5G Security Guide

Version 2.0

20 October 2021

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Contents

1 Introduction

1.1 Overview

The fifth generation (5G) telecommunication system will deliver enhanced mobile broadband, massive machine type communications, and ultra-reliable and low latency communications to subscribers. 5G will also provide multi-network slicing, multi-tenancy, multi-level of services and multi-connectivity network capabilities to initiate the vertical industry to join the operation and development of the 5G services regime.

Alongside the new capabilities in 5G, there are also changes in how networks are built and managed. These include virtualisation and containerisation, network function virtualisation (NFV), open source software, SDN security monitoring, security assurance, security of O-RAN interfaces and components, network slicing, programmable network, multi-access edge computing (MEC) and combined development and operations functions, so called DevOps. These new techniques 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 realised 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 other principles based concepts including:

- Use of mutual authentication – ensure that sender and receiver have an established trusted and secured relationship
- Assume zero trust – operate on the basis of not automatically trusting anybody or anything inside or outside the network perimeter
- 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 and GSMA).

1.2 Scope

Unless stated otherwise, the discussions in this document refer to the capabilities supported by 3GPP Release 16, i.e. the second release of 3GPP standards for 5G. The content of this version 2.0 reflects current understanding in 2021.

Further updates of this document will be made to reflect the 3GPP work on future 5G Releases. The next version of the document is planned for 2022 to ensure the document reflects Release 17.

NOTE: A number of topics included in this document are managed by organisations and standards development organisations other than 3GPP. These topics continue to evolve but not necessariy in step with 3GPP Relases. Key developments on these topcs will be covered in future versions of this document.

1.3 Abbreviations

Term	Description
5GC	5G Core Network
5G-RG	5G Residential Gateway
5GS	5G System
5GSTF	GSMA 5G Security Task Force
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
ALS	Application Layer Security
AMF	Core Access and Mobility 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
EAP	Extensible Authentication Protocol
ECIES	Elliptic Curve Integrated Encryption Scheme
EAP-AKA	Extensible Authentication Protocol – Authentication and Key Agreement

Term	Description
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
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
GUTI	Globally Unique Temporary Identifier
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
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
MCVideo	Mission Critical Video
MEC	Mobile / Multi-Access Edge Computing
MISP	Malware Information Sharing Platform

Term	Description
MITM	Man-In-The-Middle
MME	Mobility Management Entity
MNC	Mobile Network Code
MNO	Mobile Network Operators
MPS	Multimedia Priority Service
MR	Measurement Report
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 Authorization 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 PLMN
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network

Term	Description
POI	Point Of Interconnect
PRD	Permanent Reference Document
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(ality)
SECAM	Security Assurance Methodology
SeGW	Security Gateway
SEPP	Secure Edge Protection Proxy
SIDF	Subscription Identifier De-concealment Function(ality)
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
SRVCC	Single Radio Voice Call Continuity
SS	Synchronisation Signal
SSH	Secure Shell
SUCI	Concealed Subscription Identity

Term	Description
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
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

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)
[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

Ref	Doc Number	Title
[10]	GSMA PRD IR.88	LTE and EPC Roaming Guidelines
[11]	ENISA Signalling Security	Signalling 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 Signalling 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
[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

Ref	Doc Number	Title
[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
[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

Ref	Doc Number	Title
[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
[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

Ref	Doc Number	Title
[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
[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

Ref	Doc Number	Title
[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
[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/

Ref	Doc Number	Title
[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/

2 Summary of New Security Features in 5G

A range of resources exist that detail the security enhancements that 5G will deliver over earlier generation mobile technologies. “Why 5G will lead to improved security for mobile communications” [119] provides a helpful overview. Additionally, the article “Comparing 5G to Wi-Fi 6 from a security perspective” [120] discusses security in 5G and Wi-Fi.

The key aspects of the security features inherent in the 5G specifications are described in the sections below. For further details please refer to the appropriate 3GPP standards such as TS 23.501 [31] and TS 33.501 [1].

2.1 Unified Authentication Framework & Access-Agnostic Authentication

- 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 N3IWF in Release 16, 5G includes a single authentication infrastructure for both 3GPP access and non-3GPP access.
- Authentication methods used include 5G AKA, EAP-AKA and any EAP method.
- Any method can be used to authenticate the User Equipment (UE) over both access types.

2.2 Primary Authentication

- Newly developed 5G AKA and EAP–AKA' (both mandatory to be supported for the UE and the serving network)
- EAP-TLS [13] 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).

2.3 Secondary Authentication

- 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
- 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-PLMN (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

- 5G introduces a SUbscription Concealed Identifier, called SUCI, a privacy preserving identifier concealing the Permanent Subscription Identifier (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 maybe required by some regulatory environments

- SUPI is decoupled from paging procedure, i.e. no paging of the UE using SUPI is allowed, and paging occasions use temporary identifier
- Use of 5G Global Unique Temporary Identifier (5G-GUTI) with stricter temporary subscription identifier refreshment requirements
- Initial NAS message ciphering

In addition, 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.

2.6 RAN Security

- Support of user plane 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 gNB supports a verify software updates function before installation
- Support PDCP Counter check to detect maliciously inserted packets.

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.

- IAB uses the CU/DU architecture, the IAB operation via F1 (between IAB-donor and IAB-node) is invisible to the 5GC.
- IAB performs relaying at layer-2, supports multi-hop backhauling and dynamic topology updates.

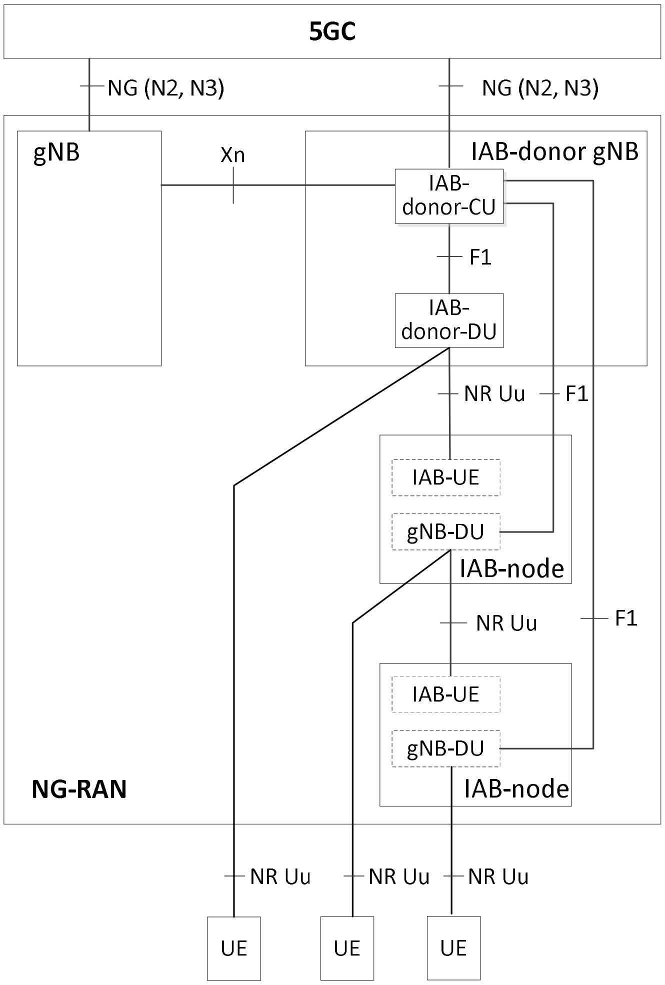


Figure 1 – IAB architecture for 5GS

- The IAB-node (IAB-UE)

  - Supports ciphering, integrity protection and replay protection of NAS-signalling between the IAB-UE and the 5GC and IAB-UE and the IAB donor.
  - IAB-node (IAB-UE) and the 5GC 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 user plane supports confidentiality, integrity and replay protection for the user plane
  - F1-C and management traffic carried over the 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

- NFs support HTTP/2 over 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 allow 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 PLMN
- Between PLMNs, interconnect security is provided for all service based signalling traffic, which solves the 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
- The new SBA security architecture in Figure 2which illustrates the different sets of security features for the following security domains as 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)

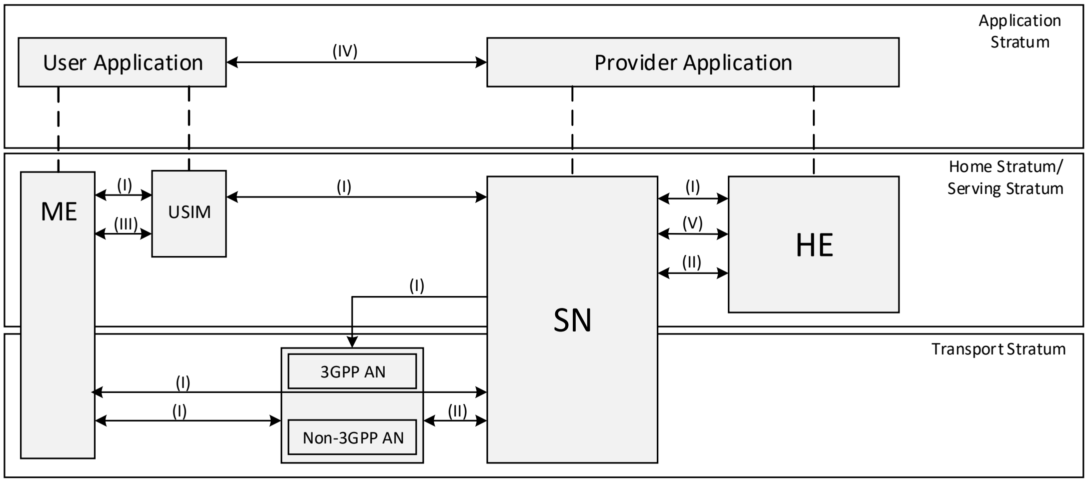


Figure 2– Overview of the security architecture

2.8 Roaming Security

2.8.1 Roaming interfaces between PLMNs except for N32

- Shall be confidentiality, integrity, and replay protected
- NDS/IP shall be used as, unless security is provided by other means, e.g. physical security
- Origin of messages shall be authenticated.

2.8.2 Secure Edge Protection Proxy (SEPP)

- The Security Edge Protection Proxy (SEPP), a non-transparent proxy, protects the messages that are sent over the N32 interface between Service Consumers and Service Producers.
- The SEPP implements application layer security for all the service layer information exchanged between two NFs across two different PLMNs and supports topology hiding of the home network from the roaming partners and IPX service providers.
- See sections 3.1 and section 8.3 for more details on the SEPP and for the inter-PLMN signalling message flow over the N32 interface.

2.9 5GS-EPS Interworking Security

- Security for seamless mobility between Evolved Packet System (EPS) and 5G system
- Addressed for different UE connected states (i.e. security handling in state transition)
- Support for legacy security measures for core network messages i.e. SS7, 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 (EDCE5)

- EDCE5 = 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 New Radio (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)

- 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 recieving 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 security should use the 3GPP Security aspects of Common API Framework (CAPIF) in TS 33.122 or equivalent security.

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

- Redundant user plane paths based on dual connectivity.
- The UP security policy of the two redundant PDU sessions has the same setting for encryption and integrity protection.
- Redundant transmission of the PDU sessions on the 5GC internal N3 interface, see Figure 3, and for roaming users, on the N9 interface with external roaming partners
- NDS/IP to protect redundant data transferred via the two PDU sessions over the N9 interface.

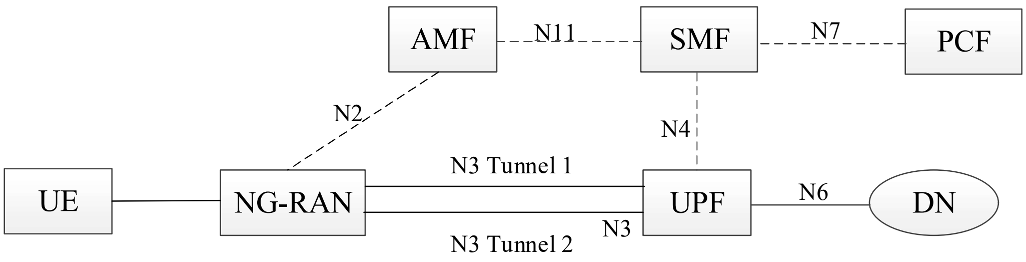


Figure 3 – Redundant transmission with two N3 tunnels between the UPF and a single NG-RAN node

2.14 Security For Time Sensitive Communications (TSC)

- In Release 16, the 5G System supports TSC as defined in IEEE 802.1 Working Group Time Sensitive Networking (TSN) standards like IEEE 802.1AS-Rev [92][92] as depicted in Figure 4.
- Access security for a TSC-enabled UE
- Protection of user plane data in TSC including gPTP control messages.

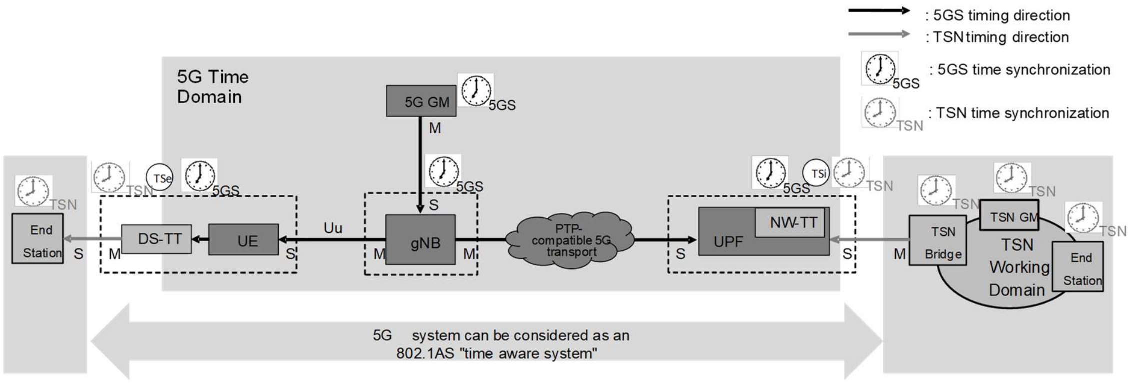


Figure 4 – 5G system modelled IEEE 802.1AS compliant for TSN time synchronization

2.15 Security for 5GLAN services

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

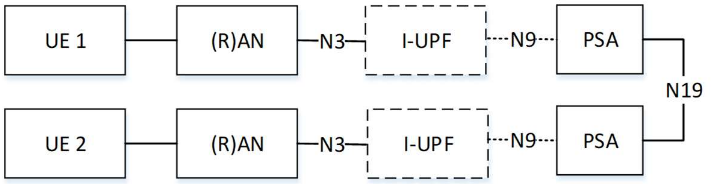


Figure 5 – N19-based user plane architecture in non-roaming scenario

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

- Security of trusted non-3GPP access to a 5GC 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 in Figure 6.

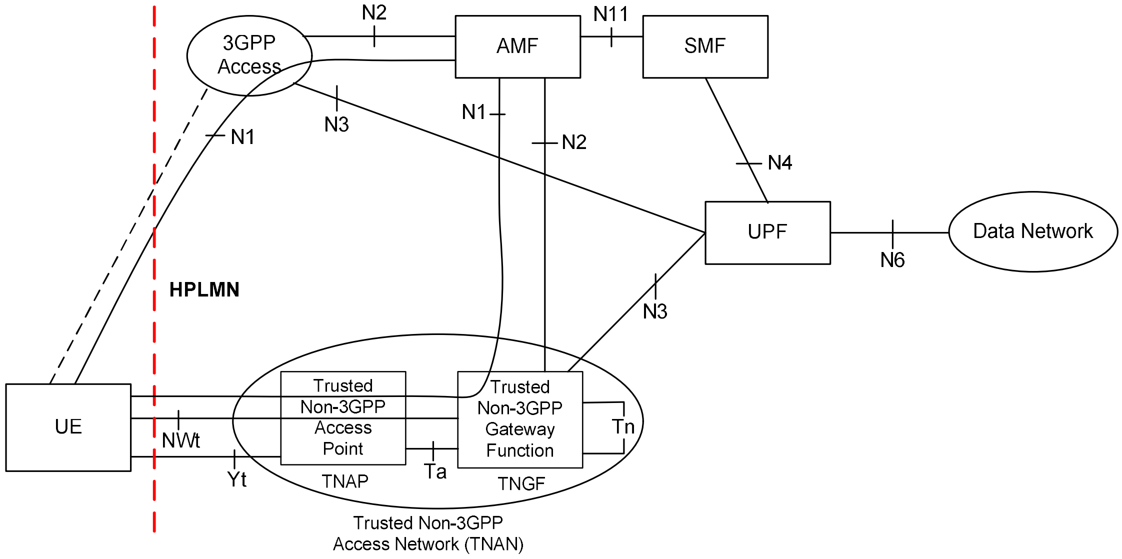

3GPP Access
N2
AMF
N11
SMF
N1
N3
N1
N2
N4
HPLMN
UPF
N6
Data Network
N3
UE
Trusted Non-3GPP Access Point
Trusted Non-3GPP Gateway Function
Tn
NWt
Yt
TNAP
Ta
TNGF
Trusted Non-3GPP Access Network (TNAN)

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

- UE registers to the 5GC 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 user plane 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 5GC 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.

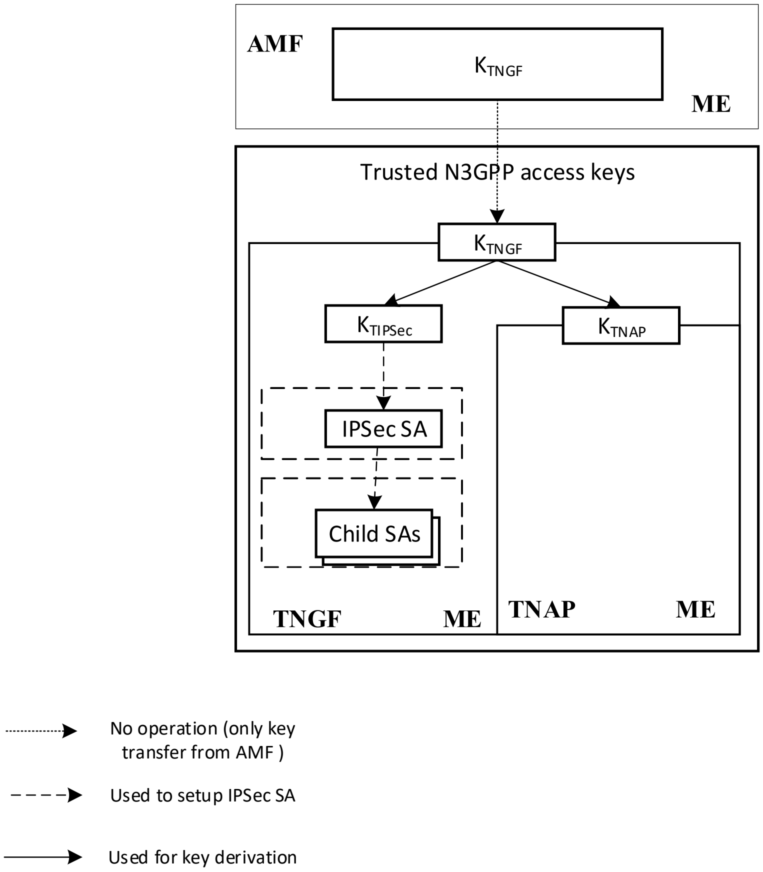


Figure 7 – Key hierarchy for trusted non-3GPP access

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 the 5G Core Network CP and UP functions via 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 Residential Gateway (5G-RG), see Figure 8, or Fixed Network Residential Gateway (FN-RG), see Figure 9, can access the 5GC via the N3IWF or via the TNGF.

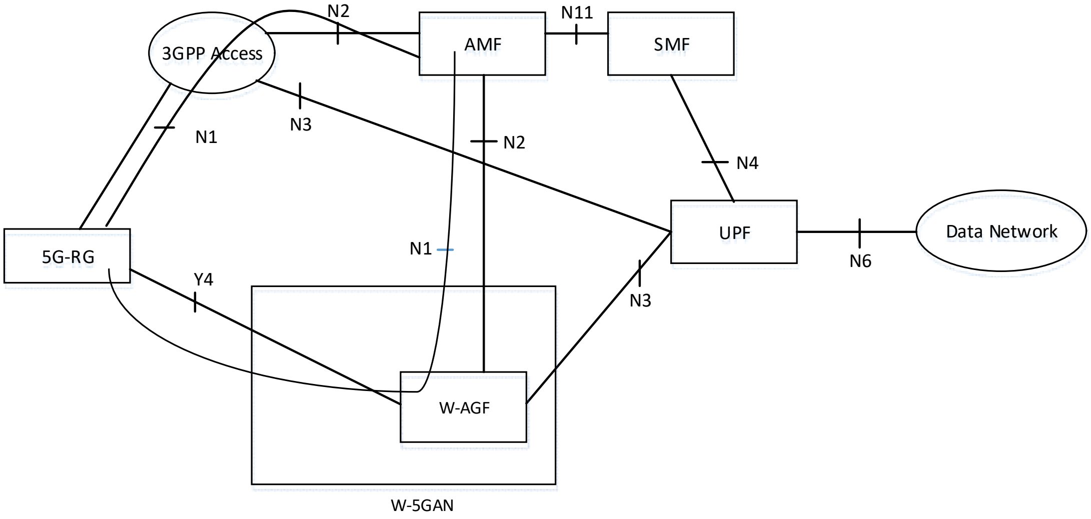


Figure 8 – Non-roaming architecture for 5GC for 5G-RG with W-5GAN and NG RAN

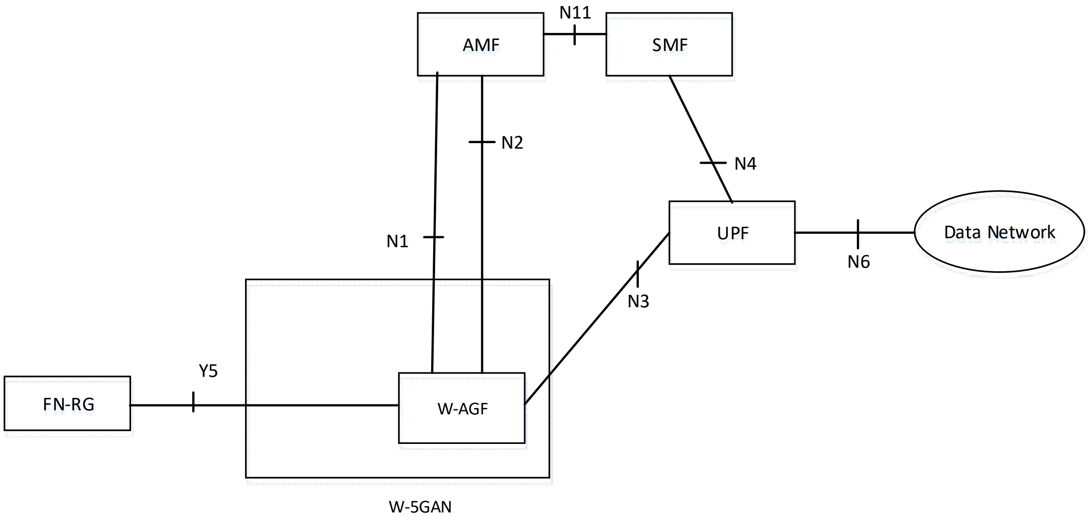


Figure 9 – Non-roaming architecture for 5GC for FN-RG with W-5GAN and NG RAN

- 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 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.
- Integrity, confidentiality, and replay protected.

2.18 UE Security Visibility and Configurability

- UE provides the following security information to the applications in the UE (e.g. via APIs), on a per 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)
  - Serving network identifier

- UE supports a Man Machine Interface to individually disable/enable ME's radio technologies, regardless of PLMNs such as GSM/EDGE, WCDMA, 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/disallow are at least GSM/EDGE, WCDMA, E-UTRA, and NR

2.19 Cryptographic Enhancments

- TLS Profile:
  - Support in OCSP Status extention
  - 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)RSA Digital Signature – no longer recomanded 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.

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.
- Support for AAA Server-side Network Slice-Specific Re-authentication and Re-authorisation procedure.
- Support for AAA Server triggered Slice-Specific Authorisation Revocation.
- Security for network slices management:
  - Support for mutual authentication between the management service consumer and the management service producer using TLS, based on either 1) client and server certificates or 2) pre-shared keys for TLS 1.2 or TLS 1.3
  - TLS-based protection of OAM interactions between the management service consumer and the management service producer
  - Support for OAuth-based authorization and local policy authorization of management service consumer's requests.
- The core network should support slice specific authorisation and authentication.

See Section 13 for more details about Network Slicing.

3 New Elements and Functions in 5G Security Architecture

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

- The entity sitting at the perimeter of the PLMN network to interconnect with another PLMN directly, via IPX providers or roaming hubs
- Implements application layer security for all the signalling messages exchanged between any two NFs across two different PLMNs and provides protection against eaves dropping on sensitive information and replay attacks
- Provides end-to-end authentication, integrity and confidentiality protection via signatures and encryption of all HTTP/2 roaming messages.
- Offers key management mechanisms for setting the required cryptographic keys and performing the security capability negotiation procedures.
- Performs message filtering and policing, topology hiding and validation of JSON objects including cross-layer information checking with address information on the IP layer.

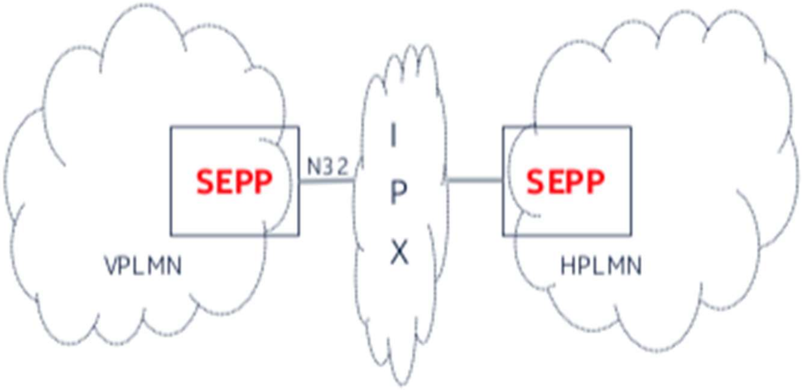


Figure 10 – New SEPP and N32 Interface for 5G inter-operator working

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, where security functions were introduced many years after the 4G/3G/2G technology had already been standardised and deployed. Please refer to section 11 for more details.

3.2 AMF: Access and Mobility Management function

- 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)

- Serves as the anchor for security in 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

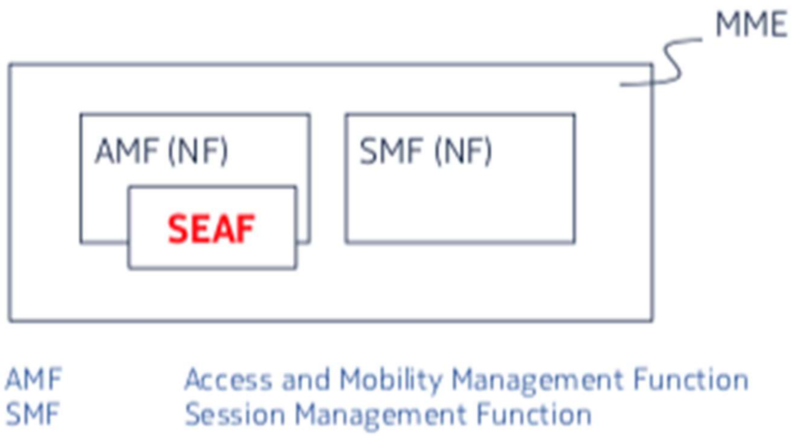

MME
AMF (NF)
SEAF
SMF (NF)
AMF Access and Mobility Management Function
SMF Session Management Function

Figure 11 – New SEAF as anchor for security in 5G

Note: The MME is the related functional component in an LTE Core Network (CN).

3.4 AUSF: Authentication Server Function (in home network)

- 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)
- 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 Release 16, support for Network Slice-Specific Authentication and Authorisation. Release 15 introduces network slicing without authentication

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 12 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 subscription permanent identifier (SUPI).
- Provides 5G home environment (HE) AV to the AUSF

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

- SUCI (concealed subscription identifier) -> SUPI

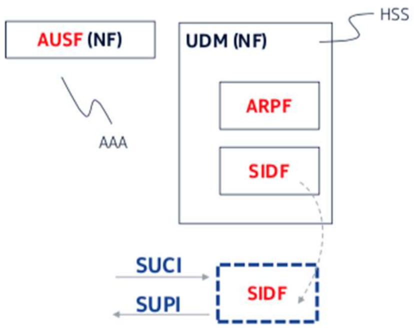


Figure 12 – New elements introduced in 5G for the authentication vector working between SUCI and SUPI

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 SIDF (Subscription Deconcealment Function 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 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

- 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

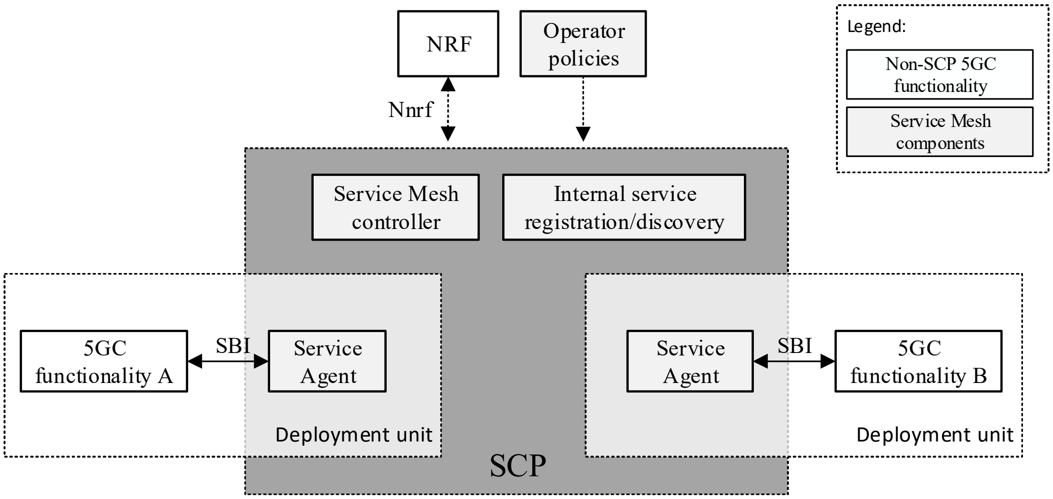


Figure 13 – SCP Service mesh co-location with 5GC functionality

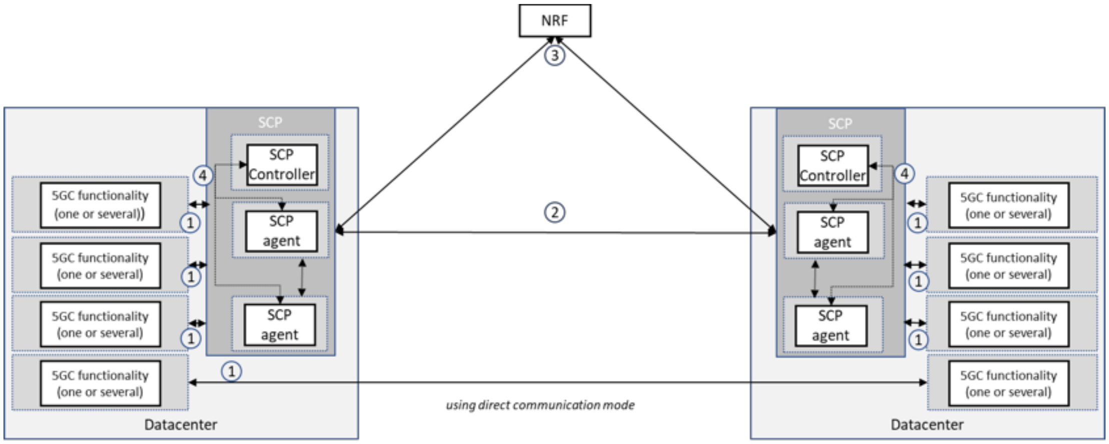

NRF
3
SCP
SCP Controller
4
5GC functionality (one or several))
1
SCP agent
5GC functionality (one or several)
1
5GC functionality (one or several)
1
SCP agent
5GC functionality (one or several)
1
Datacenter
2
using direct communication mode
SCP
SCP Controller
4
5GC functionality (one or several)
1
SCP agent
5GC functionality (one or several)
1
SCP agent
5GC functionality (one or several)
1
5GC functionality (one or several)
Datacenter

Figure 14 – Overview of SCP deployment

3.8 IPUPS: Inter PLMN UP Security

- Operators can deploy UPFs with IPUPS functionality at the network border to protect against invalid inter PLMN N9 traffic in home routed roaming scenarios as in Figure 15.

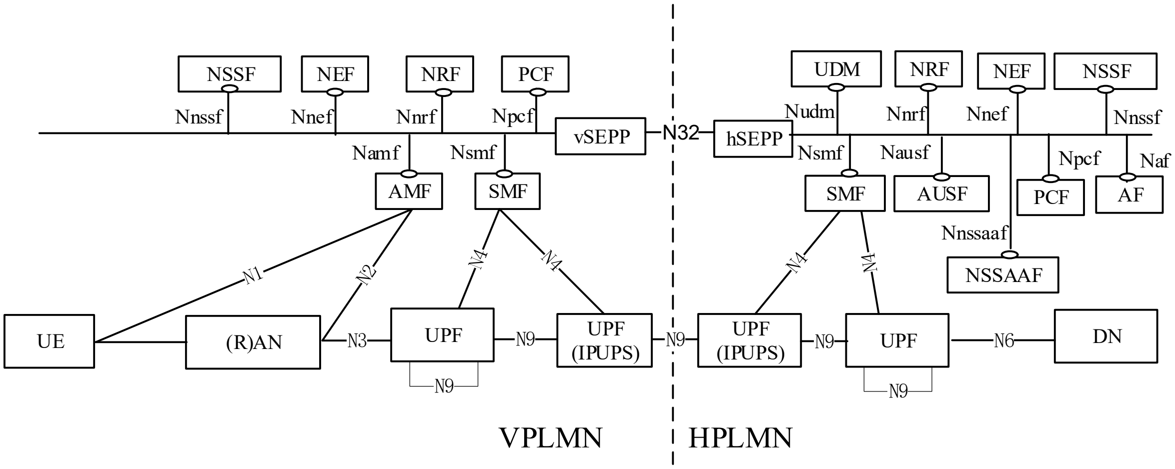


Figure 15 – Roaming 5G System architecture - home routed roaming scenario in service-based interface representation employing UPF dedicated to IPUPS

- IPUPS discards malformed 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

- N58: Reference point between AMF and the NSSAAF
- N59: Reference point between UDM and the 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 an a AAA proxy (AAA-P).
- NSSAAF support AAA-S triggered Network Slice-Specific Re-authentication and Re-authorisation and Slice-Specific Authorisation Revocation
- Relay EAP messages towards a AAA-S or AAA-P and performs protocol conversion as needed.

Notify 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 13.

4 5G Enhancements in Subscription Identifier Privacy

4.1 SUPI and SUCI

The Subscription Permanent Identifier (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 the encrypted SUPI that includes the Mobile Country Code (MCC) and Mobile Network Code (MNC) and the encrypted Mobile Subscription Identity Number (MSIN), which is encrypted with the 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.

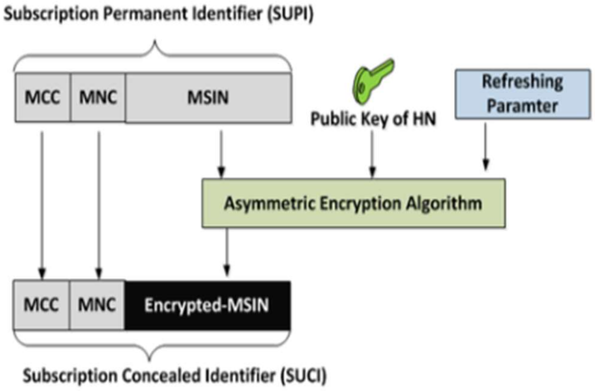

Subscription Permanent Identifier (SUPI)
MCC
MNC
MSIN
Public Key of HN
Refreshing Paramter
Asymmetric Encryption Algorithm
MCC
MNC
Encrypted-MSIN
Subscription Concealed Identifier (SUCI)

Figure 16 – Encryption mechanism from SUPI to SUCI

4.2 5G-GUTI Refresh

It is mandatory to refresh a 5G Globally Unique Temporary Identifier (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 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) to retrieve the subscriber identity by forcing the UE to attach to the Rogue base Station (RBS) or attach to the real base station while tracking the unencrypted traffic over the air. This only works if the 5G NR is supported by a 5GC. In a non-standalone scenario, with a 4G CN, this protection is not available.

In addition, 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

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

5.1 Authentication Confirmation

As part of authentication, the UE computes a cryptographic checksum (*RES) that binds the challenge (RAND) issued by the home network to the USIM as well as the name of the serving network as seen by the UE. This checksum is sent to the visited network which may forward it to the home network. 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, the home network responds with an "authentication confirmation", message 10 in Figure 6.1.3.2-1 in TS 33.501 [1], i.e. an indication on whether or not the checksum is correct.

The goal of this authentication confirmation is to combat fraud, so a missing or failed authentication enables the home network to deny network access. Therefore, the visited network should wait for message 12 in Figure 6.1.3.2-1 in TS 33.501 [1][1] before providing service to a UE because the home network could still signal an authentication failure. A MNO could feed missing/failed authentication confirmation into their anti-fraud systems and/or other signalling functions in order to prevent service for UEs where confirmation is not achieved. If there is a different outcome with 5G AKA, there is either a technical error, or one party is 'cheating'.

5.2 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 "Subscriber Identity Deconcealment Function (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.

5.2.1 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 control plane SOR solution that allows the HPLMN to direct the UE during or after registration on the VPLMN. Details on the interfaces and how the registration process occurs in a 5G System (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][31] and 3GPP TS 24.501 (Rel.15) [26], and the steering of roaming 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].

5.2.2 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, a 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 prioritise 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.

5.2.3 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.

5.3 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:

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.

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. Then the UE can use the 5G security procedures with the transfer of the SUCI encryption of the SUPI executed by the logic within the UE.

   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.

3. **5G UICC with USIM application –** The encryption of the SUPI is executed by the logic inside the 5G UICC.

   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.

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.

5.4 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. These features need to be implemented by device manufacturers, 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.

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][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 operating system.

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.

5.5 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 RADIUS protocol, where the length of the user name 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.

5.6 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][105] and will be covered in subsequent versions of of the LTE Roaming guidelines in GSMA PRD IR.88 [10] and the 5GC 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 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.

6 Increased Home Control

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.

6.1 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 a 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 Multimedia Priority Service (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][106] that are common across two or more mission critical services:

- **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 mission critical services 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, there may be an additional need to differentiate between sorts of roaming traffic given that, more frequently, operators use partners' networks for M2M and IoT services. This may include services with very critical service characteristics that may require a specific treatment to ensure the roaming traffic is rerouted via other resources.

8 Using Internet Protocols within 5G Core

8.1 3GPP Reference

There will be significant changes to the architecture and communication protocols with the introduction of 5G. 3GPP decided to make use of protocols from the IT world. This will allow the 5G Core systems to be virtualised in virtualisation environments that were created for the IT world because 3GPP recognised that telco protocols and the architecture of the mobile network, to date, are not well supported by existing virtualisation environments. 3GPP expects to simplify use of existing virtualisation environments by taking this step.

As a result, 3GPP's architecture group SA2 decided to move to the new Service Based Architecture (SBA). That means all the Network Functions (NF) of the 5GC will be connected via a service bus. For more details see the 5G architecture specification 3GPP TS 33.501 [1] and in particular figure 4.2.4-1.

3GGP CT3 and CT4 concluded on the use of standard Web protocols for the Service Based Architecture (SBA) of 5GC for Release 15.

The 5G SBA Network Stack is further detailed in 3GPP TS 33.501 [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
- JSON (see IETF RFC 7159 [4]) as the serialisation protocol
- To apply a RESTful framework for the APIs design whenever possible and use custom methods otherwise;
- To support notification with two HTTP client-server pairs;
- The OpenAPI 3.0.0 as the Interface Definition Language.

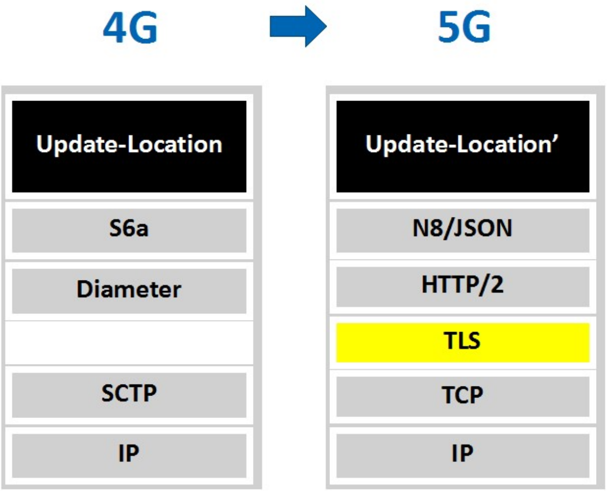


Figure 17 – Use of protocol stacks in 4GCN and 5GC

Note: This diagram is for illustration purposes only. Strictly speaking there is no Location Update message in 5G and, instead, the Nudm_UECM_Registration is used to update the HPLMN about location changes.

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][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 8.8. 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[1], will have to manage the increased scope of these protocols. Once located, the time to patch for relevant vulnerabilities should be short.

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 will require 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 will become a relatively 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) will 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 SBA and instead are proposing solutions that include a single (or few) certificates that have wildcard identities. This allows the certificate to be used on any NF and reduces the management overhead.

Although this simplified approach will support transport encryption between NFs, it will not be able to validate that an endpoint is a legitimate one. 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 a 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][53], see also the following section 8.3.

8.3 Inter-PLMN Signalling Message Flow Over N32

This refers to the solution for 5G Interconnect Security over the N32 interface between 5GCs with the Security Edge Protection Proxy (SEPP), which is a new protection element introduced into the 5G network architecture, as depicted in Figure 18.

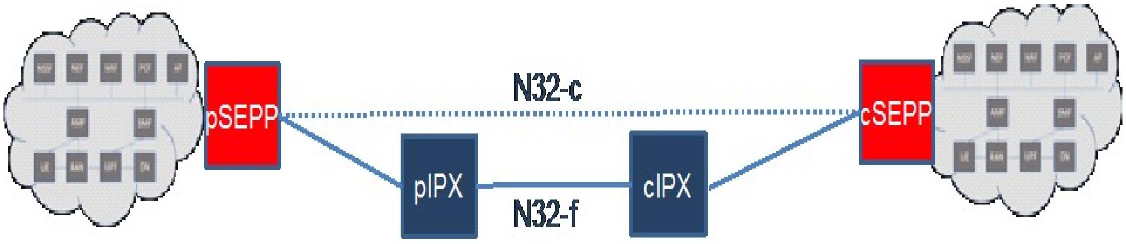


Figure 18 – Overview of N32-c and N32-f interfaces

[1] https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

- SEPP – Provides encryption, integrity and authentication
  - IPX Providers do not have a N32 interface, or SEPPs (formally)
- SEPPs authenticate using TLS (N32 control = N32-c)
  - Negotiate cipher suites for messages over interconnect (N32)
  - Exchange protection policies per roaming partner
- SEPPs encrypt and sign all messages over N32-f using JOSE (JSON web signing encryption)
  - Using JWE – JSON web encryption & signature (with symmetric key from TLS key exchange)

The information transfer over the N32 interface needs to be encrypted as the N32 interface is also used for e.g. the key renewal exchange with the SEAF.

- IPX Providers modify, append and sign changes
- Using signed JSON patches

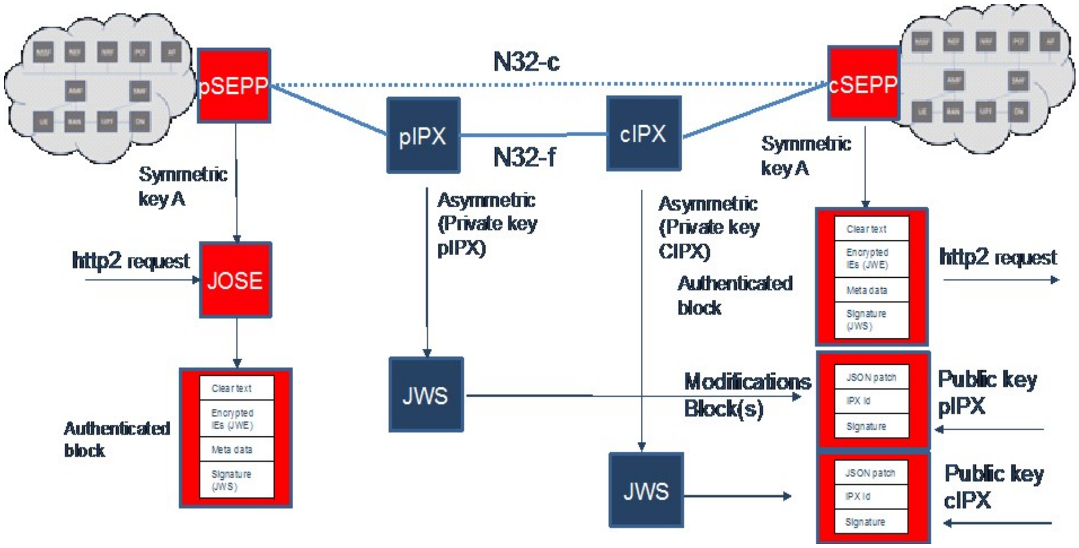


Figure 19 – Message flow over N32-c and N32-f interfaces

The common application errors in Table 2, as defined in section 5.2.7.2 of 3GPP TS 29.500 [85][85], may also be used for the N32-c Handshake service.

Protocol or application Error	HTTP status code	Description
INVALID_API	400 Bad Request	The HTTP request contains an unsupported API name or API version in the URI.
INVALID_MSG_FORMAT	400 Bad Request	The HTTP request has an invalid format.
INVALID_QUERY_PARAM	400 Bad Request	The HTTP request contains an unsupported query parameter in the URI. (NOTE 1)
MANDATORY_QUERY_PARAM_ INCORRECT	400 Bad Request	A mandatory query parameter, or a conditional query parameter but mandatory required, for an HTTP method was received in the URI with semantically incorrect value. (NOTE 1)
OPTIONAL_QUERY_PARAM_ INCORRECT	400 Bad Request	An optional query parameter for an HTTP method was received in the URI with a

Protocol or application Error	HTTP status code	Description
		semantically incorrect value that prevents successful processing of the service request. (NOTE 1)
MANDATORY_QUERY_PARAM_MISSING	400 Bad Request	Query parameter which is defined as mandatory, or as conditional but mandatory required, for an HTTP method is not included in the URI of the request. (NOTE 1)
MANDATORY_IE_INCORRECT	400 Bad Request	A mandatory IE (within the JSON body or within a variable part of an "apiSpecificResourceUriPart" or within an HTTP header), or conditional IE but mandatory required, for an HTTP method was received with a semantically incorrect value. (NOTE 1)
OPTIONAL_IE_INCORRECT	400 Bad Request	An optional IE (within the JSON body or within an HTTP header) for an HTTP method was received with a semantically incorrect value that prevents successful processing of the service request. (NOTE 1)
MANDATORY_IE_MISSING	400 Bad Request	A mandatory IE (within the JSON body or within the variable part of an "apiSpecificResourceUriPart" or within an HTTP header), or conditional IE but mandatory required, for an HTTP method is not included in the request. (NOTE 1)
UNSPECIFIED_MSG_FAILURE	400 Bad Request	The request is rejected due to unspecified client error. (NOTE 2)
NF_DISCOVERY_FAILURE	400 Bad Request	The request is rejected by the SCP because no NF Service Producer can be found matching the NF service discovery factors.
INVALID_DISCOVERY_PARAM	400 Bad Request	The request is rejected by the SCP because it contains an unsupported discovery parameter (i.e. unknown 3gpp-Sbi-Discovery-* header). (NOTE 1)
RESOURCE_CONTEXT_NOT_FOUND	400 Bad Request	The notification request is rejected because the callback URI still exists in the receiver of the notification, but the specific resource context identified within the notification payloadis not found in the NF service consumer.
MODIFICATION_NOT_ALLOWED	403 Forbidden	The request is rejected because the contained modification instructions attempt to modify IE which is not allowed to be modified.
SUBSCRIPTION_NOT_FOUND	404 Not Found	The request for modification or deletion of subscription is rejected because the subscription is not found in the NF.
RESOURCE_URI_STRUCTURE_NOT_FOUND	404 Not Found	The request is rejected because a fixed part after the first variable part of an "apiSpecificResourceUriPart" (as defined in clause 4.4.1 of 3GPP TS 29.501) is not found in the NF. This fixed part of the URI may represent a sub-resource collection (e.g. contexts, subscriptions, policies) or a custom operation. (NOTE 5)
INCORRECT_LENGTH	411 Length Required	The request is rejected due to incorrect value of a Content-length header field.
NF_CONGESTION_RISK	429 Too Many Requests	The request is rejected due to excessive traffic which, if continued over time, may lead to (or may increase) an overload situation.
INSUFFICIENT_RESOURCES	500 Internal Server Error	The request is rejected due to insufficient resources.
UNSPECIFIED_NF_FAILURE	500 Internal Server Error	The request is rejected due to unspecified reason at the NF. (NOTE 3)

Protocol or application Error	HTTP status code	Description
SYSTEM_FAILURE	500 Internal Server Error	The request is rejected due to generic error condition in the NF.
NF_FAILOVER	500 Internal Server Error	The request is rejected due to the unavailability of the NF, and the requester may trigger an immediate re-selection of an alternative NF based on this information. The SCP may also use it, as indication for re-selection.
NF_SERVICE_FAILOVER	500 Internal Server Error	The request is rejected due to the unavailability of the NF service, and the requester may trigger an immediate re-selection of an alternative NF service based on this information. The SCP may also use it, as indication for re-selection.
NF_CONGESTION	503 Service Unavailable	The NF experiences congestion and performs overload control, which does not allow the request to be processed. (NOTE 4)
TIMED_OUT_REQUEST	504 Gateway Timeout	The request is rejected due a request that has timed out at the HTTP client (see clause 6.11.2).
SCP_REDIRECTION	307 Temporary Redirect 308 Permanent Redirect	The request is redirected to a different SCP (see clause 6.10.9).
NOTE 1: "invalidParams" attribute shall be included in the "ProblemDetails" data structure indicating unsupported, missing or incorrect IE(s) or query parameter(s) or 3gpp-Sbi-Discovery-* header(s). NOTE 2: This application error indicates error in the HTTP request and there is no other application error value that can be used instead. NOTE 3: This application error indicates error condition in the NF and there is no other application error value that can be used instead. NOTE 4: If the reason for rejection is a temporary overload, the NF may include in the response a Retry-After header field to indicate how long the service is expected to be unavailable. NOTE 5: If the request is rejected because of an error in an URI before the first variable part of an "apiSpecificResourceUriPart", the "404 Not Found" HTTP status code may be sent without "ProblemDetails" data structure indicating protocol or application error.		

Table 2 – Protocol and application errors common to several 5GC SBI API specifications

The following application errors listed in Table 3 below are specific for the N32-c Handshake service.

Application Error	HTTP status code	Description
REQUESTED_PARAM_MISMATCH	409 Conflict	This represents a parameter mismatch has been detected by the receiving SEPP, i.e. received data-type encryption or modification policy conflict with the one manually configured for the specific roaming partner and IPX provider

Table 3 – Application errors for N32-c

3GPP also improved, in Release 16, use of the internet protocols in the 5G core. In particular, the error codes on the N32-f interface were improved and the following new codes in Table 4 were introduced in section 6.1.5.3.7 of 3GPP TS 29.573 [86] to allow a finer detection what kind of security error occurred.

Enumeration value	Description
"INTEGRITY_CHECK_FAILED"	The integrity check verification on the received N32-f message failed.

"INTEGRITY_CHECK_ON_MODIFICATIONS_FAILED"	The integrity check verification on the modifications block of the received N32-f message failed.
"MODIFICATIONS_INSTRUCTIONS_FAILED"	Failed to apply the JSON patch instructions in the modifications block of the received N32-f message.
"DECIPHERING_FAILED"	The deciphering of the encrypted block of the received N32-f message failed.
"MESSAGE_RECONSTRUCTION_FAILED"	The reconstruction of the original HTTP/2 message from the received N32-f message failed.
"CONTEXT_NOT_FOUND"	The n32fContextId is unknown in the receiving SEPP.
"INTEGRITY_KEY_EXPIRED"	The integrity keys in the receiving SEPP have expired.
"ENCRYPTION_KEY_EXPIRED"	The encryption keys in the receiving SEPP have expired.
"POLICY_MISMATCH"	The encryption policy verification on the received N32-f message has failed, e.g. protected IEs are not ciphered, or unprotected IEs are ciphered.

Table 4 – Enumeration N32fErrorType

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

8.4 Application Layer Security (ALS)

The guidelines for 5G Application Layer Security (ALS) with HTTP/2 and JSON can be found in GSMA PRD FS.36 “5G Interconnect Security” [52][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 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][9] and in FS.21 [17].
- A sketch of the security situation with interworking with Diameter and SS7 is further explained in section 11 “Protection with Parallel Signalling technologies”.

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 supporting 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:

- 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][14].
- Use of Call Detail Records (CDRs) generated by the active elements on the SBA network. However, with CDRs, the visibility of the network actions becoming reactive because the results normally become available after the call releases 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][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 Increased Security Patching

8.8.1 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][59] already includes in Binding Security Requirement (BSR) 17 requirements in “Secure Configuration of Network Elements, Network Services and IPX Services”.

8.8.2 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, operating system, 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 internet of Things (IoT) and machine-to-machine (M2M) devices.

8.8.3 Security of IoT devices

Based on practical experience in MNO networks, these 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.
- 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, patch procedures must exist and the manufacturers must be willing to maintain their software/firmware and provide patches. Furthermore, how to deploy patches and for which types of devices must be defined. Critical decision points include the following questions:

  - Distribution via OTA?
  - Does bandwidth support that?
  - Does battery consumption of constraint devices allow for that?
  - How to treat low-cost IoT devices?

8.9 Sharing Threat Intelligence Information between MNOs

Similar as for SS7 and Diameter as 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][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 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. As this is a new technology for the telecommunication ecosystem, the industry, including the new verticals that use 5G for their communication needs, does not yet know all of the attacks MNOs are likely to face. Therefore, rapid integration of countermeasures against new attack scenarios, based on latest threat intelligence information and analysis, is important to avoid having outdated security protection and giving a false sense of security.

8.10 Additional Security Guidelines

The security architecture of 5GS networks is hierarchical and classified by domain during their design and the following additional security guidelines may be considered:

Additions to SBA API Security

1. Mutual authentication for SBA APIs using both client and server-side certificates.
2. Use of OAuth for SBA API request authorisation and Logging of SBA API requests.
3. Use of load balancing and monitoring capabilities for SBA API requests.
4. Monitoring of SBA API data communications.

Additions to Transport Security

1. Use of certificates for IPsec to secure transport traffic.
2. Hardening of transport network elements (e.g. optical devices).
3. Implement optical-layer encryption.
4. Implement optical-layer intrusion detection.

Management and Orchestration

1. Use of cryptography on all management interfaces for confidentiality, integrity and replay protection.

2. Use of certificate-based authentication on all management interfaces.
3. Use of SDN flow analytics capabilities in SDN controllers.
4. Integration of all management systems with centralised AAA/IAM for authentication and authorisation of administrative users.

Zero Trust Environment – Telco Cloud

1. Use of micro segmentation in telco-cloud as a solution for enforcing zero-trust communications between virtual payloads and hosts.
2. Secure-boot of telco-cloud infrastructure (including host firmware, OS and hypervisor).
3. Integrity checking of virtual payloads before execution.

Additions to Security for End-User Devices

1. Use of certificate-based authentication of IoT devices.
2. Monitoring of device communications and use of network security analytics solutions to detect device security issues.
3. 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 Messaging and Voice

9.1 Short Message Service (SMS)

The following sections apply to 5GS SMS in Release 15 and 16. It is noted that the Release 16 updates have no major impact on SMS Roaming and SMS Interconnect. These are expected to be updated with the Release 17 SMS_SBI work item, as described in 3GPP TR 29.829 [74].

9.1.1 SMS Roaming

The roaming architecture for SMS over NAS (SMSoNAS) is described in 3GPP TS 23.501 [31]. As shown in Figure 20, 5GC signalling for the outbound roaming subscriber between the Visited PLMN and Home PLMN is protected by the SEPP interworking over the N32 interface.

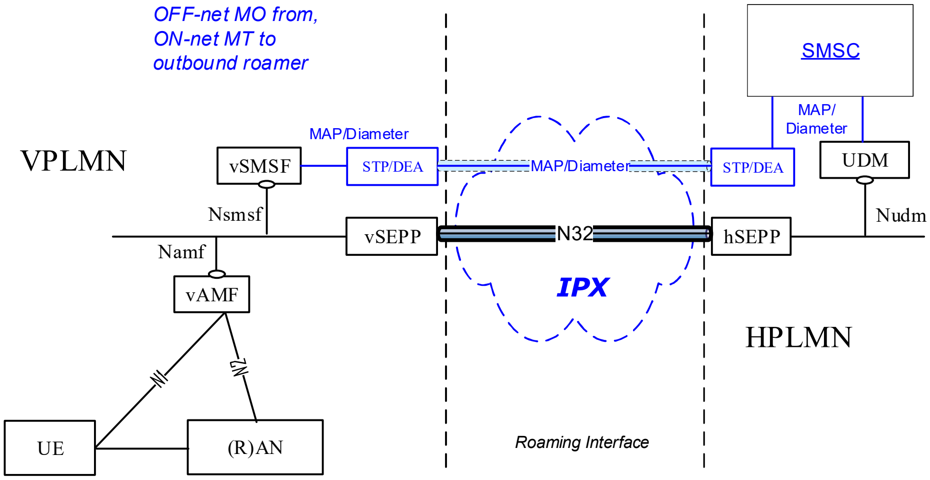


Figure 20 – SMSoNAS Roaming

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 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.

Ideally, SMSoNAS roaming in 5GS should be included within the scope of the SEPP protection over the N32 interface. This will require the SMS roaming operations to be supported over the Service-Based interface. This is being considered for Release-17 as described in 3GPP TR 29.829 [74].

In the case of SMS over IP (SMSoIP) roaming in 5GS, for as long as the outbound roamer continues to roam on IMS, the SMS messaging shall be protected over the UPF N9 Home-Routed connection between the VPLMN and HPLMN, as shown in Figure 21. Otherwise, the roamer's SMS will fallback to SMSoNAS.

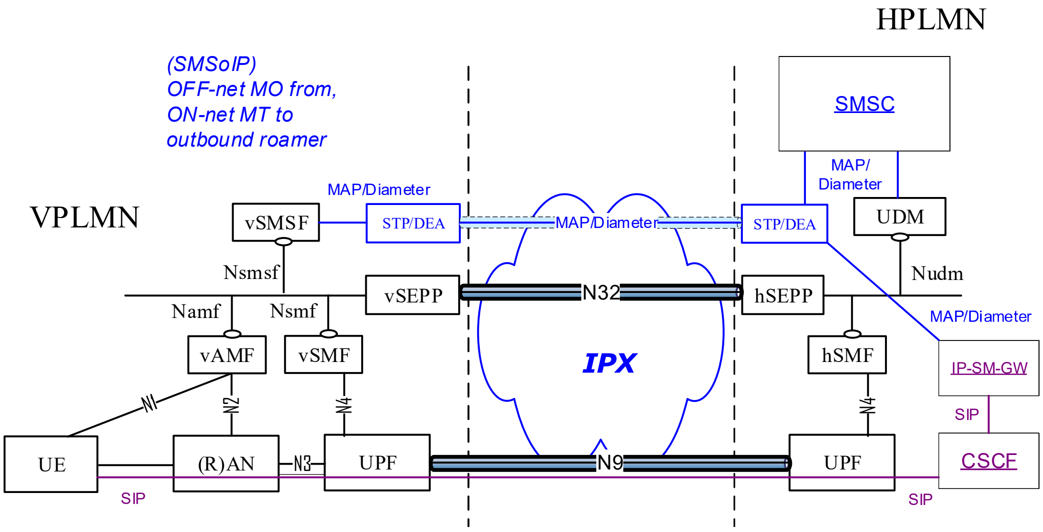


Figure 21 – SMSoIP Roaming

9.1.2 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 22:

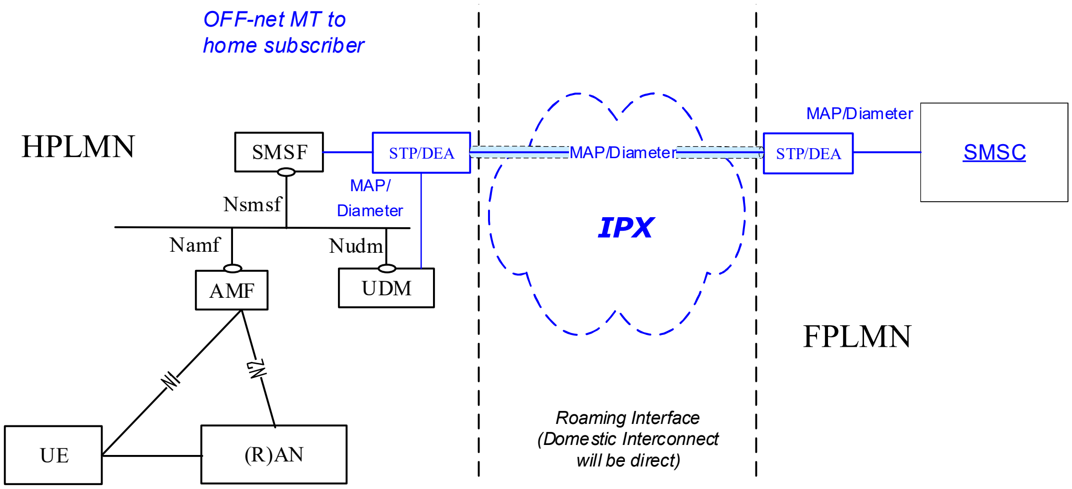


Figure 22 – Inter-operator SMS for Domestic (direct) and International (direct or via IPX) interworking

Consequently, inter-operator SMS in 5GS is not currently supported through the N32 interface and it will not benefit from the same level of protection that is offered by the SEPPs.

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.

Ideally, inter-operator SMS messaging in 5GS should also be included within the scope of inter-PLMN security via the N32 interface, similar to the proposal for SMS roaming. This new design will require 3GPP to consider applying the Service-Based interface for inter-operator SMS, if applicable. This is being considered for Release-17 as described in 3GPP TR 29.829 [74].

9.2 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 23.

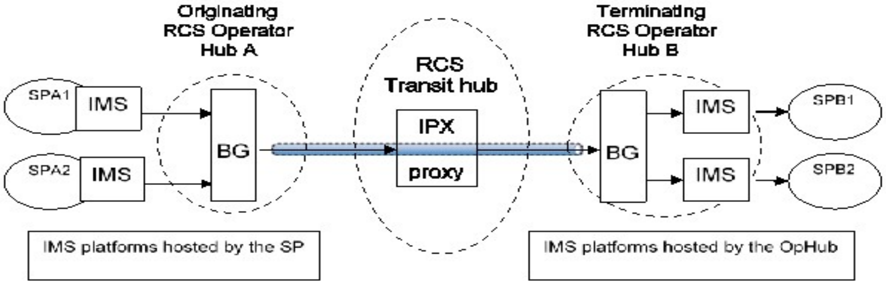


Figure 23 – RCS Technical Architecture, from Figure 5-5 in IR.65 [56][59]

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 IP Multi-Media Subsystem (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 19.16.

9.3 Voice over 5G

Voice quality gained significant ground with Voice over LTE (VoLTE) with the deployment of 4G LTE networks. Voice over 5G (Vo5G) service will build on those advancements as evolved voice systems leverage combined 5G core network elements along with IP Multimedia Systems (IMS), VoLTE enhancements, 5G Evolved Packet Core (EPC) and other 5G New Radio (5GNR) radio access network equipment, such as smart antennas.

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 enhanced mobile broadband (eMBB) services are delivered through 5G Radio and the enhanced LTE/EPC.
2. **Vo5G/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 Vo5G 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. Vo5G will also provide enhanced support for real-time communications including Rich Communications Services (RCS) integration.

Vo5G 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 telepresent robotics are some of the key solution areas that will leverage Vo5G, specifically VoNR.

10 N9 – User Plane Data Transfer with GTP-U

GTP 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 is inherited in 5G SBA.

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

For the user data traffic on the N6 interface to public network or private networks security according to FS.37 [64] is recommended.

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

3GPP Release 15 introduced the SBA for the mobile packet core with control plane (CP) and user plane (UP) separation natively designed within the SBA. The SEPP enables a 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 Inter-PLMN User Plane Security (IPUPS) introduced in 3GPP Release 16 in the UPF itself, and not by a separate network function. It is applicable in 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 Network Domain Security/Internet Protocol (NDS/IP) by means of IPSec with peering partners.

The IPUPS functionality as shown at the network borders on the N9 interface in Figure 24 is based on a principle of detect, correlate and filter incoming GTP-U user plane packets.

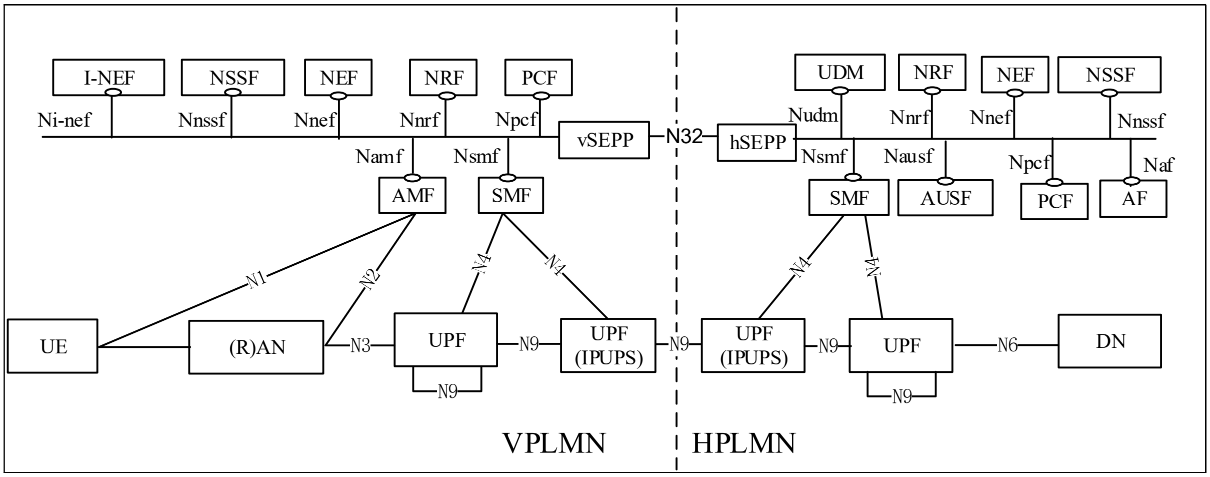


Figure 24 – IPUPS for UP protection on the inter-PLMN N9 interface

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.

10.2 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 user plane tunnel that is unique per subscriber session. If the incoming GTP-U is destined for one 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].

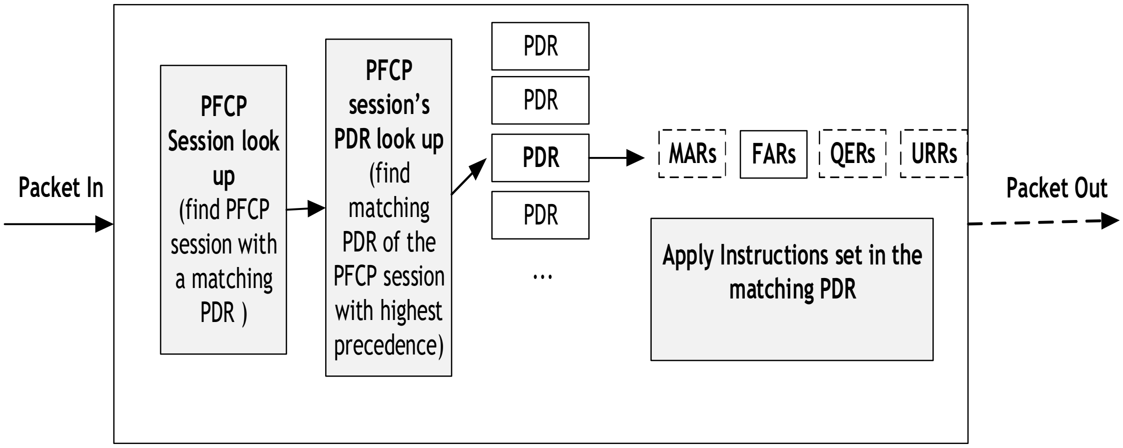

Packet In
PFCP Session look up (find PFCP session with a matching PDR)
PFCP session's PDR look up (find matching PDR of the PFCP session with highest precedence)
PDR
PDR
PDR
PDR
...
MARs
FARs
QERs
URRs
Apply Instructions set in the matching PDR
Packet Out

Figure 25 – Packet forwarding model for PFCP session context lookup

The packet forwarding model performs PFCP session context lookup as outlined in Figure 25.

- 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 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].

11 Legacy Signalling Technologies

11.1 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 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].

11.2 Coexistence of Signalling Protocol Suites

The existence of parallel protocol suites and technologies offers an excellent opportunity for hackers to build attack vectors with access via different signalling connections. Multi-Protocol filtering logic 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 Software Defined Network (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 and 5G + LTE scenarios should be protected. Figure 26 sketches the multi-domain signalling coexistence assuming SS7 is interworked to HTTP2 via Diameter, and reverse.

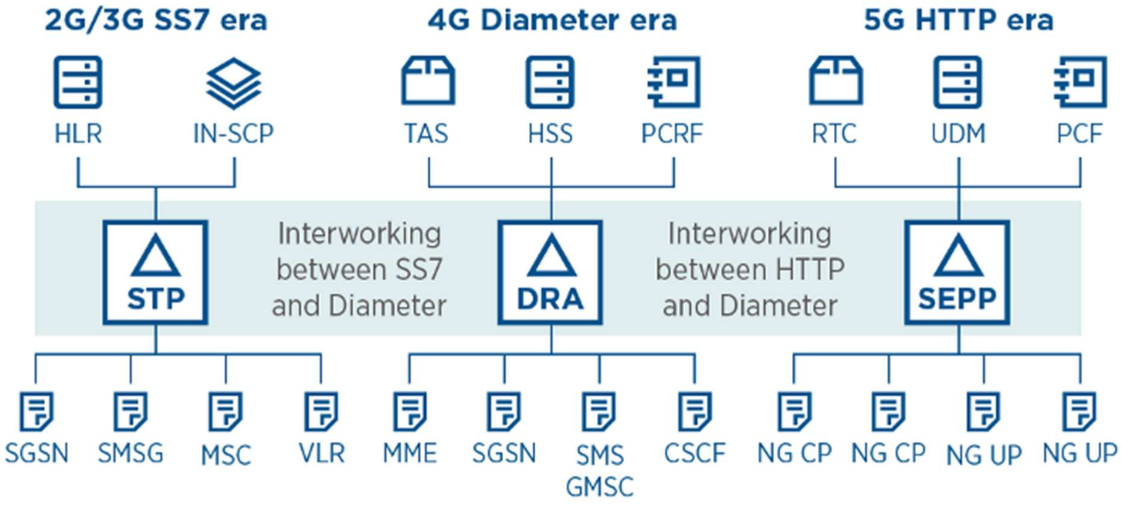


Figure 26 – Multi-domain signaling scenario between different technologies

Figure 27 sketches the protection capabilities with the various combinations of signalling technologies.

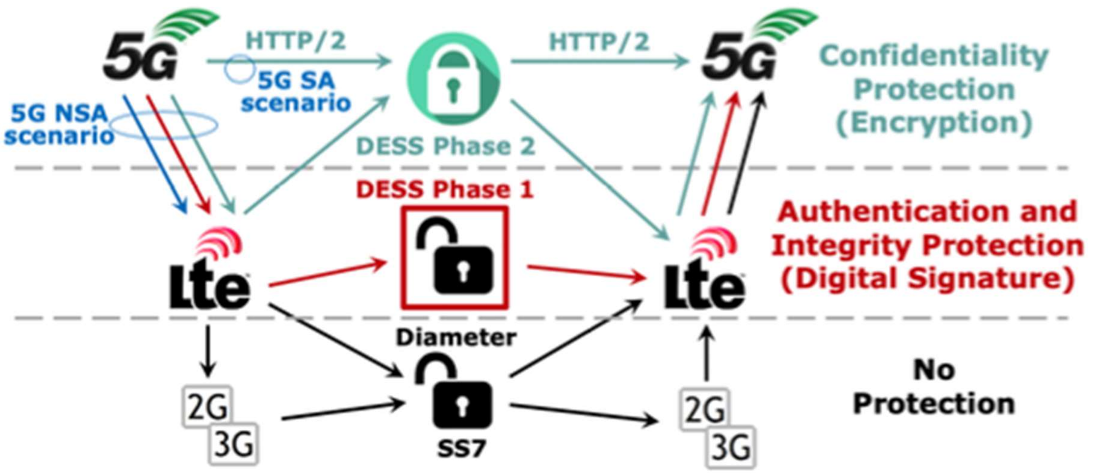


Figure 27 – Protection capabilities for multi-domain signaling between different technologies

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 28 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].

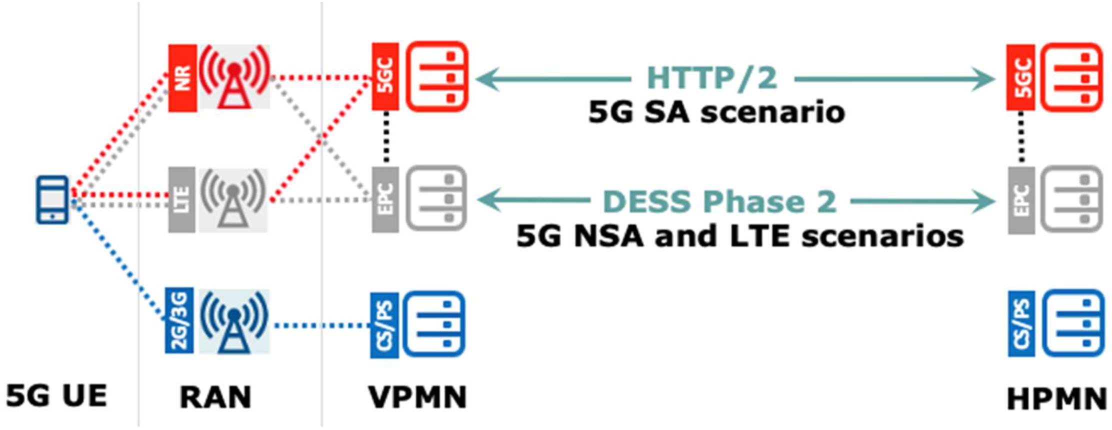


Figure 28 – Confidentiality Protected Roaming Traffic Scenarios

The less protected of the roaming scenarios apply when the roaming traffic is exchanged via either the standard Diameter signalling (without the DESS enhancements) or via SS7 signalling. This is illustrated in Figure 29, 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 signaling as specified in GSMA PRD FS.11 [7].

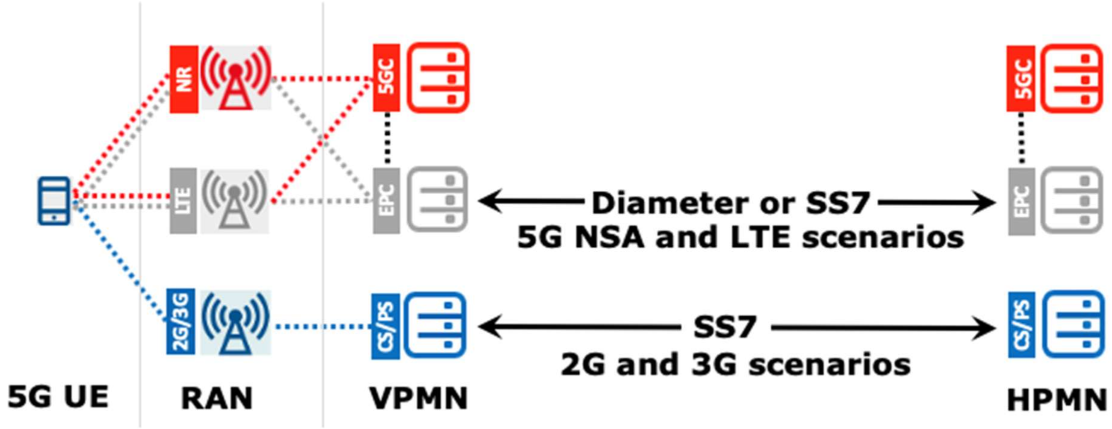


Figure 29 – Least Protected Roaming Traffic Scenarios

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 signaling with the existence of legacy technologies like 2G, 3G, 4G and 5G in combination with the coexistence of SS7, Diameter and HTTP/2 signaling 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.

11.3 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. SMS over NAS 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 cryptogaphic 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, 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 tradeoffs 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.

12 Impact of Cloud on 5G Security

12.1 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 widely accepted MITRE ATT&CK® Framework [79] provides a systematic approach to capture adversarial behavior targeting cloud environments. Examples of cloud associated attacker 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.

12.1.1 Cloud Infrastructure Reference Model (CIRM)

The Cloud Infrastructure Reference Model (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 architctures.

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.

12.1.2 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
- **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

12.1.3 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].

12.2 Virtualisation

In the virtualised world the threats can be more devastating than in the physical world. Those threats could be propagated faster in a virtualised environment. Not only they can induce a number of unknown damages, chain reactions and havoc, but also realise more effects than in the physical environment.

Traditional security software is designed for the physical environment. Virtualisation or containerisation comes with a lack of visibility from host operating system (OS) to guest virtual machines (VMs) or containers, low adoptability to multi-level purpose guest virtual machines or containers, and insufficiency in maintaining the consistency of attack free to guest machines, that can introduce a number of potential vulnerabilities to the network infrastructure.

Under the programmable network environment, NFV entities and SDN controllers differ from the traditional bare-metal network elements by using network softwareisation and centralised control of physical and virtual resources that expose them to the attack opportunities. As a result of intruding the SDN, it might affect the physical and virtual resources, and the entire network to the users i.e. tenants and end-users or consumers.

The network must be designed to ensure its security, that of its users and their traffic against cyber-attacks. Appropriate flexible security mechanisms may be applied.

5G is also intended to deliver an independent control of logical network slices and to provide isolatable network resources for the tenants with their plethoric network services. 5G has a series of isolation types, which must be integrated into the defence mechanism. These types of isolation must be integrated when the end-to-end network slice and supporting network infrastructure is being designed and implemented that can prevent attacks across tenants and tenant's subscribers' information.

12.3 Network Design

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 Operating System (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

12.3.1 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 operating system (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 open source software components that need to be managed properly. The NIST publication NIST SP 800-204B entitled “Attribute -based Access Control for Micro-services-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 fine tuning, 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, NFVI, supports 6 types of virtualisation technologies, the foundations of which are VMs and containers. Containers and microservices are the future 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.

▪ Safeguarding Containers in Multi-Tenant Cloud Environments

The NIST Internal Report (NISTIR) 8320A “Hardware-Enabled Security: Container Platform Security Prototype” [98][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.

12.3.2 Security Guidelines for Storage of UICC Credentials

GSMA PRD FS.43 [90][90] provides security guidelines for the protection of UICC credentials stored within an MNO. Use of a hardware security module (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 a 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 network function virtualisation (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.

13 Network Slicing

13.1 Overview

Network slicing is defined in GSMA's Future Networks document "An Introduction to Network Slicing" [110][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 Control Plane and User Plane 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 TWIF (Trusted WLAN Interworking Function) 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 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).

13.1.1 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 Network Slice instance can be associated with one or more S-NSSAIs, and an S-NSSAI can be associated with one or more Network Slice instances and Multiple Network Slice instances 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 Network Slice instances simultaneously.

13.1.2 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.

13.1.3 Interworking with EPS

A 5GS operating a network slice may need to interwork with the EPS 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 EPS to 5GS, 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 EPS and 5GS.

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.

13.1.4 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 30 illustrates some examples of how network slices can be utilised to deliver communication services, including NSaaS.

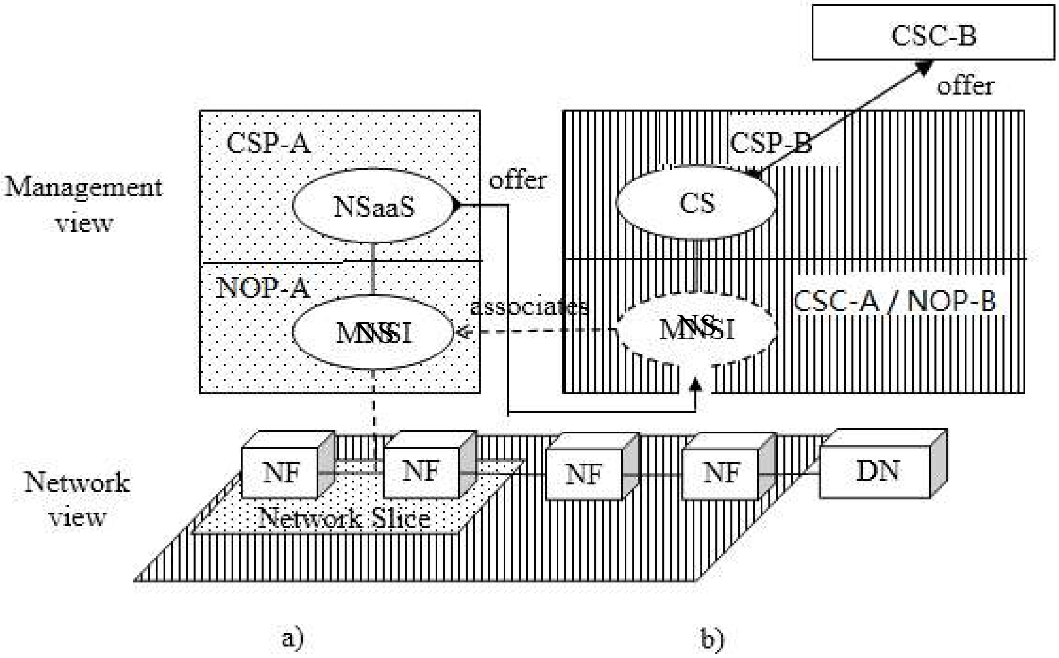


Figure 30 – Examples of Network Slice as a Service (NSaaS), 3GPP TS 28.530 [111]

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.

13.2 Standardised Security Features

13.2.1 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.

13.2.2 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.

13.2.3 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.

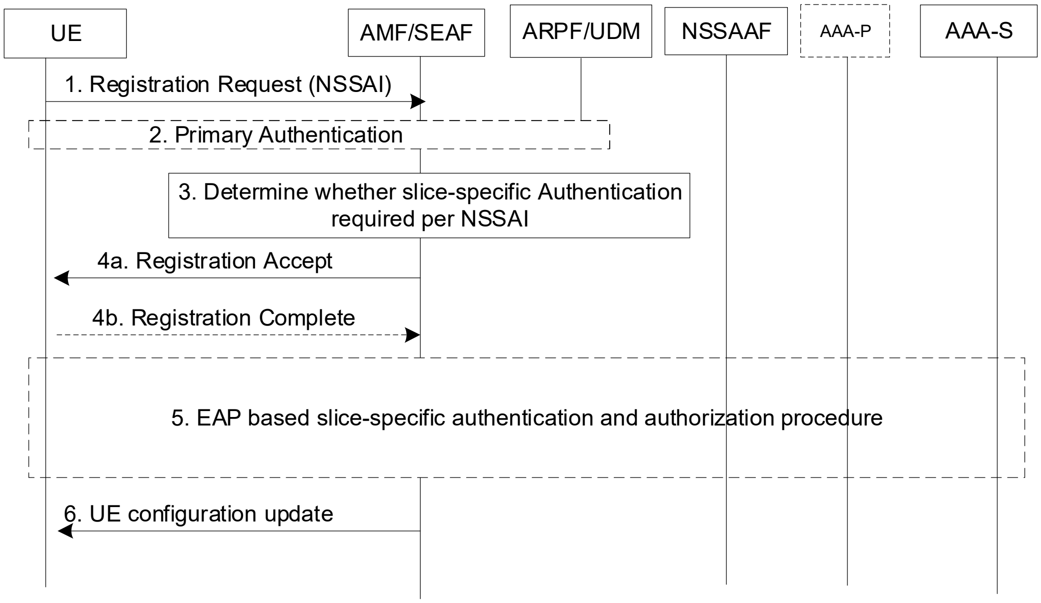

UE
AMF/SEAF
ARPF/UDM
NSSAAF
AAA-P
AAA-S
1. Registration Request (NSSAI)
2. Primary Authentication
3. Determine whether slice-specific Authentication required per NSSAI
4a. Registration Accept
4b. Registration Complete
5. EAP based slice-specific authentication and authorization procedure
6. UE configuration update

Figure 31 – 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.

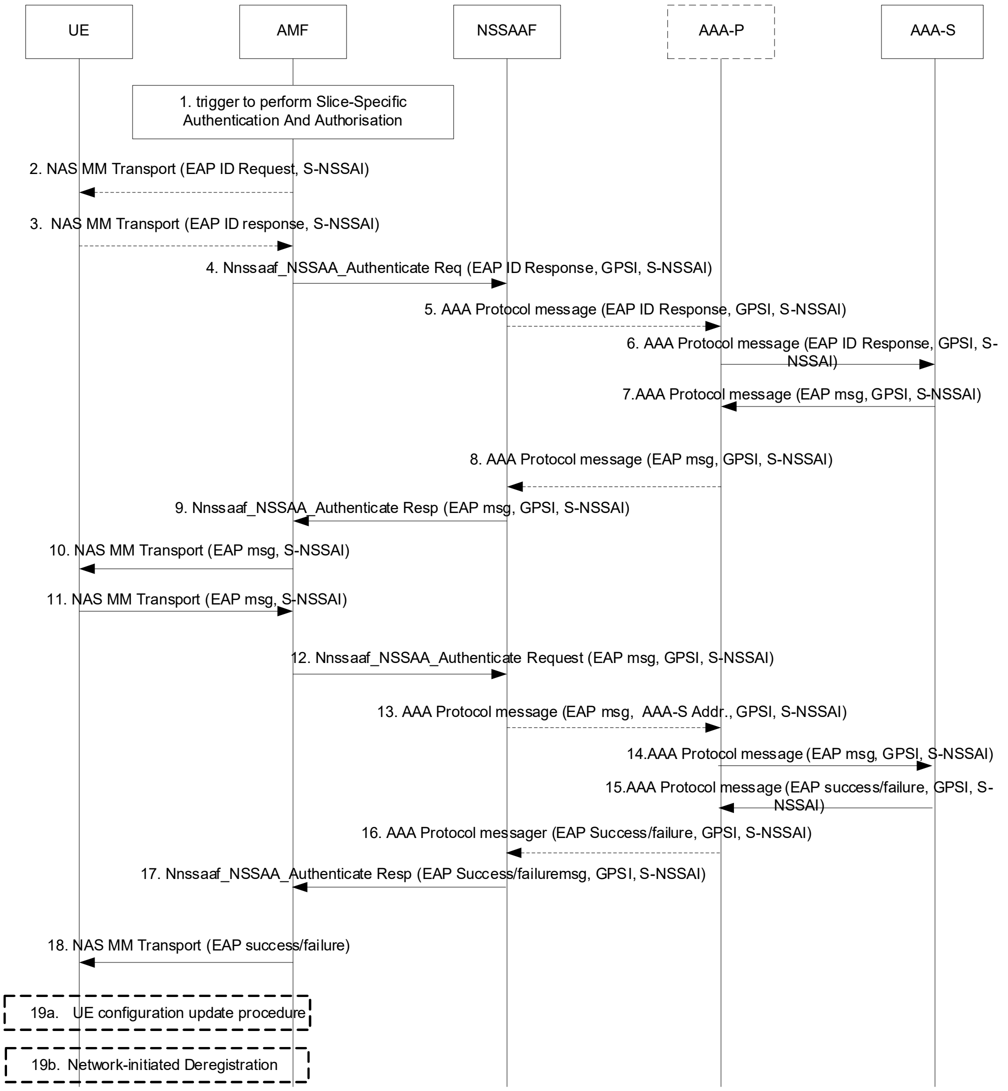

UE
AMF
NSSAAF
AAA-P
AAA-S
1. trigger to perform Slice-Specific Authentication And Authorisation
2. NAS MM Transport (EAP ID Request, S-NSSAI)
3. NAS MM Transport (EAP ID response, S-NSSAI)
4. Nnssaaf_NSSAA_Authenticate Req (EAP ID Response, GPSI, S-NSSAI)
5. AAA Protocol message (EAP ID Response, GPSI, S-NSSAI)
6. AAA Protocol message (EAP ID Response, GPSI, S-NSSAI)
7.AAA Protocol message (EAP msg, GPSI, S-NSSAI)
8. AAA Protocol message (EAP msg, GPSI, S-NSSAI)
9. Nnssaaf_NSSAA_Authenticate Resp (EAP msg, GPSI, S-NSSAI)
10. NAS MM Transport (EAP msg, S-NSSAI)
11. NAS MM Transport (EAP msg, S-NSSAI)
12. Nnssaaf_NSSAA_Authenticate Request (EAP msg, GPSI, S-NSSAI)
13. AAA Protocol message (EAP msg, AAA-S Addr., GPSI, S-NSSAI)
14.AAA Protocol message (EAP msg, GPSI, S-NSSAI)
15.AAA Protocol message (EAP success/failure, GPSI, S-NSSAI)
16. AAA Protocol messager (EAP Success/failure, GPSI, S-NSSAI)
17. Nnssaaf_NSSAA_Authenticate Resp (EAP Success/failuremsg, GPSI, S-NSSAI)
18. NAS MM Transport (EAP success/failure)
19a. UE configuration update procedure
19b. Network-initiated Deregistration

Figure 32 – Network Slice-Specific Authentication and Authorisation procedure TS 23.502 [112][112]

13.3 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 33 elucidates the end-to-end isolation of the network slices in a 5G network.

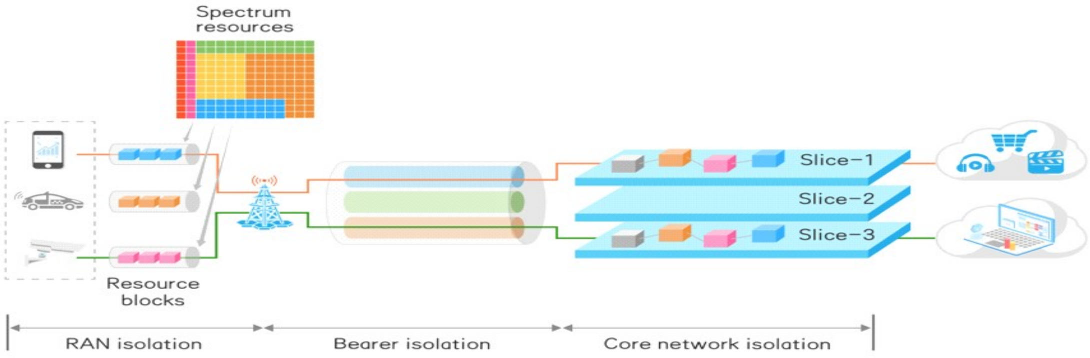


Figure 33 – End-to-end isolation in RAN, TN, and CN of slices in a 5G network

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

Figure 34 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.

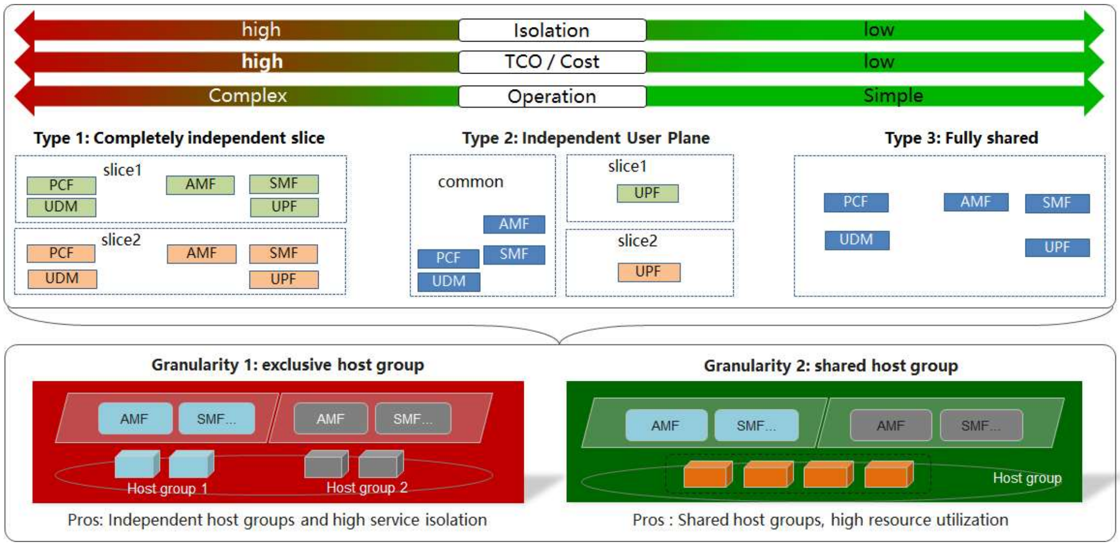

high
Isolation
low
high
TCO / Cost
low
Complex
Operation
Simple
Type 1: Completely independent slice
slice1
PCF
UDM
AMF
SMF
UPF
slice2
PCF
UDM
AMF
SMF
UPF
Type 2: Independent User Plane
common
AMF
PCF
SMF
UDM
slice1
UPF
slice2
UPF
Type 3: Fully shared
PCF
AMF
SMF
UDM
UPF
Granularity 1: exclusive host group
AMF
SMF...
AMF
SMF...
Host group 1
Host group 2
Pros: Independent host groups and high service isolation
Granularity 2: shared host group
AMF
SMF...
AMF
SMF...
Host group
Pros : Shared host groups, high resource utilization

Figure 34 – Slice Security Isolation Models

Figure 35 below depicts possible interactions of various communication service providers with different network slices. As highlighted in Figure 33 (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.

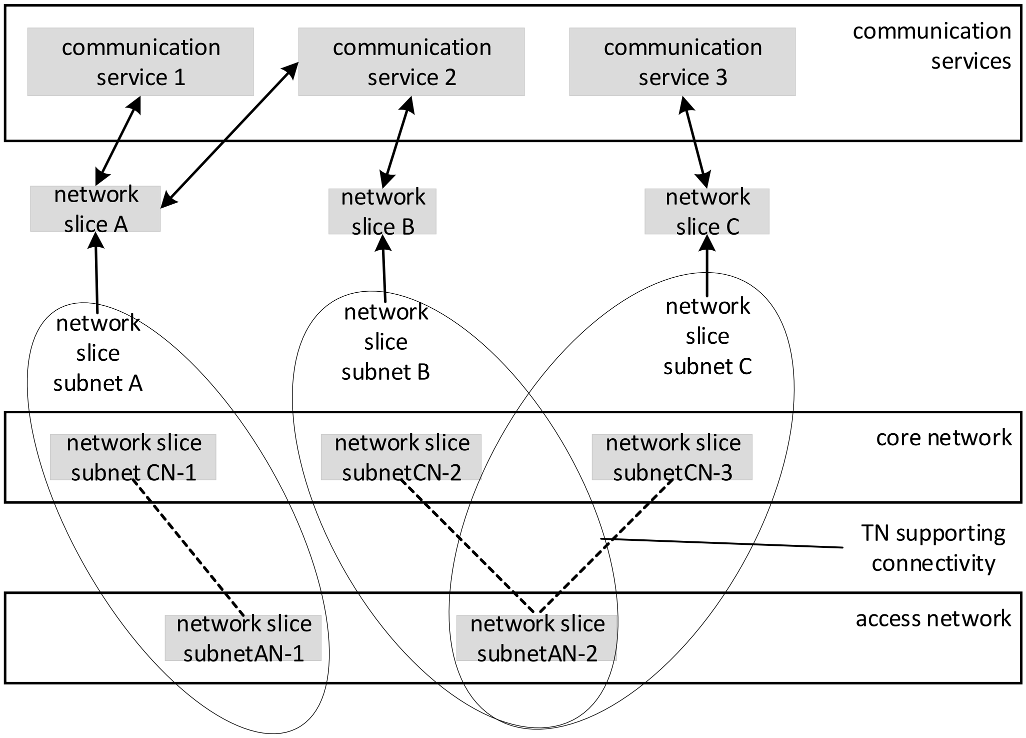


Figure 35 – Communication services provided by multiple network slices, TS 28.530 [111]

13.4 Slice Lifecycle Management

The lifecycle management of network slicing, can be described by four phases Preparation. Commissioning, Operation and Decommissioning as shown in Figure 36 below.

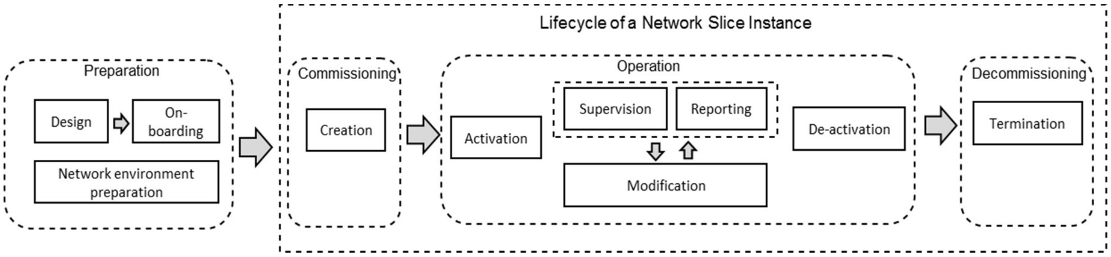


Figure 36 – Management aspects of network slicing, TS 28.530 [111]

A network slice may include non-3GPP parts e.g. data centre network (DCN), transport network (TN), 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 37 below.

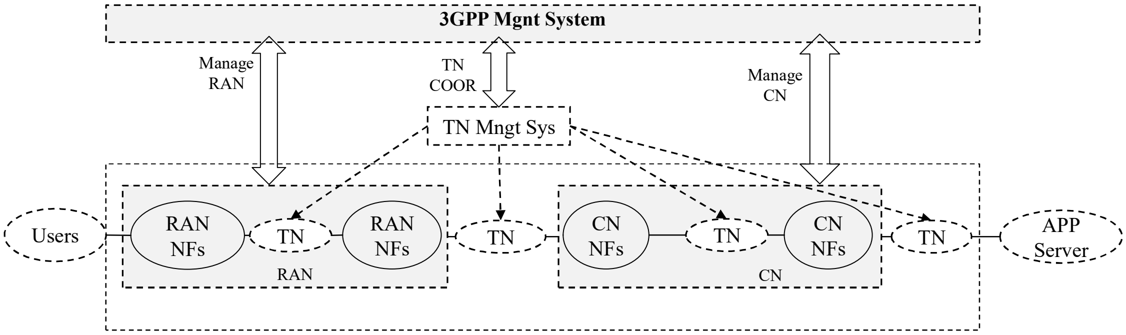


Figure 37 – An example of coordination between 3GPP and Non-3GPP management systems TS 28.530 [111]

13.4.1 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.

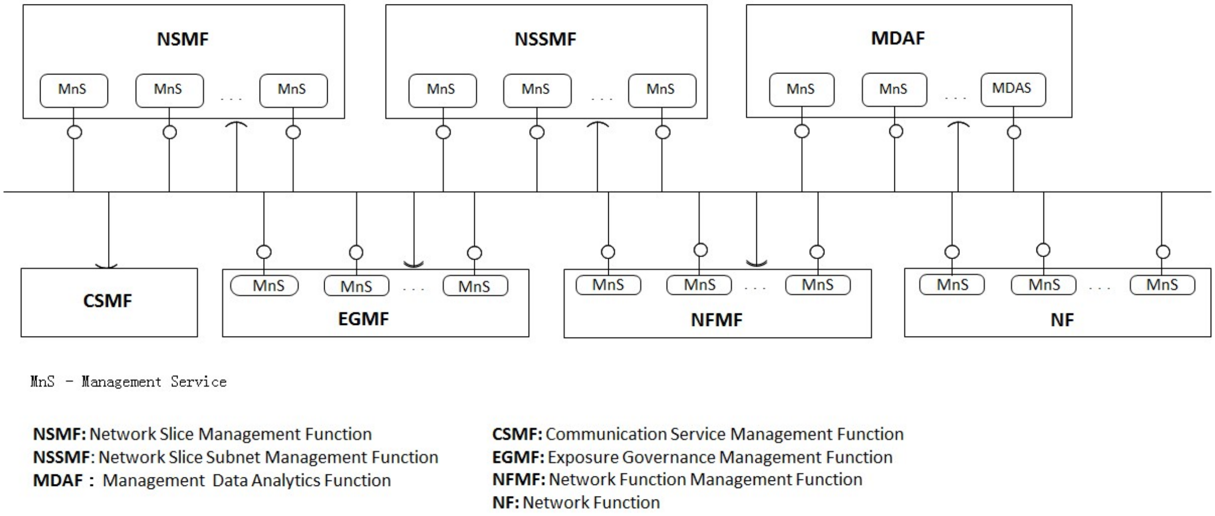

NSMF
MnS
MnS
. . .
MnS
NSSMF
MnS
MnS
. . .
MnS
MDAF
MnS
MnS
. . .
MDAS
CSMF
MnS
MnS
. . .
MnS
EGMF
MnS
MnS
. . .
MnS
NFMF
MnS
MnS
. . .
MnS
NF
MnS - Management Service
NSMF: Network Slice Management Function
NSSMF: Network Slice Subnet Management Function
MDAF : Management Data Analytics Function
CSMF: Communication Service Management Function
EGMF: Exposure Governance Management Function
NFMF: Network Function Management Function
NF: Network Function

Figure 38 – 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.

13.4.2 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 39.

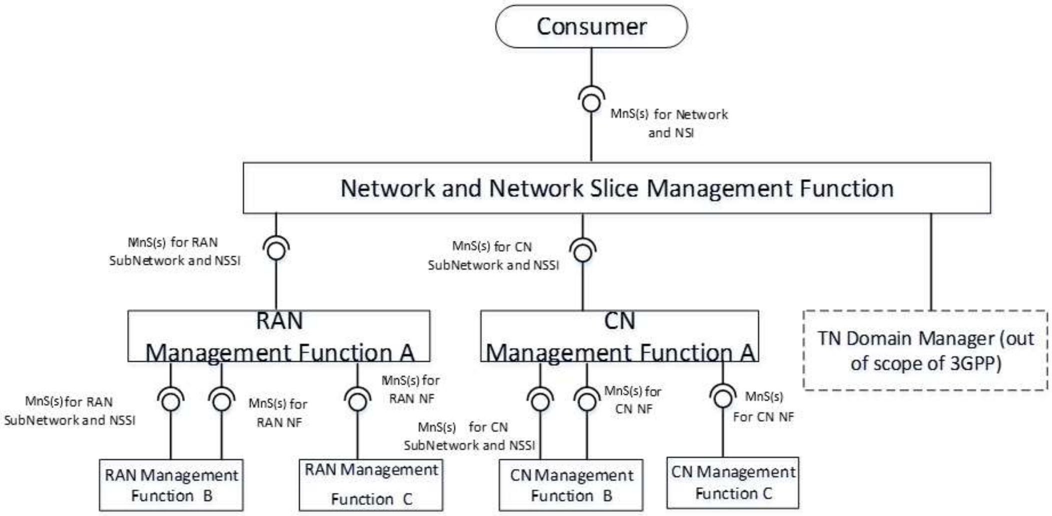

Consumer
MnS(s) for Network and NSI
Network and Network Slice Management Function
MnS(s) for RAN SubNetwork and NSSI
MnS(s) for CN SubNetwork and NSSI
RAN Management Function A
CN Management Function A
TN Domain Manager (out of scope of 3GPP)
MnS(s)for RAN SubNetwork and NSSI
MnS(s) for RAN NF
MnS(s) for RAN NF
MnS(s) for CN SubNetwork and NSSI
MnS(s) for CN NF
MnS(s) For CN NF
RAN Management Function B
RAN Management Function C
CN Management Function B
CN Management Function C

Figure 39 – 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][113] and FS.31 [63][63] that can assist operators identify relevant threats and recommended security and privacy controls.

13.4.3 Management security for network slices

The creation, modification, and termination of a Network Slice Instance (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.

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.

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.

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.

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

14.1 SDN Architecture

Software Defined Networks (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 control plane 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.

14.2 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 40.

- **Application plane:** consists of applications for various network functions such as network management, QoS management and security services, etc.

- **Control plane:** is 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 control plane for dealing with the data packets or traffic flows.

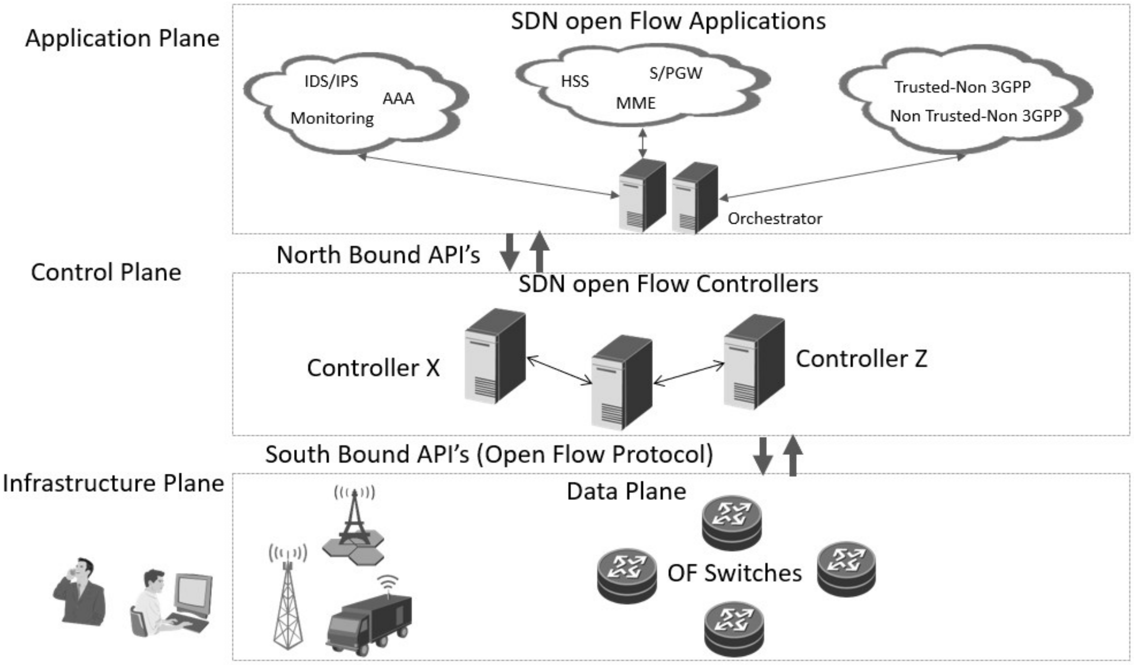


Figure 40 – OpenFlow tiered SDN Architecture

14.3 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, but also provide visibility to other protocols such as TCP and UDP. 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. Existing SIEM solutions were mostly adapted and designed for physical systems and boundaries.

With SDN, it is possible to create network monitoring applications that collect information and make decisions based on a network-wide holistic view. This enables centralised event correlation on the network controller and allows new ways of detecting and mitigating security incidents.

To design an effective Security monitoring system in 5G networks, focus is needed in the following area:

- **Heterogeneity:** analysis of different control and user plane traffic flows over the network domains and new interfaces between Software Defined Mobile Networks (SDMN) and existing networks and identification of related flows in different network domains.

14.4 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.

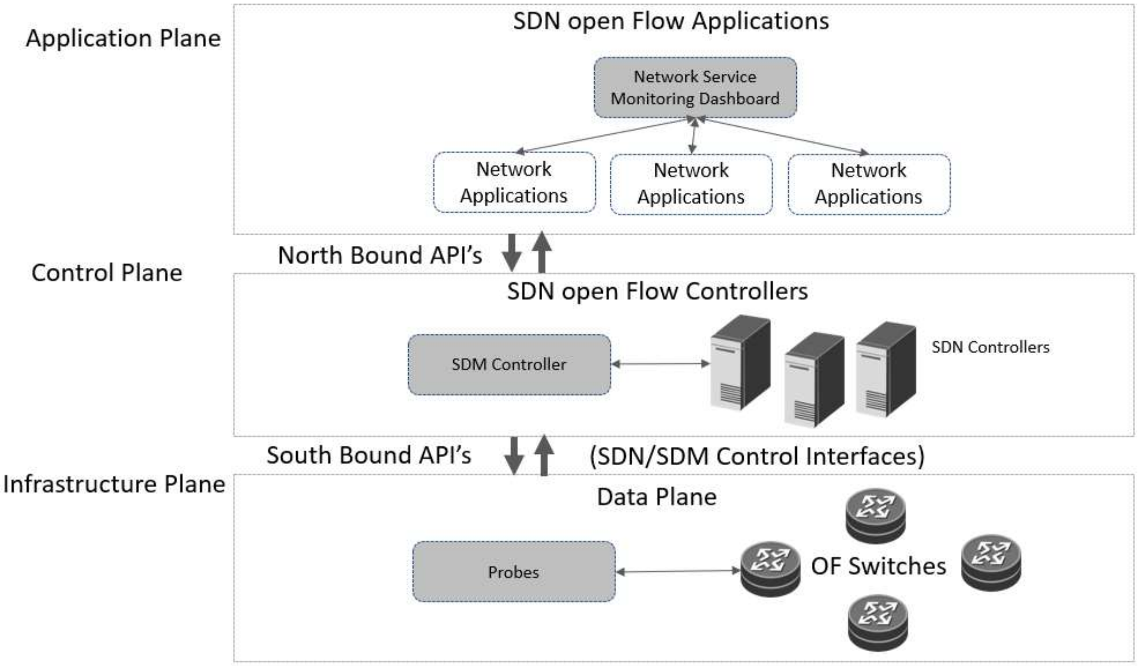


Figure 41 – SDN monitoring architecture for 5G Networks

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 14.4.1, section 14.4.2 and Figure 42 for the added Modules and Interfaces of the SDM architecture.

14.4.1 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.

14.4.2 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 linksto be obtained. In this way, applications and network functions can send requests.

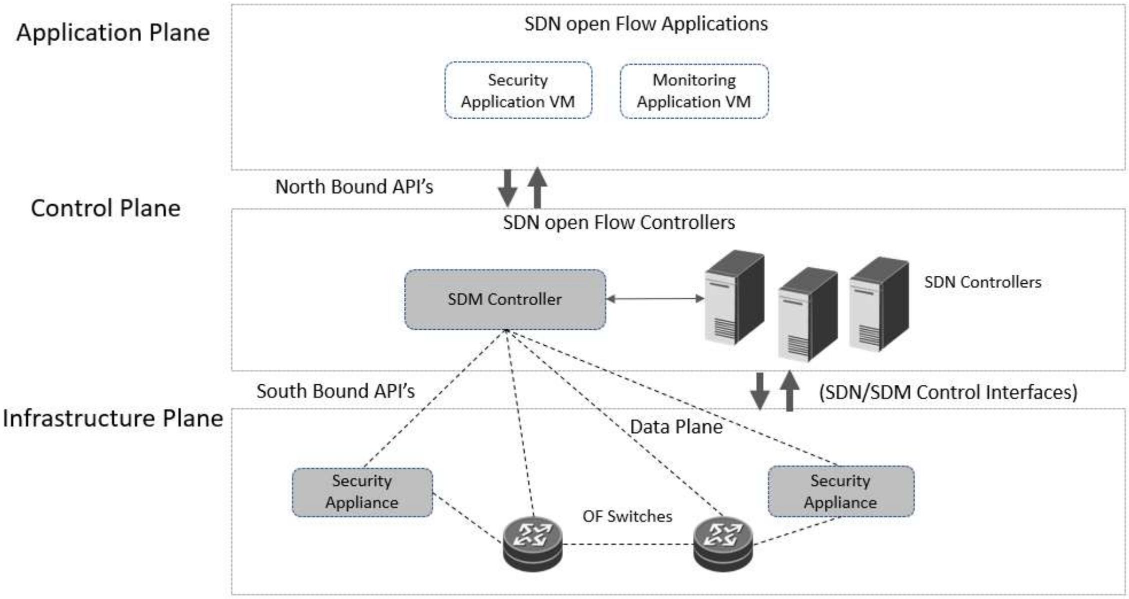


Figure 42 – SDM Controller components and Interfaces

15 Open RAN Security

Open RAN (O-RAN) is a paradigm shift in RAN architecture and deployment leveraging SDN and NFV by disaggregating traditional RAN functions, implemented in software, deployed on independent cloud infrastructures, connected via standard interfaces, etc., Complementary to 3GPP and other RAN initiatives O-RAN can improve supply chain security and reduce costs.

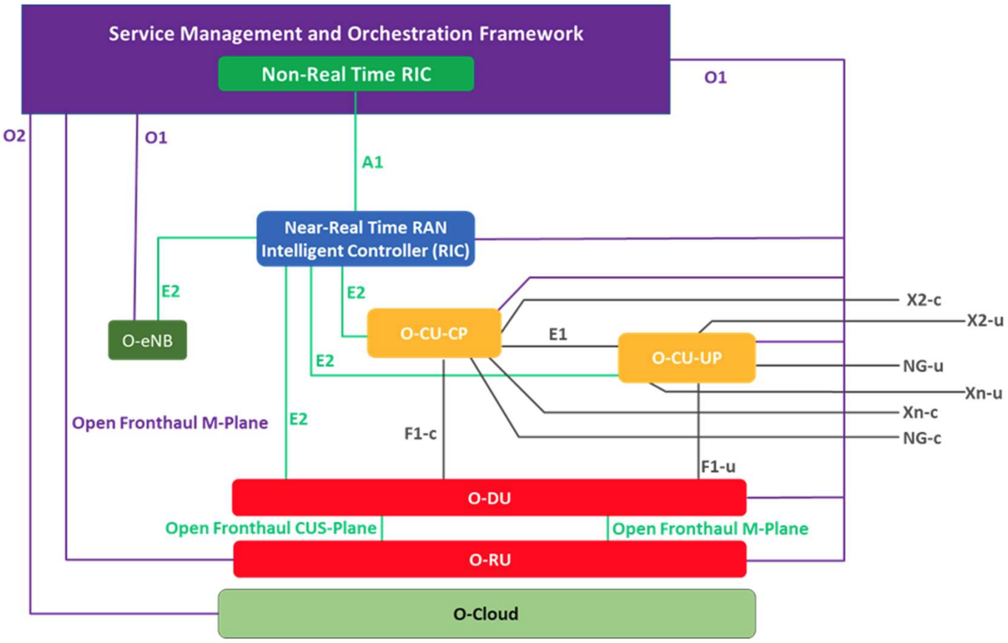


Figure 43 – O-RAN Logical Architecture

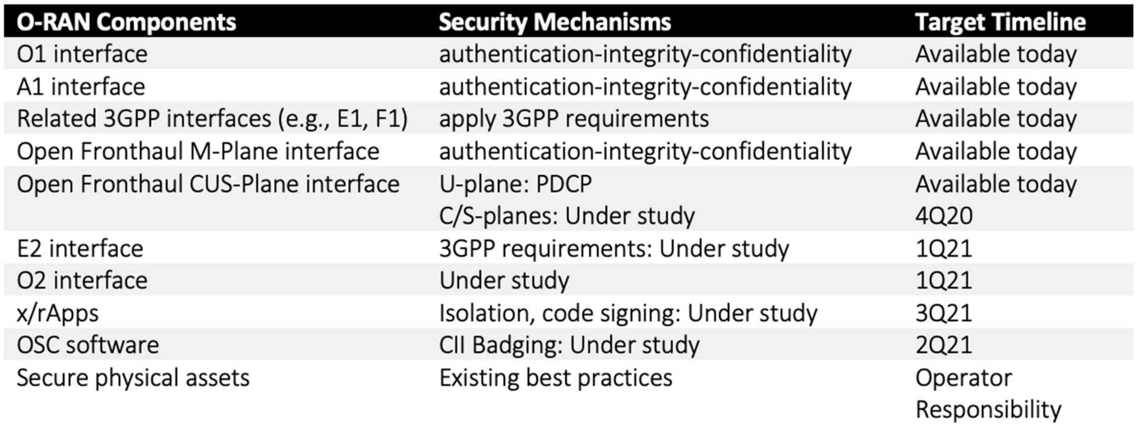
O-RAN also faces security challenges as other virtualised architectures:

- Disaggregation of functions increases the RAN threat surface.
- New challenges with monitoring and troubleshooting security issues in a disaggregated multi-vendor RAN architecture.
- The strict latency requirements on RAN need to be considered when implementing security controls, such as encryption, on the Open Fronthaul Interface.
- 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 IoT devices requires all RAN deployments to protect against the increasing likelihood of attacks by compromised devices.

Recognising the security challenges and criticality of a secure RAN, the O-RAN Alliance is following the 3GPP security design practices of rigorous threat modelling and risk analysis. In addition, the O-RAN management, Orchestration and Open Fronthaul M-plane interfaces are protected using security best practices such as TLS and/or Secure Shell (SSH), mutual authentication using X.509 certificates, access controls, robust logging and input validation.

The separation of O-RAN Distributed Unit (O-DU) and O-RAN Radio Unit (O-RU) introduces a potential new attack surface in the RAN. The open fronthaul interface operating the lower layer split (LLS) interface, and the threats to this interface will drive the security controls on the interactions between O-DU and O-RU, whereby security is key to delivering the benefits of this separation.

O-RAN security is evolving to adopt modern security best practices. Table 5 provides a partial view of the existing security controls and community's progress.



O-RAN Components	Security Mechanisms	Target Timeline
O1 interface	authentication-integrity-confidentiality	Available today
A1 interface	authentication-integrity-confidentiality	Available today
Related 3GPP interfaces (e.g., E1, F1)	apply 3GPP requirements	Available today
Open Fronthaul M-Plane interface	authentication-integrity-confidentiality	Available today
Open Fronthaul CUS-Plane interface	U-plane: PDCP C/S-planes: Under study	Available today 4Q20
E2 interface	3GPP requirements: Under study	1Q21
O2 interface	Under study	1Q21
x/rApps	Isolation, code signing: Under study	3Q21
OSC software	CII Badging: Under study	2Q21
Secure physical assets	Existing best practices	Operator Responsibility

Table 5 – Status of O-RAN Components and Security Mechanisms

For more details see the blog of the O-RAN Alliance "The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components" [93][93].

16 Security of Open Source Software

The GSMA whitepaper "Open networking and security of open source software deployments" [99][99] presents security considerations for practical deployment of Open Source Software (OSS) and open networking based on the report "Open Source Software Security [100].

A variety of deployment scenarios is explored within virtualised mobile networks to identify various 'shades' of open source varying from unique new proprietary code developments through commercially-supported software packages including significant open source code and on towards open source community-supported software packages, such as;

- as VNF on top of Cloud / Network Function Virtualisation Infrastructure (NFVI)
- as a component within a disaggregated solution
- as part of a wider Software as a Service (SaaS), e.g. as part of an O-RAN solution
- as middleware abstraction between the Commercial Off The Shelf (COTS) compute layer and applications layer sitting on the top
- re-used within vendor executable code with the executable code difficult to inspect.

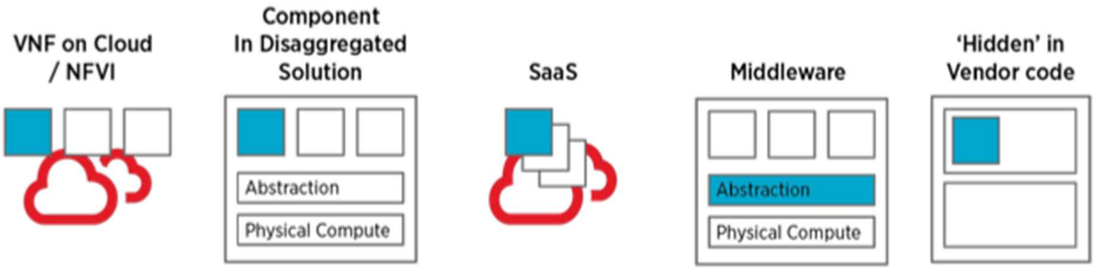


Figure 44 – Open Source Software (OSS) deployment arrangements

The whitepaper explains the differences between open interfaces and open source as these lifecycles operate at different cycle times as well as both concepts requiring different actions. In addition, the importance of layered security defences is outlined as well as broader security considerations such as whole systems thinking, hybrid networks, holistic penetration testing and threat & risk assessments. DevSecOps as a concept of 'shifting left' security activities into earlier lifecycle phases to embed security through the lifecycle of a system is also highlighted.

Specific coverage of the Open-Radio Access Network (O-RAN) Alliance security considerations to reflect on open source software security considerations is featured.

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

- Where vendor software includes open source components directly within code or is included in a full stack supply, encourage vendors to update/patch upstream components quickly or enable operators to act directly.
- Incorporate a Software Bill Of Materials (SBOM) to ensure full visibility of the deployed code in use.
- Exploit the strengths of open source transparency through code inspection, Source Code Analysis (particularly to generate and validate an SBOM), dynamic application security testing and encouraging use of coding standards through both vendor-Software Development Life Cycles and Core Infrastructure Initiative.
- Where infrastructure virtualisation is delivered through a software package that is open source code- derived, use scanning tools to identify obsolete, end-of-life and vulnerable products and encourage a supply arrangement to enforce the ability to update out of date components within a stack.
- Ensure that all open source components are supported by the community, industry groups and/or the supplier for all OSS components included in all products.
- 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 Cloud iNfrastructure Telecom Taskforce (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, open networking is changing this and may mean there are different vendors involved in each layer.

- The O-RAN Alliance Security Group is defining security requirements to align to the specifications and interfaces. GSMA is keen to assist the O-RAN Security Group to drive the maturity of security specifications that will build confidence for large scale deployments. These are important security considerations that require comprehensive design, feasibility and testing approaches that build maturity through practical experience.

- Consider the total operating environment into which open source code is deployed such that holistic security outcomes are considered across both new and existing infrastructures.

- Utilise a lifecycle approach such that security is designed-in, comprehensively tested in detail and in context, deployed securely and then operated to maintain this security in-life.

17 Security Assurance for 5G

17.1 Network Equipment Security Assurance Scheme (NESAS)

GSMA's Network Equipment Security Assurance Scheme (NESAS) [16][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 45 illustrates the collaborative roles of 3GPP and GSMA within the scheme.

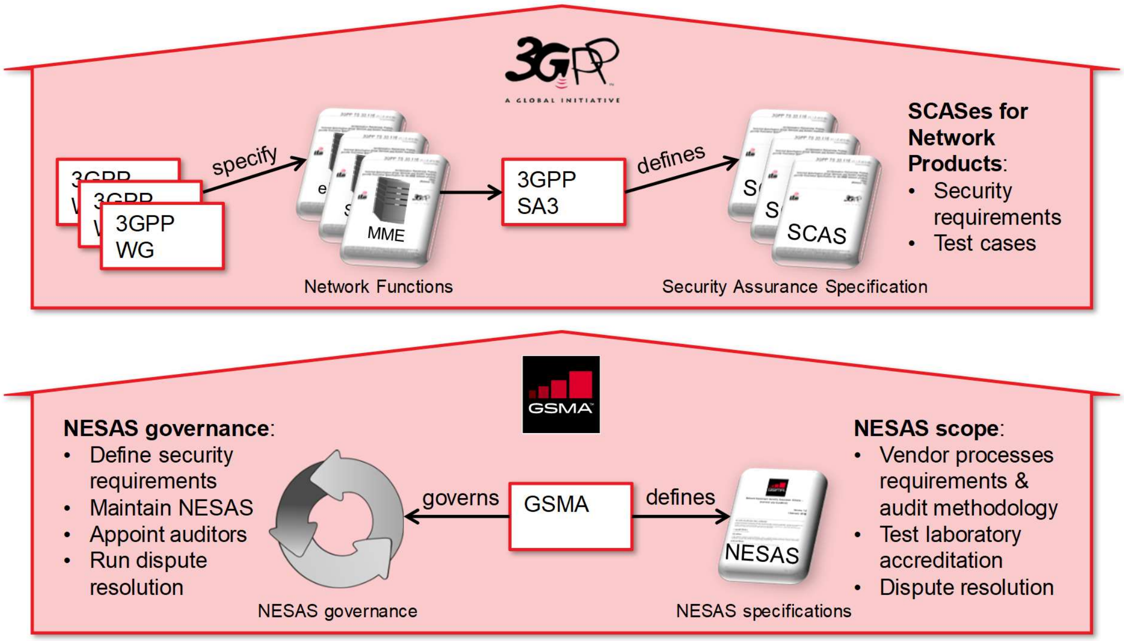


Figure 45 – Roles of 3GPP and GSMA in NESAS

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.

17.2 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/

17.3 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 stardards 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.

18 Regulatory Aspects and Industry Papers

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 servies that will be delivered by 5G. A range of initiatives and publications have emerged in a number of 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.

18.1 National and Regional Regulations

18.1.1 EU Level Regulations and Position Papers on 5G

18.1.1.1 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" [11].

Considerations on 5G security

- IPX securityaspects, 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 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 Network Function Virtualisation (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 break out from Diameter to use HTTP/2 as a base applicative layer and that wil 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 REST API for which known vulnerabilities exist and these are often more quickly discovered and exploited than was the case with older protocols.

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.

18.1.1.2 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][88], ENISA provides guidance (“the framework”) to EU national authorities on the technical details of implementing Articles 40 and 41 of the European Electronic Communications Code (EECC).

This is accompanied by the “5G Supplement to the Guideline on Security Measures under the EECC” [94][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.

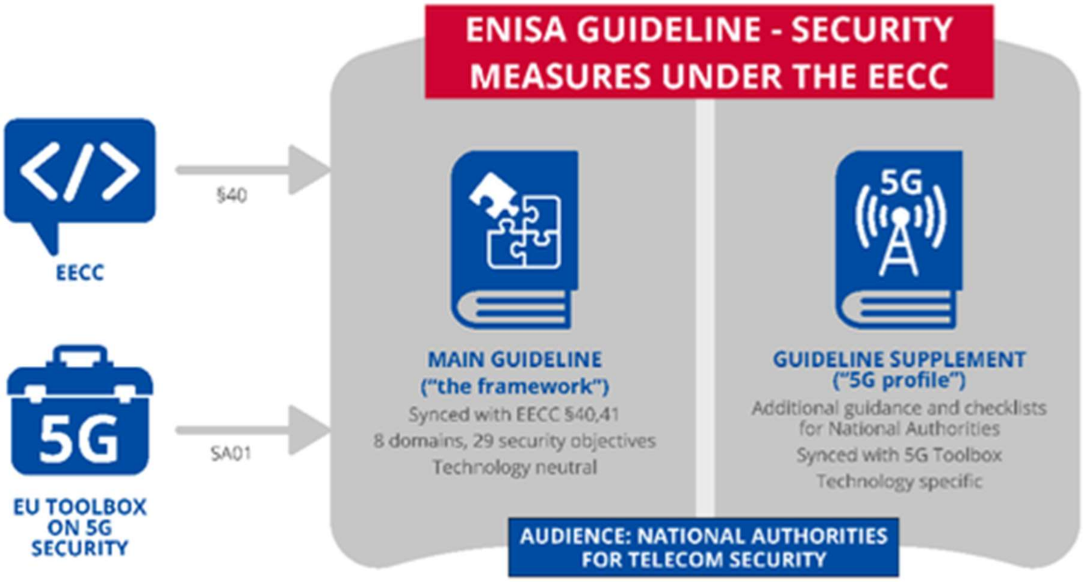

ENISA GUIDELINE - SECURITY MEASURES UNDER THE EECC
EECC
§40
5G
EU TOOLBOX ON 5G SECURITY
SA01
MAIN GUIDELINE
(“the framework”)
Synced with EECC §40,41
8 domains, 29 security objectives
Technology neutral
5G
GUIDELINE SUPPLEMENT
(“5G profile”)
Additional guidance and checklists for National Authorities
Synced with 5G Toolbox
Technology specific
AUDIENCE: NATIONAL AUTHORITIES FOR TELECOM SECURITY

Figure 46 – 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.

18.1.1.3 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 signaling in the 3GPP standards for 5G and they contain useful inights on the impact on network monitoring and the storage of user credentials in a HSM.

18.1.1.4 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.

18.1.1.5 The EU's Cybersecurity Strategy for the Digital Decade

The EU's Cybersecurity Strategy for the Digital Decade [101][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.

18.1.2 UK Telecommunications (Security) Bill

Telecoms 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 new Bill 216 will strengthen 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 will also provide the Government with new national security powers to issue directions to public telecoms providers in order to manage the risk of high risk vendors. While they are already banned from the most sensitive ‘core’ parts of the network, the Bill will allow the Government to impose controls on telecoms providers’ use of goods, services or facilities supplied by high risk vendors.

18.1.3 US Regulations and Position Papers on 5G

18.1.3.1 Secure 5G and Beyond Act of 2020 (S.893)

The U.S. “Secure 5G and Beyond Act of 2020” [30][30] was signed into law on March 23, 2020. It requires the US president to develop and implement a domestic security strategy for next-generation wireless communications networks. It also requires the U.S. to assist allies and partners in securing next generation mobile telecommunications networks. The U.S. “National Strategy to Secure 5G” was also released at the same time. This focused on assessing the risks, identifying core security principles for 5G infrastructures and managing the risks.

18.1.3.2 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.

18.1.3.3 FCC CSRIC WG2's Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation

The US FCC CSRIC Working Group 2 "Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation" [67] focuses on security enhancements brought about by 5G NSA, device threat mitigation and changes in workforce skills and training. Because the NSA architecture relies heavily on 4G infrastructure in the core, many of the vulnerabilities of 4G networks will exist in a 5G NSA deployment.

For **device security,** the report recommends consideration of a device-security management system for 5G networks. The following areas should be considered for standards development:

- A policy-based security management system
- Leverage Artificial Intelligence (AI) to detect malicious or anomalous device behaviour
- Leverage device management capabilities to act as a policy feedback loop.

For the **workforce,** WG2 recommends that industry establish best practices for employee training to address the transition to 5G SA highlighting the key activities that maintain carrier grade reliability and security. This may include workforce training on cloud architecture, network virtualisation and software defined networking, all of which are important foundational aspects of 5G SA architecture.

For **Control Channel Threats** with 5G NR, WG2 recommends that the industry leverage the flexible transmission capabilities of broadcast messages and signals. These technological advancements should be leveraged to provide interference mitigation and resilience.

With respect to **Threat Response Analysis, Academic Papers** it concludes that previously identified threats should continue to receive industry review and assessment. WG2 recommends higher layer security protections to mitigate user plane threats.

18.1.3.4 FCC CSRIC WG3's report to Mitigate Security Risks to IP-based Protocols

The USA FCC CSRIC Working Group 3 report "Report on Best Practices and Recommendations to Mitigate Security Risks to Current IP-based Protocols" [38] provides recommendations to mitigate the security risks.

The report focuses on Domain Name Server (DNS) and Border Gateway Protocol (BGP) as these protocols continue to evolve as the Internet continues to grow. Likewise, best practices continue to evolve. There are new best practices being developed, and implementation of existing measures such as the Resource Public Key Infrastructure (RPKI) continues.

The recommendations in this report are of value in the context of the Secure Implementation Guidelines with NESAS, as described in section17.1.

18.1.3.5 FCC CSRIC WG3's View on 5G Security

The following findings on 5G security are listed in the FCC CSRIC Working Group 3 report "Network Reliability and Security Risk Reduction – Final Report – Recommendations to Mitigate Security Risks for Diameter Networks" [12][12].

- The same network functions found in 3G and 4G will also exist in 5G to support roaming sessions.
- HTTP2 is being introduced as a transport for JSON and RESTful protocols to support 5Gsignaling but legacy Diameter interfaces will remain.
- QUIC is being considered to improve HTTP/2's performance of connection-oriented web applications currently over TCP by establishing a number of multiplexed connections between two endpoints over the UDP transport protocol.
- A pure 5G Core Network (i.e., 5GC) relies on HTTP2 interfaces, except for some legacy interfaces.
- Where the 5G radio terminates a Gateway (g)Nb into the existing 4G EPC, all of the EPC diameter interfaces are maintained.
- Most early 5G deployments will see the introduction of a new RAN and continued use of the existing 4G core network with the result that Diameter will continue to be supported for some time.
- 3GPP has defined 11 implementation models for 5G but with Release 15 only the NSA-based options 3/3a/3x are being considered with a 4G LTE Core because many of the CN functions are not defined by 3GPP with that release.

18.1.3.6 FCC CSRIC WG3's and WG2's Reports on Risks introduced by 3GPP Releases 15 and 16 5G Standards and Recommendations

The US FCC CSRIC Working Group 3 "Report on Risks introduced by 3GPP Releases 15 and 16 5G Standards" [91] evaluates the 3GPP Releases 15 and 16 standards, identifies areas of risk, and develops risk mitigation strategies to minimise risk in core 5G network elements and architectures.

The report examines the security enhancements of 5G NR network and the 5GC network, with a primary focus on the SA architecture. Several recommendations are given on how to mitigate potential 5G security threats, as well as proposed future work. Additional work on optional 5G features related to security and privacy will be the focus of a future WG3 report.

The FCC is advised to especially stimulate initiatives working on the framework for trusted 5G networks. To the industry, guidance is given on the following main topics:

- Safegarding NF elements like UDM and SMSF against attacks via both HTTP and via SS7/Diameter. The last due to interworking with 3G/4G networks and roaming by what known attacks to HLR/HSS and MSC/VLR could be repeated in a 5G network.

- To educate and train the workforce to operate and maintain carrier grade reliability and security in a 5G SA environment including virtualization and network slicing.

- The use of open source and open interfaces with a key role for standards offers a foundation and architecture for improving security in 5G provided that security is addressed as a fundamental consideration of all open source architectures.

- To ensure security in network slicing, the following factors should be considered:

    - **Slicing Isolation:** resources dedicated to one slice cannot be consumed by another slice and data/traffic cannot be intercepted/faked via another slice.

    - **Automated Slicing Security Management and Orchestration tools:** to cope with the dynamic nature of slicing with a complete network view.

    - **Slice-specific assurance level:** to ensure that all network functions used in a slice must meet the assurance level required for the services in the slice.

    - **Protection of slicing-specific procedures:** use of standardized security measures and standardized slicing-specific procedures for slice selection, authentication and authorization, or slice access by 3rd party tenants.

    - **Per slice network security measures:** as a slice is a virtual network, so general network security measures must be applied per slice like virtual firewall, zoning and traffic separation, cryptographically protected protocols integrity protection for platform and functions and AI/ML based analytics.

The US FCC CSRIC WG2 “Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture” [115][115] identified and evaluated optional features that if not implemented could reduce the effectiveness of 5G security and provided recommendations to address gaps. The primary focus is on the 5G NSA architecture (Option 3) that leverages the 4G ePC to support 5G NR and 4G capable devices and services. This report analyzed the 3GPP security specifications that are labelled “mandatory to implement” and are “optional for carriers to deploy” for both 5G (3GPP TS 33.501 [1]) and 4G (TS 33.401 [116]). Security categories included in the analysis included the following:

- NAS signaling confidentiality and integrity

- User plane confidentiality and integrity

- RRC signaling confidentiality and integrity

- Core network security

The primary recommendation is for carriers and operators to follow the guidance in previous reports ([12], [38] and [67]) discussing risks and mitigation strategies when determining their deployed security architecture. Additional recommendations included the continuation of the FCC CSRIC 5G security initiative, addressing the 5G SA architecture and using best practices as a reference when working with vendors and suppliers.

18.1.3.7 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 Annoucement (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). The solicitation specifically seeked innovative approaches and technologies to protect legacy, current and 5G mobile network communications, services and equipment against all threats and vulnerabilities.The BAA, at this time, has not been funded.

18.1.3.8 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. Even if U.S. networks are secure, U.S. data that travels overseas through untrusted telecommunication networks is potentially at risk of interception, manipulation, disruption, and destruction.
- 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.
- Despite security enhancements over previous generations, it is unknown what new vulnerabilities may be discovered in 5G networks. Further, 5G builds upon previous generations of wireless networks and will initially be integrated into 4G Long-Term Evolution (LTE) networks that contain some legacy vulnerabilities.
- Untrusted companies may be less likely to participate in interoperability efforts. Custom 5G technologies that do not meet interoperability standards may be difficult to update, repair, and replace. This potentially increases the lifecycle cost of the product and delays 5G deployment if the equipment requires replacement. The lack of interoperability may also have negative impacts on the competitive market as companies could be driven out if the available competitive market decreases.

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 User Equipment, Radio Access Network (RAN) and CN.

18.1.3.9 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.

18.1.4 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].

18.1.5 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 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.

18.1.6 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:

1. 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.
2. 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.
3. 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.

18.1.7 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.

18.1.8 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.

18.1.9 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.

18.1.10 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.

18.1.11 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 packet forwarding control protocol (PFCP). Therefore, also in 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.

18.1.12 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 operating systems 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.

18.1.13 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 in 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.

19 5G Security Research

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 Coordinated Vulnerability Disclosure (CVD) programme. A summary of the various disclosures that specifically relate to potential weaknesses in the 5G security standards is provided below.

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

The research paper “A Formal Analysis of 5G Authentication” [19][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]:

19.2 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 Radio Resource Control (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].

19.3 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 increases, indicating the presence of the target. The researchers observed that paging messages for any particular device will only happen in specific timeslots, 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].

19.4 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 man-in-the-middle 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].

19.5 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.

19.6 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][28] discusses potential security problems by dynamically testing the control plane 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 identified.

19.7 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.

19.8 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 64kbit/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 user plane 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 user plane integrity protection.

19.9 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.

19.10 5GReasoner: 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].

19.11 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 user equipment 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.

19.12 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.

19.13 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 users vs potential DoS to the network.

19.14 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/de-registration 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.

19.15 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.

19.16 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 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

A.2 Other Information

Type	Description
Document Owner	Fraud and Security Group
Editor / Company	Pieter Veenstra, NetNumber
Contributors	Silke Holtmanns, Adaptive Mobile Looi Kwok Onn, Anam Technologies Mansour Ganji, Bell Mobility 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

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.