to prohibit the eNodeB or gNodeB from running the UECapabilityEnquiry procedure before RRC security establishment. The network should run the RRC UECapabilityEnquiry procedure only after AS security has been activated so the vulnerabilities no longer exist.

Further details are contained in the GSMA briefing paper [42].

20.6 New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols (CVD-2019-0020)

The research paper “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols” [27] describes privacy threats by activity monitoring attacks. The paper addresses the risks with the policies for the sequence number (SQN) of the AKA protocols in 3G and 4G and the improvements with the asymmetric encryption of the SUPI in 5G.

Although the paper was not submitted to GSMA under its CVD programme, it was considered when the research was made public. The claims in the paper are known security risks and no need for further action was concluded.

20.7 Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane (CVD-2019-0021)

The research paper “Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane” [28] discusses potential security problems by dynamically testing the CP components in an operational LTE network. The procedure of semi-automated dynamic testing consists of three steps:

1. Creating security properties based on specification analysis.
2. Generating and conducting test cases that violate the security properties.
3. Classifying a problematic case.

LTEFuzz successfully identified 15 previously disclosed vulnerabilities and 36 new vulnerabilities in LTE design and implementation among the different carriers and device vendors. It also demonstrated several attacks that can be used for denying various LTE services, sending phishing messages, and eavesdropping/manipulating data traffic.

LTEFuzz would remain useful for 5G NSA as long as open-source LTE implementations such as srsLTE support 5G in radio communication. Additional development would be required to support 5G SA, as the CN is likely to change.

Although the paper was not submitted to the CVD programme, it was notified through a GSMA member [29]. The claims in the paper are known security risks and no need for further identification.

20.8 Lost Traffic Encryption: Fingerprinting LTE/4G Traffic on Layer Two (CVD-2019-0022)

The research paper “Lost Traffic Encryption: Fingerprinting LTE/4G Traffic on Layer Two” [39] provides a detailed analysis of website fingerprinting and a water-marking attack to identify victims within LTE networks.

Traffic fingerprinting enables an adversary to exploit the metadata side-channel of transmissions with impact on the user’s privacy. These attacks succeed in LTE and 5G networks due to similar layer-two functionality.

According to the impact assessment by the GSMA [40], this research is interesting from an academic perspective and a known risk, but no action was considered necessary.

20.9 IMP4GT: IMPersonation Attacks in 4G NeTworks (CVD-2019-0024)

The research paper “IMP4GT: IMPersonation Attacks in 4G NeTworks” [70] describes an uplink impersonation attack and a downlink impersonation attack, both using a false base station. The researchers show how the attacks can be used to perpetrate billing fraud, commit fraud by impersonating a website and taking over a user’s account, obtain unauthorised access to customer services and/or to bypass an MNO’s firewall.

A user traffic modification vulnerability exists because user traffic in LTE is encrypted but not integrity protected. An integrity check allows both ends of a communication to detect if data was modified in transit. This same attack applies to 5G as user-data integrity protection is optional to use or only up to 64 kbit/s data rates.

As a long-term solution for both LTE and 5G, GSMA in consultation with 3GPP, in a briefing paper [71] advises MNOs to:

- Ensure that newly purchased LTE/5G terminals and base stations support UP integrity protection to the fullest extent specified in the 3GPP standards.
- Assess the feasibility of a gradual upgrade of LTE/5G terminals and base stations in the field to support full rate UP integrity protection.

20.10 Security Analysis of 5G Mobile Networks (CVD-2019-0028)

The research paper “Security Analysis of 5G Mobile Networks” [76] analyses how subscriber security can be attacked by exploiting design constraints or flaws in the 5G mobile network including broadcasting, paging and dedicated unicasting channels.

After detailed analysis, the GSMA Governance Team concluded the research was not new and no specific action was required.

20.11 5G Reasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol (CVD-2019-0029)

The research paper “5G Reasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol” [54] proposes a framework for property-guided formal verification of control-plane protocols spanning across multiple layers of the 5G protocol stack.

5GReasoner has identified 11 design weaknesses resulting in attacks having both security and privacy implications and discovered 5 previous design weaknesses that 5G inherits from 4G and can be exploited to violate its security and privacy guarantees.

After detailed analysis of the scenarios, the GSMA Governance Team judged the scenarios as nil or low impact in practice [55].

20.12 Eavesdropping Encrypted LTE Calls with REVOLTE (CVD-2019-0030)

The research paper “Eavesdropping Encrypted LTE Calls With REVOLTE” [72] describes an attack that takes advantage of some network equipment reusing the same key which encrypts the data transmitted between the radio mast and the UE between different calls.

This allows the attacker to decode and listen to a targeted call, if the attacker 1) knows the victim’s phone number, 2) can identify a specific call they wish to listen in to, 3) gets the UE

to answer an ‘attack’ call from the attacker while the victim remains connected to the same cell, 4) records the same radio signals as the victim UE for the duration of the attack, and 5) keeps the attack call going for the period of time they wish to listen in to the original call.

The following set of remedies are listed in the GSMA briefing paper [73]:

- All eNB vendors need to check their products for potential keystream re-use and develop a patch for affected network products.
- 3GPP standards need to be clearer that rekeying is required before bearer ID re-use.
- For future 3GPP releases, to add defined UE behaviour when facing such eNBs.

The same attack technique could potentially be used to target other types of traffic sent via the radio network, or similar calls in 5G networks, however these have not been assessed in this research.

20.13 5G SUCI-Catchers: Still catching them all? (CVD-2020-0033)

The research paper “SUCI-Catchers: Still catching them all?” [77] demonstrates a 5G SUCI-Catcher attack within a functional 5G SA network.

The GSMA Governance Team concluded the ‘SUCI-catching’ attack was considered to be of academic interest but the ‘probing’ attack low-threat and low-impact and neatly summarised in research paper “A Survey of Subscription Privacy on the 5G Radio Interface” [78]. Probing is where an attacker already knows the subscription identity, e.g., an IMSI or an MSISDN plus some associated information, and wants to find out whether the subscriber with this identity is present in a given area. This is a far less powerful attack than a catching attack. There are many possible ways to carry out such an attack, e.g., send a bunch of (if possible silent) SMSs or other “activity triggers” to the MSISDN and see if there is a corresponding flurry of signalling in the cell you are monitoring.

20.14 LTE/5G Downgrade Attack (CVD-2020-0034) and The Dos attack with registration request and service reject (CVD-2020-0036)

By sending NAS messages without integrity protection, a rogue eNB/gNB can cause a UE to not use a tracking area (TA) for a period of ~30-60 minutes. When carried out for all TAs in a geographic area, the user will lose 4G/5G connectivity in that area (including the security benefits) for the period, forcing the UE to connect to the less secure 3G/2G mobile systems.

The research also looks at a back-off timer for congestion being triggered within a UE by a rogue base station that would cause a DoS for the user for 15 – 30 minutes. In case of congestion, the network must be able to instruct UEs to back-off for a certain time without increasing the network load by having to establish a security context first.

Both vulnerabilities are the result of a network design risk assessment whereby the protocol design strikes a balance between potential limited DoS to individual user’s vs potential DoS to the network.

20.15 The leakage and manipulation of UeIdentityTagInfo (CVD-2020-0035)

This research identified that in ETSI GS MEC 014 (5G Mobile Edge Computing) no authorisation is mandated for retrieval and registration/deregistration of UeIdentityTagInfo.

However, MEC 009 specifies the usage of OAuth token and TLS credentials for all APIs (including MEC 014), and ETSI was requested to add a reference to MEC 014 to avoid misunderstanding.

20.16 A Stealthy Location Identification Attack (SLIC) (CVD-2020-0040)

The research paper “A Stealthy Location Identification Attack (SLIC) Exploiting Carrier Aggregation in Cellular Networks” [81] describes how an attacker, by passive eavesdropping, can compare the path an arbitrary user takes to other known paths within a building served with multiple secondary cells connected to a primary cell – subject to preconditions. In the researcher’s demonstration, they show how this can be used to identify the walking path taken by a target user when the user is downloading at least 40Mbps.

A similar situation may exist in the 5G network – and if 5G deployments support more carrier aggregation in particular deployment setups, then the attack could be slightly more powerful.

The GSMA Governance Team concluded on the following proposed countermeasures:

- operators to configure their networks to change temporary device identifiers frequently.
- 3GPP to modify the standards to add noise to the unused parts of the message that leaks information.

20.17 A side channel vulnerability that allows attacker hijacking TCP connection under LTE/5G Network (CVD-2020-0042)

The research paper “A side channel vulnerability that allows attacker hijacking Transmission Control Protocol (TCP) connection under LTE/5G Network” [118] describes an attack, which takes advantage of insecure TCP connections between a victim UE and a Rich Communications Services (RCS) server to send spoofed RCS messages to targeted users. This is not a flaw in 5G, nor a flaw in RCS - it is about operator architectural decisions in TCP server deployments e.g. RCS server deployment.

Mobile network operators should ensure that their RCS services are protected against IP-spoofing attacks and operators should also update their risk analysis and mitigations to include similar IP-spoofing attack vectors on other TCP-based services, specifically services which are hosted externally and don’t natively use TLS / NDS security e.g. SIP-based SaaS services.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	Sep 2020	New document that provides an overview of 5G security and related aspects	GSMA TG	Pieter Veenstra, NetNumber
2.0	Oct 2021	Document updated to reflect security enhancements included in 3GPP Release 16. New sections have been added on a range of topics including virtualisation, network slicing, software defined networks, open RAN, open-source software and security assurance. References have also been added pertaining to published reports and security research	GSMA FASG	Pieter Veenstra, NetNumber
3.0	16 Jul 2024	Document updated to reflect Zero Trust, Layer 7 security, including threat inspection, expansion on network virtualization to include container environments and security, considerations for Post Quantum cryptology.	GSMA FASG	Galina Pildush, Palo Alto Networks

A.2 Other Information

Type	Description
Document Owner	Fraud and Security Group
Editor / Company	Galina Pildush, Palo Alto Networks
Contributors	Silke Holtmanns, Enea Looi Kwok Onn, Infobip Mansour Ganji, One New Zealand Niraj Rathod, BT Sven Lachmund, Deutsche Telekom Stan Wong, Hong Kong Telecommunications Yair Kler, Huawei Lei Zhongding, Huawei Imran Saleem, Mobileum Anja Jerichow, Nokia Travis Russell, Oracle John Kimmins, Palindrome Technologies Zhaoji Lin, ZTE James Moran, GSMA Galina Pildush, Palo Alto Networks

	Muddasar S Ahmed, MITRE Michaela Vanderveen, MITRE Roger Brown, GSMA Roger Piqueras Jover, Google Bo Zhang, Huawei Herve Collet, Thales Nataliya Stanetsky, Google Jie Ma, China Mobile Jiwan Ninglekhu, Google Andreas Pashalidis, BSI Ben Wheeler, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com.

Your comments or suggestions & questions.