Baseline Security Controls
Version 3.0
01 September 2023

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

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

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Background

Mobile Network Operators provide the backbone for mobile telecommunication technologies. At enterprise level the industry offers a wide array of services, diversifying from traditional connectivity into content and managed services. At the same time 5.1 billion [1] users depend on Operators to maintain their connectivity; an item considered a basic human right under UN Article 19 [2]. This results in a mixed threat landscape of traditional IT, radio and mobile related threats.

Based on this position the industry has a responsibility to secure customer information and services. The GSMA has developed the following baseline security controls to help Operators understand and develop their security posture to a foundation (base) level.

These controls are not binding; this is a voluntary scheme to enable an Operator to assess and understand their own security controls. The GSMA do not require access to the results but are suitably positioned to discuss specific output and identify remedial resources if desired.

1.2 Scope

This document outlines a specific set of security controls that the mobile telecommunications industry should consider deploying. The solution description identifies specific advice that would allow the Operator to fulfil the control objectives.

These controls stand separate to, but may be supported by, local market legislation and regulation. They do not replace or override local regulations or legislation in any territory. Their purpose is to enhance and supplement security levels within the mobile telecommunications industry.

1.3 Intended Audience

This document has been created as a list of controls, supported by a separate checklist of questions related to the controls. It is recommended that the checklist be completed by a person, or team, associated with the controls. For example, and as shown in Figure 1:

- The corporate security team could be assigned Section 2.1
- The device team could be assigned Sections 2.2.1 to 2.2.3
- The radio network team could be assigned Section 2.2.4
- The network engineering team could be assigned Sections 2.2.5 to 2.2.7
- The core network team could be assigned Section 2.2.8
- The network operations team could be assigned Section 2.2.9 and 2.2.10
- The network security team could be assigned Section 2.2.11
- The roaming team could be assigned Section 2.2.12

The overarching output is intended for use by the senior security personnel to understand the Operator's internal security posture.

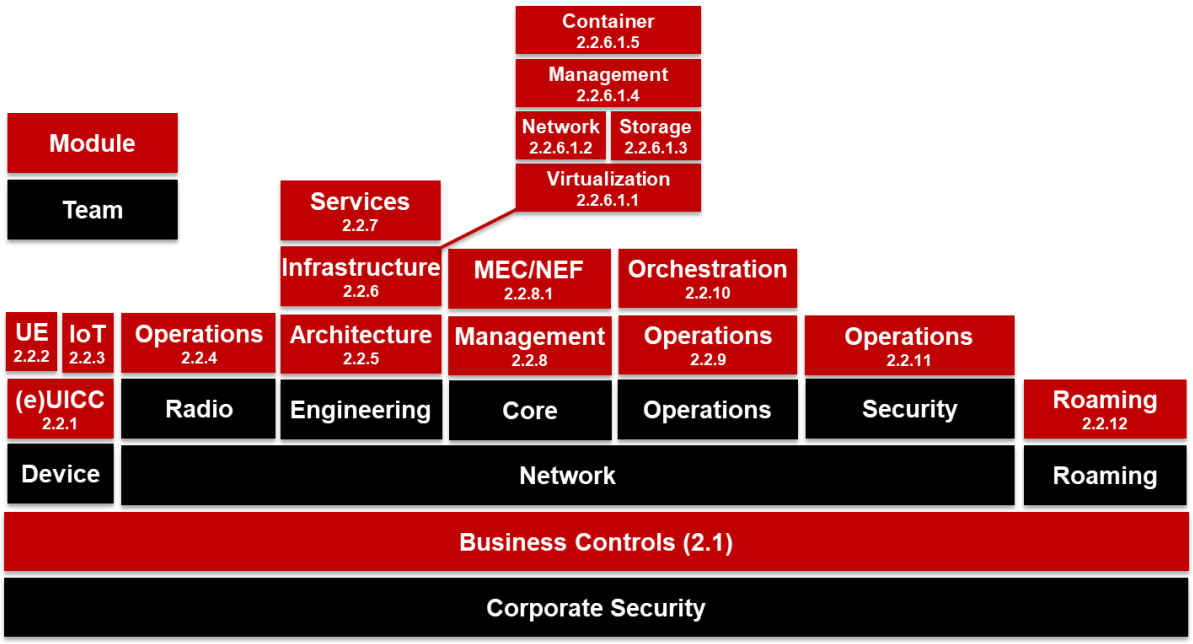


Figure 1: Mobile Operator Teams and Associated Controls

1.4 How to use this Document

Operators utilising these controls should compare the control(s) listed to their deployed internal security controls, identify and assess potential gaps, then respond to highlighted gaps within their organisation(s). The assessment can be completed using the accompanying checklist. Table 1 outlines the potential responses to the questions. These responses are aligned to recognize levels of maturity of information security and business controls. Levels 1 through to 5 represent recognition of the control and progress in development of its maturity. Level 0 has been added to reflect the stage prior to recognition of the need for implementation of the control. Controls can also be identified as Not Applicable (N/A) provided that the control has been reviewed and there is a justification as to why it is not applicable within a given context.

NOTE Failure to populate the checklist with accurate information will reduce its effectiveness.

How the controls are implemented is the responsibility of the Operator and specifics are not covered in this document. It is expected that internal implementation documentation or solutions are understood and approved by the Operator's Chief Information Security Officer (CISO) or equivalent. These are baseline (minimum) controls; if the assessed Operators have already implemented security controls that are considered more secure than those listed in this document the GSMA does not recommend reducing the security level implemented.

The GSMA provides supporting documentation, by way of Permanent Reference Documents (PRD), that outline specific details of some controls and recommendations, these are located on GSMA's Member Gateway. These may be beneficial to an Operator that identifies a gap in its technical controls.

The GSMA recognises the industry standard work by the Centre for Internet Security (CIS) Controls [3] and has aligned to these wherever appropriate. Where the controls have been used this is referenced into the Reference field. It should be noted that as CIS is focussed upon general computing cyber-security, therefore not all CIS controls are incorporated within the baseline: only those relevant to typical Operator systems.

It is also not rational to universally adopt a target maturity of Level 5 for all controls: only what is appropriate and proportionate for each of those controls. Typically, an organisation will first identify a strategic plan for maturity improvement over time. For instance, a limited set of the most significant controls could be targeted for improvement in Year 1, further controls improved in Year 2, within a strategic five-year plan aiming for an eventual target level of maturity profile tuned for each of the controls. An example is provided in the companion Annex A Excel tool, which is used to self-assess maturity.

Maturity Marking	Definition
N/A: Not Applicable	The GSMA baseline security control objective does not apply to the Operator. All 'N/A' responses should be supported with an explanation in the corresponding 'Notes' column.
Level 0: None	Control not present and has not yet been considered for implementation by the Operator. All 'Level 0' responses should be supported with an explanation in the corresponding 'Notes' column.
Level 1: Initial	The Operator has considered the control for implementation and has undertaken a gap analysis of the control against current policy and practice. There may be ad-hoc or localised implementation of the control, but the control is not supported strategically. A control improvement road map has been prepared to increase the level of maturity to an applicable target level of maturity. An outline of the road map and/or reference to it should be recorded in the corresponding 'Notes' column.
Level 2: Repeatable	The control has started to be adopted within the Operator's policies and practices. Progress has been made on its implementation and is included within a detailed programme of work which is underway. Progress is regularly reviewed by a programme board and where the control is implemented it is to a consistent, repeatable, standard. Progress of implementation of the control on the road map and programme plans should be recorded in the 'Notes' column.
Level 3: Defined	The control has been fully adopted within the Operator's policies and practices. The control has started to be embedded in governance and management processes, but this is not yet complete. Resourcing and training plans cover oversight of the control and these have started to be implemented. Progress of implementation of the control on the road map, programme and resourcing/training plans should be recorded in the 'Notes' column.

Maturity Marking	Definition
Level 4: Managed	The governance and management processes that oversee and operate the control are now fully in place and largely resourced by appropriately skilled and trained personnel. Plans are developed to monitor the effectiveness of the control and to put into place a process of regular review and improvement of the control. This includes considering feedback on control effectiveness from incident investigations and reviews. Progress of implementation of the control on the road map, programme/resourcing/training plans and review/improvement plans should be recorded in the 'Notes' column.
Level 5: Optimised	The control review/improvement processes are embedded and operating effectively (this level of maturity should not be claimed until those processes have undertaken several review cycles, e.g. six months or more). The control oversight has moved from the programme mode to business-as-usual status. Current control effectiveness status and improvement plans should be recorded in the 'Notes' column.

Table 1: Response to Security Controls/Maturity Levels

1.5 Terms of Use

This document is provided by the GSMA for information and Members internal use only. It is provided "as is" without any warranty and liability to the GSMA and its Members. The GSMA and its Members cannot be held accountable or liable for the use of the document.

1.6 Abbreviations

Term	Description
3DES	Triple Data Encryption Standard
3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AMQP	Advanced Message Queueing Protocol
API	Application programmable interface
AUSF	Authentication Server Function
BAU	Business as Usual
BC	Business Continuity
BCM	Business Continuity Management
BSI	British Standards Institute
BSS	Business support services
BSIMM	Building Security in Maturity Model
CA	Certificate Authority
CAB	Change Approval Board
CASB	Cloud Access Security Broker
CAPIF	Common API Framework
CIS	Centre for Internet Security
CISO	Chief Information Security Officer

Term	Description
CKMS	Cryptographic Key Management System
CPE	Customer Premise Equipment
CRL	Certificate Revocation List
CSIRT	Computer Security and Incident Response Team
CWPP	Cloud Workload Protection Platform
DES	Data Encryption Standard
ECIES	Elliptic Curve Integrated Encryption Scheme
EIR	Equipment Identity Register
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
eUICC	Embedded UICC
FASG	Fraud and Security Group
FFG	Fire, Flood and Gas
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GGSN	Gateway GPRS support node
GPRS	General Packet Radio Services
GRC	Governance, Risk and Compliance
GSM	Global System for Mobile – 2G Network
GSMA	GSM Association
GT	Global Title
GTP	GPRS Tunnelling Protocol
HA	High Availability
HLR	Home Location Register
HSM	Hardware Security Module
HSS	Home Subscriber Server
HTTPS	Secure Hypertext Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning
IDPS	Intrusion detection and prevention services
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
IPX	Internetwork Packet Exchange
iUICC	Integrated UICC
LCM	Lifecycle Management
LTE	Long Term Evolution - 4G Network

Term	Description
MAP	Mobile Application Part
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
MQ	Message Queue (SDN Java-based message service)
NAS	Non-Access Stratum
NE	Network Element
NESAS	Network Equipment Security Assurance Scheme
NFV	Network Function Virtualisation
NIDD	Non-IP Data Delivery
NIST	National Institute for Science and Technology (US)
NR	New Radio
OEM	Original equipment manufacturer
OS	Operating System
OSINT	Open Source Intelligence
OTA	Over the air
PAM	Privileged Account Management
PCEP	Path Computation Element Communication Protocol
PDN GW	Packet Data Network Gateway
PIN	Personal Identity Number
PKI	Public Key Infrastructure
PMN	Public Mobile Network
PRD	Permanent Reference Document
RAEX	Roaming Exchange
RAN	Radio Access Network
RCS	Rich Communication Services
RFC	Request for Comment
RSA	Rivest–Shamir–Adleman
SAE	System Architecture Evolution
SAML	Security Assertion Mark-up Language
SAS	Security Accreditation Scheme
SCEF	Service Capability Exposure Function
SDLC	Software Development Lifecycle
SFTP	Secure File Transfer Protocol
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIEM	Security Information and Event Management
SIGTRAN	Signalling Transport

Term	Description
SIM	Subscriber Identity Module
SLT	Security Leadership Team
SMS	Short Message Service
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Centre
SS7	Signalling System 7
SSL	Secure Sockets Layer
STP	Signal Transfer Point
SUCI	SUbscription Concealed Identifier
T-ISAC	Telecommunication Information Sharing and Analysis Centre
TDE	Transparent Data Encryption
TEE	Trusted Execution Environment
TMSI	Temporary Mobile Station Identity
TPM	Trusted Platform Module
TRE	Tamper Resistant Element
UE	User equipment
UICC	Universal integrated circuit card
UMTS	Universal Mobile Telecommunication Service - 3G Network
UTRAN	UMTS Terrestrial RAN
VIM	Virtual Infrastructure Manager
VLAN	Virtualised Local Area Network
VNF	Virtual Network Function
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

1.7 Definitions

Term	Description
Anomaly	A deviation from the common rule.
Authentication Server Function (AUSF)	The AUSF performs UE authentication in 5G networks.
Cloud Access Security Broker (CASB)	Technology used to control access to cloud tenants and users in a distributed cloud computing environment. Typically incorporated single sign on and ticketing methods such as SAML to control access to cloud resources and direct requests overload balanced infrastructures.
Core Network	According to 3GPP the core network consists of different technology and infrastructure depending on the generation of mobile telecommunications network: GSM: Circuit switching network elements (NE) UMTS: Packet switching and Circuit Switching NE

Term	Description
	GPRS: Packet switching NE LTE: Evolved packet core (EPC) NE 5G: 5G NE
Cryptographic Key Management System	A framework and services that provide for the generation, establishment, control, accounting, and destruction of cryptographic keys and associated management information. It includes all elements (hardware, software, other equipment, and documentation); facilities; personnel; procedures; standards; and information products that form the system that establishes, manages, and supports cryptographic products and services for end entities (NIST SP 800-57).
Evolved Packet Core	LTE's core network, consisting of the Home Subscriber Server (HSS), serving Gateway (SGW), Packet Data Network Gateway (PDN GW) and Mobility Management Entity (MME).
Embedded UICC (eUICC)	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the Device and enables the secure changing of subscription Profiles.
GSMA Fraud and Security Group (FASG)	A working group focused on the fraud and security needs of the mobile ecosystem.
Gateway GPRS Support Node (GGSN)	The GGSN is responsible for the internetworking between the GPRS network and external packet switched networks.
General Packet Radio Service (GPRS)	GPRS is a protocol used to carry packet-switched data traffic on mobile telecommunications networks.
GPRS Tunnelling Protocol (GTP)	GTP is a set of protocols used to carry GPRS signalling and user plane traffic within the mobile telecommunications network.
Hardware Security Module (HSM)	A HSM is a dedicated hardware component used to securely manage key material and/or sensitive processing
Home Subscriber Server (HSS)	A Home Subscriber Server (HSS) is a database within an LTE network that contains user-related and subscriber-related information.
Interception	Interception attacks include any attacks (passive or active) where the attacker attempts to intercept or re-route traffic/data for their own gains.
IPX Provider Network	The part of the IPX Network that is operated by one IPX Provider. All IPX Provider Networks together build the global IPX Network.
Integrated UICC (iUICC)	A UICC implemented on a Tamper Resistant Element (TRE) that is integrated into a System-on-Chip (SoC), optionally making use of remote volatile/non-volatile memory
Know your customer	Implement appropriate customer relationship management, accounting and utilisation systems to understand customer requirements and behaviours. It can also refer to due diligence in establishing and operating customer accounts and monitoring for breaches of usage conditions.
Maturity Model	A broadly recognized tool, with increasing levels, that assesses the maturity of the implementation of business strategies and controls (including information security management). The model proposed for the purposes of this document is defined in Table 1 on page 6.

Term	Description
Mobility Management Entity (MME)	The MME handles the signalling related to mobility and security for E-UTRAN access in LTE networks. The MME is responsible for the tracking and the paging of UE in idle mode. It is the termination point of the Non-Access Stratum (NAS)**Error! Reference source not found.**.
Multimedia Messaging Service Centre (MMSC)	The multimedia messaging service is a standard way to send messages that include multimedia content to and from a mobile phone over a cellular network. The MMSC acts as a relay or forwarding station for these messages.
Mobile Network Operator (MNO)	A mobile network operator carries out provisioning, billing and engineering for mobile services. A full member of the GSMA.
New Radio	5G's radio interface
Network Element	Any active component on the network involved in sending, receiving, processing, storing, or creating data packets and/or voice traffic. In the mobile network, components like the Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (PGW), Home Location Register (HLR), Home Subscriber Server (HSS), and GTP firewall, as well as routers and gateways, are network elements.
Network Equipment Security Assurance Scheme (NESAS)	NESAS is a voluntary network equipment security assurance scheme operated and maintained by GSMA, with contributions from 3GPP, covering the methodology and security targets for equipment under test. It defines a globally applicable security baseline that network equipment vendors can meet.
Organisation	This is a term that can apply to any member, manufacturer, Operator or business entity within the scope of the GSMA membership.
Packet Data Network Gateway (PDN GW)	The PDN GW provides connectivity from mobile devices to external packet data networks in LTE networks.
Physical security	Security controls to protect physical components of a network.
Privileged Account Management (PAM)	System that controls access to and accounts for use of privileged user functions and security critical functions. It can also add additional rules-based authentication layers for exercise of privileges.
Security Orchestration, Automation and Response (SOAR)	SOAR represents a combination of technology and disciplines to control security operation of resource allocation (compute, storage, network and peripheral access) and mobility within virtualized, containerised, compartmentalized, cloud computing and/or distributed data centre environments.
Security Accreditation Scheme (SAS)	The SAS is a GSMA certification scheme providing assurance that suppliers manufacture and/or manage UICCs, eUICCs and iUICCs in a secure way.
Security critical software update	A software update whose main intention is to fix security vulnerabilities that were identified in the original mobile operating system, often after the device has been produced and delivered, that need to be deployed widely and quickly due to a major security incident of some kind.

Term	Description
Serving Gateway (SGW)	The SGW is the point of interconnect between the radio-side and the LTE EPC; the gateway serves the UE by routing the incoming and outgoing IP packets**Error! Reference source not found.**.
Serving Gateway (SGW)	The SGW is the point of interconnect between the radio-side and the EPC; the gateway serves the UE by routing the incoming and outgoing IP packets**Error! Reference source not found.**.
Short Message Service (SMS)	Also known as text messaging that uses standardised communication protocols to exchange short text messages
Short Message Service Centre (SMSC)	A SMSC is a network element in the mobile telephone network which delivers SMS messages.
Signalling System 7 (SS7)	SS7 is a protocol allowing phone networks to exchange information needed for managing subscriber mobility and connections, and routing calls and text messages.
Signal Transfer Point (STP)	A STP is a router that relays SS7 messages between certain network elements.
User Equipment (UE)	Devices used by the end user.
Universal Integrated Circuit Card (UICC)	The UICC is the smart card used in mobile terminals to manage subscriber credentials and network access.
Vendors	An organisation offering a product or service used by the mobile telecommunications industry.
Virtual Private Network (VPN)	A VPN extends a private network across a public network.
Vulnerability	A vulnerability is generally a set of conditions that allow the violation of an explicit or implicit security policy.

1.8 References

Ref	Document	Link
[1]	GSMA Intelligence Global Mobile Trends	GSMAi
[2]	UN Human Rights Council	Article 19
[3]	Centre for Internet Security (CIS) Controls	CIS Controls
[4]	NIST SP 800-57 Recommendation for Key Management Part 2	NIST SP 800-57
[5]	GSMA Coordinated Vulnerability Disclosure (CVD) Programme	GSMA CVD
[6]	Building Security in Maturity Model	BSIMM
[7]	Effective Business Continuity Management Guidelines for Mobile Network Operators	GSMA BCM Guidelines
[8]	GSMA Security Accreditation Scheme	GSMA SAS
[9]	GSMA Network Equipment Security Assessment Scheme (NESAS)	GSMA NESAS

Ref	Document	Link
[10]	IMEI Security Technical Design Principles	GSMA IMEI Security
[11]	Requirements for Mobile Device Software Security Updates	PRD FS.25
[12]	Anti-Theft Device Feature Requirements	PRD SG.24
[13]	GSMA IMEI Database	GSMA IMEI Database
[14]	SAS Certified Sites	SAS Certified Sites
[15]	Trusted Connectivity Alliance S@T Specifications	S@T Specifications
[16]	GSMA Security Manual	PRD FS.30
[17]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	NIST SP 800-90A
[18]	FS.27 Security Guidelines for UICC Profiles	PRD FS.27
[19]	FS.28 Security Guidelines for UICC credential protection	PRD FS.28
[20]	Security Requirements for Cryptographic Modules (FIPS140-2)	FIPS140-2
[21]	GSMA eUICC Compliance	eUICC Compliance
[22]	Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model	ISO 15408
[23]	IoT Security Guidelines Overview Document	GSMA CLP.11
[24]	IoT Security Guidelines for IoT Service Ecosystem	GSMA CLP.12
[25]	IoT Security Guidelines Endpoint Ecosystem	GSMA CLP.13
[26]	IoT Security Guidelines for Network Operators	GSMA CLP.14
[27]	IoT Security Assessment Process	GSMA CLP.19
[28]	GSMA IoT Security Assessment Checklist	GSMA CLP.17
[29]	IoT Device Connection Efficiency Guidelines	GSMA TS.34
[30]	IoT Device Connection Efficiency Test Book	GSMA TS.35
[31]	FF.21 The Fraud Manual	PRD FF.21
[32]	Small Cell Forum Comprehensive overview of small cell security	Small Cell Forum: SCF171
[33]	FS.20 GPRS Tunnelling Protocol (GTP) Security	PRD FS.20
[34]	IR.88 LTE and EPC Roaming Guidelines	PRD IR.88
[35]	FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines	PRD FS.11
[36]	FS.07 SS7 and SIGTRAN Network Security	PRD FS.07
[37]	IR.77 InterOperator IP Backbone Security Req. For Service and Inter-Operator IP backbone Providers	PRD IR.77
[38]	IR.21 GSM Association Roaming Database, Structure and Updating Procedures	PRD IR.21
[39]	IR.85 Roaming Hubbing Provider Data, Structure and Updating Procedures	PRD IR.85*
[40]	3GPP Confidentiality algorithms	3GPP Algorithms

Ref	Document	Link
[41]	SG.20 Voicemail Security Guidelines	PRD SG.20
[42]	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture	ETSI TS 133 102
[43]	3GPP System Architecture Evolution (SAE); Security architecture	3GPP 33.401
[44]	SMS Firewall Best Practice and Policies	PRD SG.22
[45]	GSMA IMEI Blacklisting	GSMA IMEI Blacklisting
[46]	Security Recommendations for Server-based Hypervisor Platforms	SP 800-125A Rev. 1
[47]	BSI TR-02102 Cryptographic Mechanisms	BSI TR-02102
[48]	NIST SP 800-57 Recommendation for Key Management Part 1	NIST.SP.800-57
[49]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	RFC 3647
[50]	EV SSL Certificate Guidelines	CAB Forum
[51]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	RFC 5280
[52]	NIST SP 800-57 Recommendation for Key Management Part 2	NIST SP 800-57
[53]	Telecommunication Information Sharing and Analysis Centre	T-ISAC
[54]	ISO/IEC 27035:2016 — Information technology — Security techniques —Information security incident management	ISO 27035
[55]	GSMA Anti-Theft Device Feature Requirements	PRD SG.24
[56]	Diameter Interconnect Security	PRD FS.19
[57]	Security Architecture and Procedures for 5G System	3GPP TS 33.501
[58]	FS.36 5G Interconnect Security	PRD FS.36
[59]	FS.42 Guidelines for MNO Filtering of Binary SMS	PRD FS.42
[60]	NIST Cybersecurity Framework (CSF)	NIST CSF
[61]	ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT	ISO/IEC 27001
[62]	ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls	ISO/IEC 27002
[63]	ISO/IEC 27011 - Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	ISO/IEC 27011
[64]	ISO 22301 - Security and resilience — Business continuity management systems — Requirements	ISO/IEC 22301
[65]	ISO/IEC 27040 - Information technology — Security techniques — Storage security	ISO/IEC 27040

Ref	Document	Link
[66]	ISO 28000 - Specification for security management systems for the supply chain	ISO/TC 28000
[67]	NIST Special Publication 800-88, Guidelines for Media Sanitization.	NIST SP 800-88
[68]	NIST Special Publication 800-190, Application Container Security Guide	NIST SP 800-190
[69]	ISO/IEC 27031 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity	ISO/IEC 27031
[70]	Developing Cyber Resilient Systems: A Systems Security Engineering Approach	NIST SP 800-160 vol 2
[71]	OWASP Application Security Verification Standard	OWASP AVAS
[72]	Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs	3GPP TS 33.122
[73]	OpenStack Neutron's documentation	Open Stack Neutron
[74]	ETSI GS NFV 002, Network Functions Virtualization, Architectural Framework	ETSI GS NFV 002
[75]	NISTIR 8276 - Key Practices in Cyber Supply Chain Risk Management, February 2021	NISTIR 8276
[76]	NIST Application Container Security Guide	NIST SP 800-53

2 Baseline Security Controls

This section defines the Baseline Security Controls. It is divided into several sub-sections and tables that are organized depending on the applicability of the types of GSMA Operator members and other stakeholders.

Operators should complete the corresponding Annex A sub-sections according to the relevance to the services they provide.

Each table is organised into three columns:

- **Reference** – the unique reference for Baseline Security Control set;
- **Objective** – the objective that is to be achieved by implementation of each control set;
- **Solution Description** – the envisaged set of controls and standards applicable to each control objective. Where greater detail is available in external standards and documents these are referenced in square brackets (refer to the References Table within sub-section 1.8).

NOTE The numbered items given under the Solution Description do not correspond to the maturity levels used to score the controls. Rather, these indicate a sequence of controls that can be applied to each Objective.

2.1 Business Controls

Business controls are controls that relate to how the overarching enterprise manages security. They are not necessarily technical in nature and may relate to reporting or communication procedures that are essential for an Operator to support business objectives regarding security.

These controls are likely to be understood and managed by the security leadership team (SLT), this team would be able to comment on how these controls are implemented.

Reference	Objective	Solution Description
BC-001	**Board Level Engagement**, where organisations fail to recognise security at Board level there is likely to be a gap in the way the organisation understands their success, risk posture, priorities and future investment on programmes. This gap introduces unnecessary security and fraud risks.	1. Regular security briefing to Board Level 2. Specific security strategy with direct senior level reporting 3. Clear board level ownership of information security risks and issues 4. Sponsorship for information security risk management funding and resourcing
BC-002	Organisations should have a **role formally recognising security** as a responsibility, CISO's often fulfil this role. Alternatively, it can be any person of senior standing, their role must be able to influence and direct enterprise level investment and change.	1. Named, accountable role 2. Formally recognised integration with organisation 3. Responsibility includes regular briefing into senior leadership 4. Formal mandate and budget
BC-003	**Organisational policies** are a set of rules that the organisation should abide by. Specific policies will be constructed in relation to security and should map to the overarching security strategy and principles of the organisation; essentially policy should underpin the organisation's security objectives.	Specific policies pertaining to (at least): a. 3rd party data/supply chain security management b. Access Control c. Asset management; including architectural design, in life management, and decommissioning d. Business continuity management e. Cloud security f. Cryptographic material management [4] g. Device, system and network asset security h. Information classification and handling i. Personnel security j. Corporate travel security k. Physical security l. Risk management m. Security incident management; including breach notification, analysis and mitigation planning

Reference	Objective	Solution Description
		n. Security monitoring; including reporting to compliance programme o. Software security update management p. Staff training and awareness q. Vulnerability disclosure management [5] Further details are provided in Annex B.
BC-004	**Governance, risk and compliance** (GRC) are three functions that complement each other, providing reporting processes to detail operational progress against strategic requirements. Governance should align to organisation policy; reporting is shared with senior leadership to explain the delivery success of the entire security programme.	1. Defined security compliance reporting to business 2. Formal security audit programme 3. Formal security governance programme that aligns with organisational policy 4. Security risks aligned to business risks 5. Programme(s) exist to implement strategy and plans for the maturity of information security risk management controls 6. Appropriate escalation paths for significant information security risks and issues 7. Security is embedded within the organisation culture and business-as-usual practices 8. Regular audits, threat intelligence and inspections of compliance against security policies 9. Regular information security risk management improvement reviews
BC-005	Ensure all projects go through a **security assessment** to confirm they are **secure by design**.	1. Project design process with defined security acceptance stage including active verification (e.g. pen testing vulnerability scans, red team exercises, etc.) 2. Threat modelling and intelligence integration based on project prioritisation and purpose 3. Select appropriate technical and non-technical controls for implementation based upon the outcome of an information security risk assessment and management activity
BC-006	Ensure all projects go through a **data protection/privacy assessment**. This assessment should align to local policy, industry regulation and relevant legislation. These will inform local data management principles.	1. Local data protection principles applied 2. Personal data identification 3. Meeting of regulatory requirements for data protection, subject access, telecommunications regulation, cybersecurity and freedom of information requirements

Reference	Objective	Solution Description
BC-007 / CIS-007	**Secure Software Development Life Cycle (SDLC) implemented**, this lifecycle should include quality control stages, with code review at module and system level, including both static and dynamic testing. Code language choice considers security issues such as type safety and vulnerable functions.	1. Application Programmable Interface (API) development and implementation included in SDLC 2. Open source and purchased software included in SDLC 3. Recognised, industry standard set of secure coding practices enforced e.g. BSIMM [6] 4. Up-to-date inventory and documentation of used and deprecated API and software versions
BC-008	**Business Continuity Management** (BCM) improves the resilience of the organisation. Developing and organisation's **ability to detect, prevent, minimise and deal with the impact of disruptive events**. In the aftermath of an incident the BCM plan will enable critical activities within the organisation to continue. In the longer term it will help the business to recover and return to Business as Usual (BAU).	1. Crisis communication measures in place 2. Operator BCM process, exercised annually [7] 3. Service specific documented BCM process, exercised annually 4. Effective data backup and restoration processes (with regular tests of recovery) 5. Capacity planning and management controls to prevent avoidable network outages 6. Disaster recovery facilities, contingency planning and security testing 7. Architectures designed to eliminate single-points of failure with redundancy, cut-over management and load-balancing
BC-009	**Physical security controls.** To reduce the risk of a physical attack being used to facilitate a logical attack an Operator's security strategy should consider physical security controls and procedures holistically.	1. Environmental controls such as fire, flood and gas (FFG) and heating, ventilation, and air conditioning (HVAC) interlinked with security management 2. Facilities maintenance reporting interlinked with security management 3. Site access management controls implemented a. Include cell and customer premise equipment (CPE) sites where possible b. Include remote Multi-access Edge Compute (MEC) sites where applicable 4. Physical security standards and risk assessments depending on the class of sites (office environments, data centres, operations centres, remote sites (manned/unmanned/lights-out), public access)

Reference	Objective	Solution Description
BC-010	Operators should implement effective supply-chain and **procurement controls** to ensure the services they operate and provide comply with legal requirements and manage supply-chain threats.	1. Security hygiene expectations e.g. patching and following cyber supply chain risk management key practices (e.g., NISTIR 8276 [75] 2. Ownership and risk governance of the service and infrastructure 3. Industry standard assessment programmes to assure vendor products e.g. NESAS [9] 4. Mapping planned logical interconnects 5. Mapping planned physical interconnects 6. Life-time support arrangements 7. Manufacturers of critical components should provide, for example, an ISO 28000 statement of compliance or local regulation compliance. 8. Manufacturers of 5G network equipment should provide, for example, an ISO 27001/2 statement of compliance or local regulation compliance. 9. Manufacturers of 5G network equipment should provide, for example, an ISO 22301 statement of compliance or local regulation compliance. 10. 5G service providers e.g. MSPs, MSSP should comply with, for example, SoC 2 (SSAE 18) for all services provided under the scope of the service agreement or local regulation compliance.
BC-011	Operators should implement **3rd party** access and **outsourcing controls** to ensure the risks of information sharing and outsourcing are effectively managed.	1. Processes to identify, prioritise and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process. 2. Procedures exist to identify and manage the risks associated with third-party access to the organization's systems and data. 3. Security controls required of internal staff and resources, including privileged access (NO-005 / CIS-004), are mirrored with prioritized suppliers 4. Contract and due diligence checks for prioritised suppliers based on a pre-procurement risk assessment 5. Breach notification from suppliers in a timely manner

Reference	Objective	Solution Description
BC-012	**Decommissioning of equipment** should consider secure sanitisation or disposal controls to avoid the risks of consequent data leaks.	1. Removing access for testing access 2. Defining and enforcing media sanitisation policies in accordance with country-specific or internationally recognised guidelines e.g. NIST SP 800-88 and ISO/IEC 27040 3. Deleting and sanitising all interfaces and configurations e.g. support for older protocols and memory 4. Policy for reuse, selling and secure and safe disposal/destruction of equipment 5. Compliance with environmental, recycling, reuse and disposal regulations
BC-013	**Products (HW/SW) are protected** from tampering either via supply chain poisoning or internal threat agents with privileged access	1. Manufacturers should support integrity verification technologies in their products/solutions including signed software / firmware packages, and secure delivery mechanisms for HW and SW. 2. MNOs should define and implement a risk-based patch management (e.g. deployment) policy. 3. Security patch policies should include minimal – maximal deployment time limits, alternative mitigation options (if they exist) and cost-benefit analysis 4. MNOs should establish hardware lifecycle policies e.g. full/partial equipment replacement, decommission. 5. MNOs should continuously monitor and evaluate the organisation's compliance against set patch management policies.
BC-014	Operators should align their cyber-security practices and compliance regimes against internationally recognised standards and cybersecurity frameworks.	1. Operators should align, where appropriate, their cybersecurity risk management and compliance with the latest published versions of internationally recognised standards, specifically: • MNOs should align BC-004 (Information Security Management) with ISO/IEC 27001/2/11. • MNOs should align BC-008 (BCM) with ISO/IEC 22301. • MNOs should align BC-011 and BC-010 (Supply Chain) with ISO/TC 28000.

Reference	Objective	Solution Description
		• MNOs should align BC-012 (Media Sanitization) with ISO 27040 or NIST SP 800-88. 2. MNOs should align existing cybersecurity risk management processes with an established and recognised cybersecurity framework such as NIST CSF.
BC-015	Operators should define clear cyber resiliency strategic objectives and incorporate these objectives into the organisation's risk management framework.	1. MNOs should define & implement objectives to: • Continue the duration and viability of essential mission or business critical functions during adversity e.g. by ensuring the availability of services and minimising the impact of service degradation (see ARCH-009), • Constrain - limit damage from adversity e.g. by identifying and isolating compromised assets. • Reconstitute – ensure the restoration of business functionality as soon as possible after an attack and determine the trustworthiness of restored resources. 2. Align the organisation's cybersecurity resiliency strategy with industry best practices such as NIST SP 800-160 vol 2.

2.2 Technological Controls

Each of the technical controls outlined are required to secure a mobile telecommunications network. The sections represent the operational team who may manage the control's area of responsibility. This team, or area, is likely to be able to comment on the Operator's solution within their network.

2.2.1 (e)UICC Management Controls

These controls are likely to be understood and managed by the SIM management team.

Reference	Objective	Solution Description
SIM-001	Establish, implement and actively manage a rigorous **SIM management programme.** This programme must focus on the secure provisioning and purchase of (e)UICC from reputable vendors.	Confirm that the UICC supplier: a. Sources UICC/eUICC cards only from SAS certified production sites [14] b. Implements Over the air (OTA) functions that are not vulnerable to known attacks [15] c. Ensure SIM based web browsers are securely deployed and configured with

		appropriate minimum security levels enabled [18] d. Implements appropriate authentication algorithms i.e. resistant to brute force attacks [16] e. Implements Authentication counters and similar mechanisms to protect against brute force attacks on physical UICC f. Uses secure random number generators [17] to create the 'seed' material for common and unique (e)UICC credentials [19], [20] g. Implements appropriate protection for subscriber keys in storage and in transit (between SIM vendor and Operator), at record layer (AES), file layer (AES, ECIES or RSA) and in transport (HTTPS, FTPS, SFTP) [19] h. Implements mechanisms to protect against side channel analysis attacks such as differential power analysis [18] i. Implement filtering for binary SMS from external sources according to GSMA [59]
SIM-002	Source eUICCs that comply with the GSMA eUICC specifications, and have declared compliance under the GSMA eSIM/M2M compliance programmes [21]	This requires: a. eUICC production at a SAS accredited site(s) [13] b. Security assurance to GSMA's defined security objectives, with resistance against ISO 15408 [22] defined attacks c. Certified functional compliance to the specifications d. Keep up to date with latest security specifications e.g. for S@T browser [15]

2.2.2 User Equipment and Mobile Equipment Controls

These controls are likely to be understood and managed by the mobile device team.

Reference	Objective	Solution Description
UE-001	Source devices that have **secure IMEI implementations**.	1. Purchase devices with secure IMEI / PEI implementations, that comply with the GSMA's IMEI security design principles [10]
UE-002	**Deliver security critical software updates** to vulnerable mobile devices with minimal delay.	1. When it is the responsibility of the operator, make available security patches that do not risk disrupting service to vulnerable devices within 2 weeks of receipt from original equipment manufacturers (OEM) [11]

Reference	Objective	Solution Description
UE-003	**Prevent the connection and use** of stolen, defective or counterfeit devices.	1. Block duplicate or invalid IMEI numbers 2. IMEI checks should be carried out to verify that the device is not blacklisted prior to providing mobile network access [45] 3. Implement and manage an Equipment Identity Register (EIR)[12] 4. Share stolen device data with the GSMA's IMEI Database [13] 5. Encourage implementation of device based anti-theft features by device manufacturers and use of them by customers [55]

2.2.3 Internet of Things Controls

The Internet of Things (IoT) is projected to grow rapidly over the next few years. Operators are diversifying and providing managed IoT services as well as hosting data generated from IoT endpoints. IoT services should be deployed and managed in a secure way and the team managing this product set should understand the following controls.

Reference	Objective	Solution Description
IOT-001	IoT service providers shall comply with **security by design** and **privacy by design** industry best practice.	1. Implement the guidelines stated in GSMA CLP.11 IoT Security Guidelines Overview Document [23]
IOT-002	IoT service platforms shall comply with **IoT security industry best practice**.	1. Implement the guidelines stated in GSMA CLP.12 IoT Security Guidelines for IoT Service Ecosystem [24] document.
IOT-003	IoT device endpoints shall comply with **IoT security industry best practice**.	1. Implement the guidelines stated in GSMA CLP.13 IoT Security Guidelines Endpoint Ecosystem [25] document.
IOT-004	Networks shall comply with **IoT security industry best practice**.	1. Implement the guidelines stated in GSMA CLP.14 IoT Security Guidelines for Network Operators [26] document.
IOT-005	IoT services shall subject to a **security assessment**.	1. Complete of an IoT security assessment as described in GSMA CLP.19 IoT Security Assessment Process [27] document and GSMA CLP.17 GSMA IoT Security Assessment Checklist [28] document.
IOT-006	IoT device endpoints shall comply with **connection efficiency best practices** to protect networks from the risks caused by the mass deployment of inefficient, insecure or defective IoT devices.	1. Ensure IoT devices comply with the guidelines stated in GSMA TS.34 IoT Device Connection Efficiency Guidelines [29] and test devices according to GSMA

Reference	Objective	Solution Description
		TS.35 IoT Device Connection Efficiency Test Book [30].

2.2.4 Radio Network Operational Controls

These controls are likely to be understood and managed by the radio network team.

Reference	Objective	Solution Description
RN-001	**Cryptographically protect GSM, GPRS, UMTS, LTE and NR network traffic** to protect against unauthorised interception and alteration of user traffic and sensitive signalling information.	1. Enable the encryption mechanisms recommended in FS.35 and forbid the use of non-encryption, where possible. 2. Ensure that control plane integrity protection in UMTS, LTE or 5G is correctly enforced 3. Ensure that user plane integrity protection is enforced where feasible and necessary 4. Protect the interface between the radio access network and the core network (S1/N2) e.g. deploy IPsec where appropriate 5. Protect the radio interface between radio access nodes i.e. eNBs/gNBs (X2/Xn) e.g. deploy IPsec where appropriate 6. Protect the F1 and the E1 interface in gNB with a split DU-CU implementation
RN-002	**Prevent user tracking** though the appropriate use of temporary device identities, for instance before the device has authenticated to the network	1. Use 3GPP defined standard temporary identifiers e.g. SUCI, TMSI when transferring unprotected device information across the network
RN-003	Detect attacks that may result in network instability; **locate anomalous activity in the network**	1. Monitor for and respond to traffic fluctuations, unusual handover patterns, dead spots and service disruption that may be due to jammers or false base stations [31] 2. Monitor the distribution of base station equipment 3. Prevent/detect bidding down attacks, authenticate as far as possible using techniques such as in IR.77 [37] and configure radio network components to detect spoofing, misaddressing/misrouting and discard mal-formed traffic
RN-004	Ensure RAN sharing initiatives **isolate data, user and control traffic** correctly	1. Design a RAN architecture that incorporates appropriate segregation of

Reference	Objective	Solution Description
		the different traffic classes using spectral or logical means 2. Segregate traffic of different Operators using isolation techniques e.g. secure tunnelling 3. Implement utilisation and accounting frameworks for resource sharing 4. Rigorously test all segregation mechanisms 5. Ensure traffic quality-of-service, prioritization and pre-emption characteristics are preserved
RN-005	Ensure **base stations are secured and maintained**	1. Ensure physical site security controls are implemented, e.g. access control to fibre communication links, protection of equipment housing, internal components, and configurations 2. Secure interfaces and management channels 3. Ensure communication between the O&M systems and the eNB/gNB are confidentiality, integrity and replay protected from unauthorised parties. Ensure the security associations between the eNb/gNB and an entity in the 5G Core or in an O&M domain are mutually authenticated
RN-006	Where **small cells** are deployed in hostile environments compensating controls should be implemented to **manage the risk** [32].	1. Secure interfaces and management channels 2. Ensure small cells are tamper resistant and tampering triggers a monitored alarm system 3. Source small cells with a: a. Trusted environment b. Trusted boot process c. Location verification d. Network isolation capability

2.2.5 Network Architecture Controls

These controls are likely to be understood and managed by the network architecture / engineering team. The intention of these controls is to implement protective structures in the E2E architecture for the network.

Given the complexity of the Network Architecture a structured approach is suggested to describe the security aspects taken to be into account.

Reference	Objective	Solution Description
ARCH-001	**Implement physical architecture layer protection** for the network infrastructure including DC infrastructure and interconnection.	1. All unused, unnecessary physical interfaces are disabled to prevent malicious access and damage. 2. Implement hardening procedures for OAM and Service elements on all elements (servers, switches, storage, etc.) used for the physical infrastructure. 3. No single point of failure is able to cause a service outage. 4. All communication paths are authenticated including peer verification. 5. ACLs are used to prevent unauthorised access and forwarding.
ARCH-002	**Implement site redundancy for Core Datacentres** able to deal with future service demands like uRLLC, eMTC and Campus solutions.	1. Deploy all service relevant components and applications, in a full geo-redundant manner. 2. Ensure geo-redundant deployments cannot influence each other. 3. With the distributed processing architecture demanded by upcoming new services, especially for multi-DC/Edge-DC architecture driven by cloud deployments, it is recommended to implement new georedundancy options that provide site-redundancy between the edge DCs and between Edge and Core DCs. 4. Service relevant Datacentres must be connected in a fully redundant and secure way such that no connection outage is able to cause a service outage. 5. The border points of datacentres (Edge/core) must be hardened and protected (ACL, Firewall, Encrypted/Authenticated communication). In addition, datacentres must not have the ability to influence or disrupt each other.
ARCH-003	**Separate the communication in Datacentres and between datacentres based on traffic class/type** and its security and sensitivity requirements by dedicated communication layers and traffic isolation	1. Traffic types and communication paths have to be identified and structured at a variety of levels, beginning with internal communication (e.g. heartbeat, internal control, orchestration, etc.) and external communication (e.g. service

Reference	Objective	Solution Description
		signalling, service user plane, OAM and billing) 2. Based on the requirements (SLA) and security aspects/sensitivity of the traffic types dedicated communication subnets have to be structured. 3. Separate traffic types from each other, L1, L2, L3, L4-L7 separation, to ensure independent, secure processing with SLA guarantees. 4. Despite layer isolation, identity information should be provided across layers for cross validation and consistency purposes (e.g. IP address, instanceID, certificate related information to upper layers).
ARCH-004	**Embed the Application Architecture into the Security domain design** to ensure proper application interaction and protection for the service	1. Correlate the application communication according to the traffic separation done in ARCH-003. 2. Ensure the Application does not perform any cross-domain routing/switching/connecting shortcut. 3. Ensure unauthorised communications between domains are prohibited or processed via a Firewall.
ARCH-005	**Design Security Zones for the different layers and exposure elements,** to have resource isolation depending on the criticality of the processing	1. Ensure the affinity/anti-affinity rules are designed to protect sensitive processing/forwarding resources. 2. Design the Zoning based on the application requirements. 3. Design the Zoning based on protocols and technology generation. 4. Design the Zoning based on legal and operational domains e.g. large operators with shared infrastructure. 5. Plan the exposed zones (to the internal/external environment) to ensure the exposed applications do not share resources with sensitive applications. 6. Use Virtual Communication Steering mechanisms like micro segmentation to protect sensitive data from external interference. 7. Implement physical separation between each of the network domains, for example, through the use of separate ToR (Top of Rack)

Reference	Objective	Solution Description
		switches and EoR (End of Rack) switches for each network domain. 8. Implement firewalls and associated policies at the ingress to each network domain. 9. Implement firewalls and associated policies at the inter-domain interconnection points. 10. Implement ingress firewalls and associated policies on external service interfaces to protect against external attack vectors.
ARCH-006	**Ensure Secure Communication** by authenticating the peering and using specified secure protocols and APIs for the interaction. This applies for internal and external layers.	1. Based on ARCH-003/004 the Communication paths have been identified. 2. Verify only the allowed paths are able to be established. 3. The peering for the communication paths need to be authenticated before establishment. 4. Unified authentication methods have to be used. 5. Secure protocols or secure APIs have to be used for all kinds of external critical intercommunication. 6. Unified authentication methods should be used.
ARCH-007	**Apply adequate security measures to Edge computing areas/datacentres** to ensure secure handling of information, including traffic separation.	1. Use appropriate measures to protect the edge datacentre like: Define Security groups, ACLs, or use virtual firewalls to isolate virtual networks. 2. The platform has to monitor the processing of the virtual resources in real time, detect malicious behaviours, and raise and isolate alarms in a timely manner.
ARCH-008	**Protect the User Plane and ensure the integrity of the Data Streams** by applying E2E Data Security measures.	1. Confidentiality and integrity protection of external data streams, in the same manner as for anti-replay protection for related interactive data streams to prevent a man in the middle attack, has to be implemented.
ARCH-009	**Cyber Resilient System, Availability Planning and Disaster Recovery.**	1. Network architectural design should include end to end disaster recovery plans aligned with ISO 27031. 2. Network architecture should clearly define availability and recovery mechanisms which would satisfy

Reference	Objective	Solution Description
		Recovery Point and Time Objectives (RPO/RTO). 3. Network architecture design should incorporate availability planning with clearly defined availability KPIs e.g. MTTR, MTBF, MTTF and real-time availability monitoring. 4. MNOs should evaluate based on their risk assessment and resiliency strategy (BCM-015): • Which of the 14 NIST SP 800-160 vol.2 Cyber Resiliency Techniques should be incorporated into the network architectural (Adaptive Response, Analytic Monitoring, Contextual Awareness, Coordinated Protection, Deception, Diversity, Dynamic Positioning, Non-Persistence, Privilege Restriction, Realignment, Redundancy, Segmentation, Substantiated Integrity and Unpredictability) • MNOs should carefully consider the minimal set of cyber resiliency Techniques which satisfies the organizations strategic cyber resiliency objectives and adhere to the Keep It Simple security design principle.
ARCH-010	**Protect, Isolate and secure connections to externally hosted services**, specifically services with direct access to the 3GPP network that operate outside the operators' control e.g. RCS connected to the IMS.	1. Establish network layer (IP) isolation which supports integrity, confidentiality and replay protection for hosted services with access to the 3GPP network. 2. Allow only protocols and ports that are actually needed on the network. Block all other protocols. 3. Implement rate control on ingress traffic originating from hosted services towards the 3GPP system.
ARCH-011	**Implement Network (IP) Layer and Transport Layer filtering, mitigate traffic spoofing** specifically at the network edges (IPX/GRX/DN) and ANs (3GPP/non-3GPP) to protect against	1. On the network layer, filter traffic at the edge of each network based on source and destination IP addresses. 2. On the transport layer, only specifically allow the application layer protocols that are actually needed on

Reference	Objective	Solution Description
	UEs / Internet endpoints spoofing operators' NEs / resource IPs.	the network or for particular communication partners. Filter and block all other protocols. 3. Install a packet filter firewall on the network edge exposed to the internet. 4. Install a packet filter on the network edge exposed to the GRX/IPX. 5. Install a packet filter on the network edge exposed to a non-3GPP access. 6. Implement IP anti-spoofing, for IP traffic originating from UEs via 3GPP and Non-3GPP ANs as well as for traffic originating from IPX/GRX/DN traffic.
ARCH-012	**Align the security architecture with domain, service and protocol specific GSMA standards.**	1. GTP Security – FS.20, FS.37 2. SIP Security – FS.38 3. SMS Security - SG.22, FS.42 4. RCS Security – FS.41 5. VoLTE Security – FS.22 6. NFV Security – FS.33 7. Algorithms Security - FS.35 8. Interconnect Security • Interconnect Signalling – FS.21 • Inter-operator IP Backbone Security - IR. 77 • Diameter Interconnect Security FS.19 • 5G Interconnect Security FS.36

2.2.6 Network Infrastructure Controls

These controls are likely to be understood and managed by the network service architecture/engineering team.

2.2.6.1 Security Network Function Virtualisation Infrastructure (NFVI) Controls

These controls are likely to be understood and managed by the Data Centre Infrastructure management teams.

Given the complexity of the Network Function Virtualisation Infrastructure, a layered approach is proposed to address each of the following logical layers of the NFVI in turn:

- Virtualisation Controls;
- Network Controls;
- Storage Controls;
- Management Controls.

- Container Controls

2.2.6.1.1 Virtualisation Controls

Reference	Objective	Solution Description
NFVI-VS-001	**Maintain the security of the Host (OS) Operating Systems,** running within VMs deployed on the NFV Infrastructure to prevent penetration from unauthorised sources and hijacking by rogue VMs (Virtual Machines).	1. Configure OS, disabling insecure services, such as Telnet, rlogin, TFTP, etc. and enable secure transmission protocols, such as HTTPS, SSH, SFTP. 2. Remove all optional operating system components that are not required by the virtual machine functionality. 3. Maximise and maintain file directory permissions and set and enforce read, write, execute and role-based permissions. 4. Delete all unnecessary user accounts and default system accounts, such as guest logins. 5. Implement a patch management policy in order to ensure OS software is kept up to date. 6. Install all feature updates and security patches as and when provided by the OS vendor.
NFVI-VS-002	**Prevent attacks through the deployment of rogue VMs**, which could be used to gain unauthorised access to the NFV Infrastructure and facilitate data leakage. CCM3.0 - IVS-02	1. Ensure the integrity of all VM images at all times. 2. Securely store all VM images and snapshots to prevent unauthorised access and tampering. 3. Implement access security controls to image repository systems in order to limit access by unauthorised personnel. 4. Conduct software malware detection testing to identify malicious code before images are deployed. 5. Implement controls that ensure uploading, updating and downloading of VM images are authenticated. 6. Implement integrity verification of VM images through the use of digital signatures, for example SHA-256, during verification, loading and updating. 7. Ensure VM images are encrypted during storage and uploading using industry standard encryption algorithms. 8. Implement policies and mechanisms that ensure all residual data associated with a VM are erased on termination of the VM for both normal and abnormal

Reference	Objective	Solution Description
		termination cases in order to prevent data leakage. 9. Any changes made to VM images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). 10. The results of a change or move of an image and the subsequent validation of the image's integrity, must be immediately available (SIEM, Audit Portals, etc.).
NFVI-VS-003	**Ensure the resilience of physical hosts supporting multiple VMs** against resource competition and overload risks that could potentially lead to physical host collapse. CCM3.0 IVS-04	1. The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload. 2. Implement mechanisms that ensure vCPU Scheduling Isolation by binding vCPUs to a single thread of a pCPU core, such that a pCPU thread can only be accessed by one VM and cannot be accessed by other VMs for the lifecycle of the VM. 3. Implement Virtual Memory Isolation by ensuring that each VM has its own dedicated memory space. Ensure that during creation of a VM the memory size is specified and put in place systems to verify that sufficient memory is available on a node to support the invocation of the VM and deny the invocation if insufficient memory is available. 4. Implement Internal Network Isolation through the implementation of suitable virtual interface technologies, such as DVS including micro segmentation and SR-IOV with leaf switch separation, in order to provide mechanisms that prevent conflicts between VMs accessing virtual ports and vNICs.
NFVI-VS-004	**Ensure boot integrity to protect server hardware and BIOS/UEFI firmware against tampering and penetration attacks,** which could further be used to penetrate VM OSs	1. Harden firmware configurations by disabling unused services. 2. Maintain, update and patch all firmware, as and when updates are provided by the hardware/firmware vendor.

Reference	Objective	Solution Description
	and Hypervisor APIs, thereby increasing the attack surface of the NFV infrastructure.	
NFVI-VS-005	**Protect the Hypervisor layer against penetration attacks and access by rogue VMs,** which could increase the attack surface of the NFV Infrastructure, from external attacks, VM escape and internal DDoS attacks.	1. Maintain, update and patch hypervisor software, as and when updates are provided by the hypervisor vendor. 2. Harden the hypervisor software to disable all unused services or enable services only when needed. 3. Implement a robust password policy for use with hypervisor administration accounts [see, NVFI-MS-001 for more details].
NFVI-VS-006	**Prevent tampering, interception, eavesdropping and replay threats** from Man in the Middle attacks to the VIM (Virtual Infrastructure Manager) interfaces.	1. Implement mutual authentication between the VIM and other NFV Infrastructure components, namely NFVM (Ni-Vnfm interface), NFVO (Or-Vi interface) and virtualised resources (Nf-Vi interface), as specified in [74]. 2. Implement encryption, integrity protection and anti-replay protection on the communication interfaces between the VIM and other NFVI infrastructure components using, for example, IPSec and/or TLS tunnels.
NFVI-VS-007	**Prevent data leakage and exposure of sensitive information** of all backup data managed in the VIM.	1. Store all backup material managed in the VIM in encrypted form. 2. Apply access control mechanisms and password protection [see, NFVI-MS-001] to the management of the backup and restore processes and files.
NFVI-VS-008	**Prevent tampering and unauthorised reconfiguration of physical hardware devices**, which could introduce potential vulnerabilities to attack vectors and potential data leakage from exposed external interfaces.	1. Put in place physical access controls to all equipment rooms and remote locations in which NFV infrastructure is installed. 2. Implement policies for controlling access and preventing access of unauthorised personnel to equipment rooms and remote locations, including for example the issuing and usage of security passes, access cards, (i.e. key cards), etc. 3. Log and review all accesses to equipment rooms and locations. 4. Ensure the policies for controlling access, include mechanisms for the revocation of access on staff turnover and include regular reviews of issued physical access authorisations.

Reference	Objective	Solution Description
NFVI-VS-009	**Infrastructure & Virtualization Security, Clock Synchronisation** CCM3.0 IVS-03	1. A reliable time source shall be used to synchronise the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.
NFVI-VS-010	**Infrastructure and virtualisation resiliency**	1. Operators should implement high availability for vital infrastructure resources where critical assets shall be deployed, specifically Compute, Object Storage, Block Storage, Shared File Systems, Networking, Dashboard, Identity service, Image service and Data processing service 2. Where NFVI message passing technologies shall be used e.g. for service communication such as MQ/ AMQP should be deployed in Highly Available mode when feasible, based on the design workloads criticality.

2.2.6.1.2 Network Controls

Reference	Objective	Solution Description
NFVI-NS-001	Where SDN Controllers are deployed to manage the networking environment within the NFV Infrastructure, **prevent unauthorised access to the controller management interface** that may lead to deliberate or accidental misconfiguration of the NFV Infrastructure platforms resulting in increased vulnerability to attack vectors and sensitive data leakage.	1. Implement and enforce access control mechanisms on the SDN Controller management interfaces [see, NFVI-MS-001]. 2. Implement SSH to protect system access and IP based ACL to implement restrictions on IP addresses that can be allowed for remote access. 3. Implement encryption, integrity protection and anti-replay protection on communications over the northbound interface of the SDN Controller by using, for example, HTTPS in the case where the interface is based on RestConf.
NFVI-NS-002	Where SDN Controllers are deployed to manage the networking environment within the NFV Infrastructure **prevent tampering, interception, eavesdropping and replay threats** from Man in the Middle attacks by a rogue SDN Controller.	1. Implement encryption, integrity protection and anti-replay protection on communications on the southbound interfaces using, for example, SSH to secure the NetConf interfaces, and TLS for Openflow and PCEP interfaces.
NFVI-NS-003	Where SDN Controllers are deployed to manage the networking environment within the NFV	1. Monitor resource utilisation of the SDN Controller and raise alarms and take

Reference	Objective	Solution Description
	Infrastructure **protect the SDN Controller against Distributed Denial of Service attacks.**	mitigating actions upon discovery of unexpected resource usage. 2. Use a clustered SDN Controller architecture to disperse attack points. 3. Implement and configure multi-level speed limit and multi-level traffic scheduling functions in SDN forwarding layer. 4. Define and rate limit the number of packets forwarded per QoS queue within the forwarding layer. 5. Implement source based dynamic abnormality detection to monitor and block abnormal message loads. 6. Implement flow tables protection by detecting and monitoring flow control messages for abnormal behaviour and deny DDoS attacks.
NFVI-NS-004	Where SDN Controllers are deployed to manage the networking environment within the NFV Infrastructure **protect the integrity of the SDN forward routing protocols** against interception.	1. Implement routing protocol security, by using authentication, for routing protocols such as OSPF, RIP, and BGP.
NFVI-NS-005	Where SDN Controllers are deployed **prevent and mitigate the element takeover of the SDN forwarder**.	1. Implement reauthentication processes of the SDN forwarder to the SDN controller. 2. Implement process validation for forwarder system processes (check all processes and routines running on the forwarder are in the expected range, and no unauthorised processes are active). 3. Validate regularly the active status on the forwarder with those planned in the controller. 4. Carry out a link and system load verification for interfaces and processes on the forwarder.
NFVI-NS-006	vSwitch Security	1. When vSwitch supports promiscuous mode, set it to reject by default to prevent attackers sniffing and capturing all the traffic in same VLAN going through vSwitch. 2. Prevent MAC address changes. Prevent OS from changing the MAC Address to reduce the ability of attackers to spoof and/or hide VMs identity.

Reference	Objective	Solution Description
		3. Mitigate ARP spoofing – vSwitch should enable ARP spoofing protection i.e. match source ARP address. 4. Prevent MAC flooding, if vSwitch switches use a content-addressable memory (CAM) table to learn and store the source address for each packet, attacker can flood these CAM tables forcing the switch to broadcast on all ports. 5. Prevent 802.1q and ISL tagging and do not permit dynamic trunking.
		6. Protect Double-encapsulation attacks, drop any double-encapsulated frames that a virtual machine attempts to send on a port configured for a specific VLAN. 7. Prevent Spanning-tree attacks – don't allow Bridge Protocol Data Unit (BPDU) to be sent from VMs to prevent attackers sending packets to change the network topology. 8. When distributed vSwitch - ensure that Netflow traffic is only sent to authorised collector IP addresses. Netflow exports may not support encryption and can contain information about the virtual network. 9. Ensure that ports are not configured to the value of the native VLAN. Some vSwitches and physical switches use VLAN 1 as their native VLAN. Frames on a native VLAN on some platforms are not tagged with VLAN tag 1. This can cause a security issue bypassing VLAN tagging. 10. Ensure ports are not configured to VLAN values reserved for physical switches. Using a reserved VLAN might result in a denial of service on the network. 11. Ensure ports are not configured to VLAN 4095. Some platforms reserve VLAN 4095 for Virtual Guest Tagging (VGT) allowing the Guest OS guest to assign VLAN tags to outbound traffic. 12. Disable port-level configuration overrides. Some vendors' vSwitches support the ability to override at the port level the security policy set at the port

Reference	Objective	Solution Description
		group level, thereby allowing VMs to setup specific port security policies. 13. Ensure that if vSwitch supports port mirror traffic, it is sent only to authorised ports/VLANs. Often, port mirroring sends a copy of all specified traffic in unencrypted format, allowing attackers to view all traffic. 14. When possible, deploy vSwitch which supports high availability e.g. in Open vSwitch (OVS) or Linux bridge with VRRP. 15. When possible set QoS rate-limiting policies on VMs, reduce the ability of a compromised VM to DoS the vSwitch / Distributed vSwitch and reduce network availability for other NFs
		16. Disable SR-IOV capabilities for the vSwitch. SR-IOV allows VM direct access to the physical HW and therefore performance improvements. However, it reduces the visibility and allows a compromised or malicious workload to bypass port-based security controls such as disable spoof checks, disable rate limitation, and even impact other VMs. Some virtualisation platforms and modern network cards provide stricter control even when SR-IOV is used; however, operators should avoid the use of SR-IOV when executing workloads with limited trust or control.

2.2.6.1.3 Storage Controls

Reference	Objective	Solution Description
NFVI-SS-001	**Prevent unauthorised access to stored data** to ensure VM resilience and prevent leakage of sensitive data and storage resilience.	1. Ensure storage isolation by implementing policies that ensure VMs can only access their own resources. 2. Assign distinct storage clusters to specific host clusters. 3. Ensure isolation of storage resource pools between different tenants, i.e. ensure storage resource pools of each tenant are isolated from other tenants. 4. Implement mechanisms to ensure tenants can only access resource pools for which they are authorised within the

Reference	Objective	Solution Description
		wider NVF Infrastructure management systems. 5. Implement IOPS (Input/Output Performance) measures on LUN (Logical Unit Number) configured disk storage to limit and to provide to each LUN dedicated overload protection. 6. Assign different dedicated LUNs for different functions.
NFVI-SS-002	Ensure newly VM bound storage or re-bound storage is empty and cannot contain malware or leftovers.	1. Verify the existing and in service storage configuration and VM assignment before creating/instantiating new VMs. 2. In the VM instantiation process ensure new unused LUN IDs and storage termination IDs are used. 3. In the storage instantiation process (establishment of the LUN relations, IOPS configuration, storage configuration) ensure the assigned storage space is empty (formatted). 4. During the VM to storage binding process, before the VM is using storage, verify the empty file/block structure situation by checking the storage (size, free space, files/blocks used).
NFVI-SS-003	Ensure the content in the storage is stored safely and can only be accessed by authenticated and authorised clients (VNFs)	1. Verify that encryption is enabled for any type of storage content. 2. Enable e.g. CHAP authentication to allow only authenticated and authorised initiators access to the LUN groups. 3. Set a password for bidirectional access e.g. CHAP authentication.

2.2.6.1.4 Management Controls

Reference	Objective	Solution Description
NFVI-MS-001	**Protect all NFV Infrastructure management systems,** including VIM and hypervisor management systems **from unauthorised access** that could lead to deliberate or accidental misconfiguration of the NFV Infrastructure platforms resulting in increased vulnerability to attack vectors and sensitive data leakage.	1. Implement and enforce a rights and domain based access control policy with defined user roles, in which different defined roles have clearly specified and enforced access rights. 2. Implement a robust password policy that applies to each user and is associated with the role of that user within the rights and domain-based access control policy that: • Ensures user password complexity, by undertaking weak password checking.

Reference	Objective	Solution Description
		• Ensures passwords stored in the system configuration files are encrypted. • There is a life cycle for passwords, requiring passwords to be changed after a defined period. • Implements a password dictionary to forbid recently used passwords. • Implements account lock out for a defined time period in the event of a defined number of consecutive failed log-in attempts. 3. Implement for high-risk border connection points an appropriate authentication mechanism, such as multi factor authentication, to validate the user permissions. 4. Implement an access logging system, which allows track and trace of all system accesses and user actions against the user's log-in identity. Maintain a scheduled backup of the track and trace logs. Define and implement policies to define the period for storage of trace backups.
NFVI-MS-002	**NFV Infrastructure API Protection**	1. Protect and isolate all NFVI endpoints. 2. Isolate NFVI endpoint at the network level based on allow-list access. 3. Enable, when supported at least TLS 1.2 access to API endpoints. 4. Monitor and alert any unauthorized attempt to NFVI APIs.

2.2.6.1.5 Container Controls

This section describes objectives and controls for containers that are used to deploy services within the NFV infrastructure of a mobile operator. Annex B.1.1 provides some background on containers.

Reference	Objective	Solution Description
CC-001	Container Image countermeasures to guard against vulnerabilities, misconfiguration, malware, embedded secrets, untrusted image sources, etc.	1. Container images should only be created from trusted sources and trusted base images. 2. Container images should be continuously scanned for vulnerabilities and malware. 3. Container images should be Integrity protected and stored in tamper resistant storage.

		4. Container images should be uniquely identifiable by cryptographic signature, container image names should be immutable that specify discrete versions 5. Containers should be scanned to identify a misconfiguration, and validate configuration settings against vendor recommendations, MNO policies and industry best practices. 6. Container images should not contain embedded Secrets, instead 'just in time' injection via secret management services should be used. Appropriate certified secret management systems should be used for secret management of critical assets, based on global certification requirements, such as ISO 19790, GB/T 37092, FIPS 140-2/140-3, etc. 7. Ensure that unnecessary packages are not installed in the container. 8. SSH and other remote administration tools designed to provide remote access to the hosts should never be enabled within containers. 9. Ensure images are scanned and rebuilt to include security patches. 10. Ensure that health check instructions have been added to container images. 11. Set least privilege access for container packages, e.g. remove setuid and setgid from packages which don't require it. 12. Ensure only verified packages from trusted sources are added to the image.
CC-002	Container Registry countermeasures to protect against insecure connections to registries, stale images in registries and unauthorised access to registries	1. Development tools, orchestrators, and container runtimes should only connect to registries over secure channels. 2. Centrally managed internal registries should only be the image repositories available for production workload deployments. 3. Automatically delete registries of unsafe, vulnerable images that should no longer be used. 4. All access to registries should require authentication and authorisation, and mutual authentication should be used. 5. Any write access to a registry should ensure that only images from trusted entities can be added.

		6. Container images added/modified in the registry should be scanned for vulnerabilities, misconfigurations and malware before they are allowed into the registry. 7. The registry should be encrypted at rest. 8. Network access to the container registry should be restricted and isolated at the network layer.
CC-003	Container countermeasures	1. Containers should be executed in an immutable manner. 2. Ensure containers are not able to send traffic across networks of differing sensitivity levels. 3. Ensure traffic between containers is restricted (often containers on the same host can communicate directly), by restricting all inter-container communication. When inter-container communication is needed, link specific containers together e.g. via custom network connection. 4. Ensure host system directories are not mounted on containers. 5. Ensure privileged ports are not mapped within the containers. 6. Ensure only needed ports are opened on the container. 7. Ensure containers run with the minimal set of file system permissions required. 8. Ensure, when needed, specifically allocated storage volumes are used for container persistence and, avoid mounting local host filesystem.
CC-004	Orchestrator countermeasures	1. Ensure all hosts in the environment only run images from the approved lists. 2. Validate image signatures **before** image execution. 3. Access to cluster-wide administrative accounts should be tightly controlled. Enforce least privilege access model in which users are only granted the ability to perform specific actions on specific hosts, containers, and images essential to their roles. 4. Orchestrators should be configured to separate network traffic into discrete virtual networks by sensitivity level/per-app/workload segmentation.

		5. Orchestrators should be configured to isolate deployments to specific sets of hosts by sensitivity levels. Workloads of different sensitivity levels should not be allowed to execute on the same host. 6. Orchestrators should ensure that nodes are securely introduced to the cluster, have a persistent identity throughout their lifecycle, and can also provide an accurate inventory of nodes and their connectivity states. 7. Orchestration platforms should be designed specifically to be resilient to the compromise of individual nodes without compromising the overall security of the cluster. 8. It must be possible to isolate and remove a compromised node from the cluster without disrupting or degrading overall cluster operations. 9. Orchestrators should provide mutually authenticated network connections between cluster members and end-to-end encryption of intracluster traffic. 10. Ensure minimum number of management nodes have been created. 11. Ensure all orchestrator services are bound to specific host interfaces. 12. Ensure all virtual overlay network communication paths are isolated to ensure confidentiality, integrity and replay protection. 13. Ensure secret management is used for managing secrets in the cluster. 14. Ensure node certificates are rotated as appropriate. 15. Ensure CA certificates are rotated as appropriate. 16. Ensure management plane is separated from data plane traffic.
CC-005	Container Runtime Countermeasures	1. Ensure all hosts in the environment execute only images from the approved lists. 2. Validate image signatures **before** image execution. 3. Automatically monitor container runtime for vulnerabilities, misconfigurations and malware. 4. Ensure, if applicable, an AppArmor Profile is enabled.

		5. Ensure, if applicable, SELiunx security options are set. 6. Ensure, if applicable, that Linux kernel capabilities are restricted within the containers. 7. Ensure, if applicable, that privileged containers are not used, re-map containers to less-privileged users e.g. via user namespace (if possible) 8. Ensure, if applicable, that host's network namespace isn't shared. 9. Ensure that hosts memory usage is limited. 10. Ensure that CPU priority is set appropriately on containers. 11. Ensure, if applicable, container root filesystem is mounted in read only. 12. Ensure, if applicable, inbound traffic is bound to specific host interfaces. 13. Ensure, if applicable, host's process namespace isn't shared. 14. Ensure, if applicable, host's IPC namespace isn't shared. 15. Ensure devices are not directly exposed to containers. 16. Ensure, if applicable, Seccomp profile is enabled. 17. Ensure, if applicable, that cgroup usage is confirmed. 18. Ensure containers are restricted from acquiring additional privileges. 19. Ensure container health is checked at runtime.
CC-006	Host OS / Infrastructure Countermeasures	1. Ensure all authentication to the OS is audited.
CC-007	Container Monitoring, Logs and accounting	1. Perform continuous monitoring of the repositories and images to ensure images are maintained and updated as vulnerabilities and configuration requirements change. 2. Ensure continuous monitoring of all access to production repositories. 3. Detailed logs shall be created and securely forwarded on any access to the repositories (Human or machine) 4. Maintain detailed accounting of all cluster activities, monitor all cluster activities, automatically align (time-base) cluster

		activities across the different cluster components. 5. Continuously monitor containers activities, specifically resources access and resource usage. Detect and notify on access or usage violations. 6. Automatically determine proper container networking surfaces, including both inbound/outbound ports and process-port bindings. 7. Monitor and detect traffic flows both between containers and other network entities, over both 'on the wire' traffic and encapsulated (overlay) traffic. 8. Detect network anomalies, such as unexpected traffic flows within the network, port scanning, or outbound access to potentially dangerous destinations.
CC-008	Container Platform Management	1. Maintain a set of trusted images and registries and ensure that only images from this set are allowed to run in their environment. 2. Centrally control exactly what images and registries are trusted and in which deployment /execution environments. 3. Enforce network layer isolation to protect administrative (APIs) and control interfaces across the cluster (Orchestrator, Registry, Host), and require authentication and authorisation over secure channels (e.g., at least TLS 1.2) to these when accessing these interfaces from secure network domains.

2.2.7 Network Services Controls

These controls are likely to be understood and managed by the network service architecture/engineering team.

Reference	Objective	Solution Description
NS-001	Slicing Authentication and Authorisation	1. Operators should consider use as a default slice-specific authentication and authorization as defined in 3GPP 23.501 5.15.10 - Network Slice-Specific Authentication and Authorisation.
NS-002	Slice lifecycle Security	1. Ensure that the management (creation, modification, and termination) of a Network Slice Instance is protected through mutual authentication and authorisation of the consumer residing

		outside the 3GPP operator's trust domain (see [60] - section 15)
NS-003	Protection between management service consumer and the management service producer	1. Provide integrity protection, replay protection and confidentiality protection between the management service producer and the management service consumer residing outside the 3GPP operator's trust domain (see [60]).
NS-004	Slice Template Security	1. Identify the specific service requirements of each vertical industry to which the network slice is assigned. 2. Security requirements may be very different from industry to industry. Appropriate technical solutions should be defined to meet these requirements and comply with the requirements and solutions defined by 3GPP (see 3GPP TR 33.813 - Security Aspects; Study on Security Aspects of Enhanced Network Slicing (Release 16) 3. Create slice templates based on GSMA NG.116 specification 4. Ensure slice templates are stored securely with appropriate access controls and tamper protected. 5. Utilise templates and automation to control network slices lifecycles and minimise manual customisations.
NS-005	Slice Isolation	1. Use of IPSEC tunnel per slice / or some other isolation mechanism may be considered appropriate that would extend from RN-TN-CN and maybe additional controls beyond to include OSS/BSS and NEF. 2. Operators should consider that some verticals would like to have control at the network level and not just the application level over the isolation e.g. control the keys generate to establish the isolation layer.
NS-006	Slice Monitoring, Logging and Auditing.	1. Slice specific logs and log traffic may be required and requested by customers and these need to be securely handled to comply with data retention, and other, regulations.
NS-007	Slice specific IE authorisation and control.	1. Validate if the authorisation claims match the API request information content. In particular, if presented with user identifiers (e.g. IMSI, charging id) check that they belong to the slice authorised

		by the token and the authenticated identity on the transport layer. 2. Operators should define and adhere to security rules, that are regularly reviewed and revised in light of emerging threats, to avoid data leakage and unauthorised actions.
NS-008	Slice information authentication token cross-validation by NF-producer	1. Presented authorisation token should contain not only service level and instance id but also the validated slice-identity information of the NF-consumer. This information is then extracted and validated for correctness and consistency with presented information on the transport layer by the NF-producer. The transport layer information might not be sufficient and a mapping between slice-id and NF information is needed.
NS-009	Application Function Security Controls	1. The network may host application functions for specific services or as part of one or several slices. The communication from and to those application functions need to correspond to the service consumed and the service provided (and potential service level agreement). Security monitoring, filtering on application layer and enforcement of authentication and authorization need to correspond to this. 2. Enforcement of security zones, if application function is not the same security / trust level as the network function it communicates with. *3.* Anomaly monitoring to prevent horizontal movement of an attacker on transport and application layer.
NS-010	Slice header information cross-validation	1. If a slice-id is presented in the header information e.g. OCI, then it should be validated that the identity in the OCI header is the same as in the authorisation token and that the authentication information on the transport layer matches with this slice.
NS-011	Non-guessable unique Slice names	1. An operator should avoid using guessable slice-ids. The SD part of the S-NSSAI is recommended to be random. No two slices should use the same S-NSSAI.

2.2.8 Core Network Management Controls

The Core Network (CN) definition has been taken from the 3GPP standards[3]. These controls are likely to be understood and managed by the Core Services Management.

Reference	Objective	Solution Description
CN-001	There should be processes for the **secure provisioning and decommissioning of users** to ensure only legitimately subscribing customers have access to services.	1. User ID (no wildcards) 2. Correct linkage between customer and UE 3. Authenticate every user on every network attach, location update, traffic event, etc. 4. Implement know your customer (KYC) systems and initiatives
CN-002	**Protect core network traffic** after it is handed over from the radio path to protect against unauthorised interception and alteration of user traffic and sensitive signalling information.	1. Deploy encryption to protect the interface between eNodeB/gNodeB and the core network e.g. by using IPsec 2. Enable end entity certificates as defined in 3GPP TS 33.310 [40] 3. Actively manage GTP_U and GTP_C / SEPP firewalls between the core network and IPX network, dropping malformed packets before they leave the core [33]
CN-003	**Prevent eavesdropping, the unauthorised deletion and modification of voicemail** content, settings and greetings and call break out to generate fraudulent traffic.	1. Enforce use of unobvious, variable length access PINs [41] 2. Notify customers of failed access attempts [41] 3. Require PIN entry for direct access to voicemail from outside home network, except in cases where the Calling Line Identifier can be reliably assured to be correct [41] 4. Restrict the number of PIN access attempts independently from the Calling Line Identifier [41] 5. Securely generate, distribute and manage PINs [41] 6. Set the frequency at which a new or replacement temporary identifier is allocated to provide adequate protection
CN-004	Use **customer anonymisation techniques** to protect identifiers that can be used to identify and track individual customers.	1. Enable the use of temporary identifiers for customers, as defined in the standards [42], [43]
CN-005	**Prevent unsolicited messaging traffic** (RCS, SMS and MMS) reaching unsuspecting customers and causing potential harm to the	1. Configure available SMSCs, STPs and SMS firewalls to reduce risk of OTA SMS attacks [44], [15] 2. Deploy SMS home routing to ensure visibility and control of messaging traffic

Reference	Objective	Solution Description
	network, including denial of service against network elements.	3. Deploy traffic filtering capabilities on the network GGSN, MMSC, SMSC, SMSF and/or STP 4. Provide customer facing spam reporting and blocking capabilities
CN-006	To prevent fraudulent activity **regular reconciliation of systems** is required.	1. Perform regular reconciliation of Call Data Records on switches, billing systems, etc. 2. Perform regular reconciliation of active subscriber profiles on networks and billing systems 3. Perform regular reconciliation of prepaid designated subscriptions on IN platforms
CN-007	**Control which devices can access the network** to protect against the connection of counterfeit, stolen and substandard devices and possible network impacts they may have.	1. Block duplicate or invalid IMEI / PEI numbers [45]. 2. Deploy Equipment Identity Register or equivalent technology capable of monitoring and blocking use of individual devices based on their IMEIs [13] 3. IMEI checks should carried out to confirm the device identify prior to providing mobile network access [45] 4. Validate device IMEIs using other techniques such as browser user agent profile checks.
CN-008 / CIS - 014	The **processes and tools used to track/control/prevent/correct secure access to critical assets** (e.g. core infrastructure) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	1. Enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. 2. Disable any account that cannot be associated with a business process or business owner. 3. Ensure that all accounts have an expiration date that is monitored and enforced. Automatically disable dormant accounts after a set period of inactivity. 4. Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. 5. Enforce detailed audit logging for access to sensitive data or changes to sensitive data.

2.2.8.1 Mobile Edge Computing Platform

This section describes objectives and controls for services running on a Mobile Edge Computing (MEC) platform. Annex B.2.1 provides some background on MEC.

Reference	Objective	Solution Description
EC-001	The network capability exposure may enable some services and/or network related data to be shared. The network function exposure interface adopts common Internet protocols, which makes the **existing security risks of the Internet** a further threat to 5G networks which **need to be protected against**.	1. Ensure integrity protection, replay protection and confidentiality protection on the network function exposure interface to the Application Function [57]. 2. Provide mutual authentication and ensure the Application Function is authorised to interact with the relevant network functions [57]
EC-002	**Securing access of verticals** to core network services and functions	1. Access and authorisation controls for third parties using core network services (e.g. Multi-access edge computing (MEC), Public Network Integrated Non-Public Network (PNI-NPN). 2. Authorisation and access controls to core network data by third parties that provide applications for the MEC. 3. Filtering for third party access for unwanted traffic and attacks.
EC-003	**Prevent MEC Applications from attacking MEC platform** / Virtualization / Hardware layer recognising that applications may contain malicious code and/or abuse their privileges. Note: MEC should be viewed like a public cloud with similar adversaries and attack vectors.	1. Block local application deployment except for emergency cases, and alert on any attempts to deploy applications locally to block bypass of central orchestration and monitoring. 2. Block installation and execution of unsigned applications. Workloads should be signed by operators or a trusted party to prevent installation and/or execution of unauthorised workloads. 3. Prevent, alert and when mandated, disable high risk workloads from deployment and execution on the MEC platform to reduce the MEC attack surface. 4. Workloads should execute with least privilege access. Access to MEC's privilege APIs/ services/ resources, should be monitored and restricted based on approved lists, and identify and block fuzzing, and scanning to prevent attacks from applications residing on the MEC platform. 5. Isolate workloads, by using multi-layered isolation between workloads and MEC platform to prevent workloads escaping the process sandboxes. 6. Isolate workload resources, specifically compute, memory, storage and network,

Reference	Objective	Solution Description
		separate MEC control and management networks from workload networks, and utilise confidentiality, integrity and replay protection mechanisms to prevent bypass / isolation break-out and spoofing/ injection into MEC platform internal functional domains. 7. Prevent direct pass-through, and malicious workloads that may bypass MEC policies by exploiting direct access to virtualisation layer/ HW resources, thereby violating MEC policies and overcoming MEC security. 8. Enforce strict rate controls (network, CPU) and resource quotas (CPU, memory, storage) to prevent DoS and/or resource exhaustion on MEC platform. 9. Utilise dedicated resources for MEC platform system level services i.e. OSS and MEC orchestrator to reduce the attack surface against critical MEC services by the application. 10. Utilise dedicated resource allocation for local MEC services (MEC platform manager, VIM, service registry, DNS handling, traffic rule control) and, when possible, execute their critical sections within a trusted execution environment to minimise the attack surface of control services executing on the same host as the workloads. 11. Prevent workloads and/or services from performing memory/process/kernel dumps to prevent a malicious workload with privileged access from performing memory/process dumps on other processes in order to steal in-memory credentials / tokens. 12. When executing workloads with lightweight virtualisation technologies e.g. containers, ensure that the associated processes enable data execution prevention (DEP/Nx), ASLR and Stack Protection to reduce the ability of malicious workloads from escaping the process sandbox. 13. Mount workloads OS/kernel/resources when possible, in read-only mode to reduce the attack surface by removing kernel/OS modification.

Reference	Objective	Solution Description
		14. Prevent mounting of sensitive system folders/files and/or sharing/providing access to sensitive folders/files to reduce the attack surface by minimising the ability of malicious apps to gain access or monitor privileged resources. 15. Use true random number generators for cryptographic operations to minimise the ability of applications to predict and or influence cryptographic operations by MEC. 16. Detect and prevent application attacks against hardware vulnerabilities e.g. row hammering, speculative execution (Meltdown, Spectre), L1TF/Foreshadow, Zombieload, etc. to detect and prevent security bypass.
EC-004	**Protect MEC Applications from other Apps / Services executing on the same MEC platform** / MEC cluster to prevent malicious apps attacking other applications executing on the same MEC platform/cluster in order to obtain information (information leakage), disrupt services (DoS), bypass access restrictions (unauthorised access). Note: MEC should be viewed similarly to a public cloud with similar adversaries and attack vectors.	1. Enforce strong workload resource isolation, specifically compute, memory and storage to prevent cross workload isolation break-out / attacks. 2. Workloads of different MEC tenants and/or different sensitivities should have dedicated networks (virtual and/or containerised overlay), and network traffic should be confidentiality, integrity and replay protected. 3. Virtual and physical interfaces should be restricted. Source (MAC/IP) protection should be enforced, at the very least, at the virtual switch/bridge. 4. Inter-host and intra-host communication policy should by default deny, i.e. prevent all communication between workloads/services unless specifically allowed. 5. Workloads must be set with resource quotas (CPU, memory, storage, IOs, Network). A default resource policy should be set for every workload which doesn't have a custom resource policy to prevent resource abuse, and resource exhaustion. 6. Fine grained real-time rate controls should be enforced on access, internal resources (Memory, IO, Network, CPU) and MEC API resources (location API, Radio Network Information API, Fixed Access API, V2X Information API, WLAN

Reference	Objective	Solution Description
		Information, Traffic Management, etc.) to prevent application DoS / SLA violations.
EC-005	MEC platform to **protect, isolate and monitor MEC network services**: APIs, O&M interfaces, from access by unauthorised parties, including users and malicious or compromised services.	1. Network level isolation of all control and management interfaces specifically HW management, virtualisation and MEC platform to minimise the attack surface and prevent unauthorised network access to critical interfaces. 2. When MEC interface Mx1 (OSS-CFS Portal) is located between trusted and untrusted security domains, e.g. public and internal domain, in addition to network level isolation (VPN/IPSEC), API protection which provides rate control, fine grained tenant-aware access control and web application firewalling capabilities should be deployed to mitigate various web-based attacks (OWASP API / REST security). 3. When exposing MEC interface Mx2 (Device App – User Application LCM Proxy), API security protection should be deployed between Mx2 and Device App. API protection should include, L7 DoS protection, fine grained tenant-aware access control and web application firewalling capabilities. 4. All MEC interfaces i.e. Mx, Mm, Mp should be protected using secure communication protocols with confidentiality, integrity and replay protection (e.g., at least TLS 1.2). 5. MEC Mp3 - MEC to Other MEC Platform interfaces may extend beyond a single operator's network, therefore Mp3 access should be strictly controlled and monitored. Mp3 should be isolated at the network level and only approved traffic based on access lists with strong authentication and authorisation should be allowed to ensure the Mp3 interface is not exploited to spread malicious applications across multiple MEC platforms or to allow adversaries to perform effective lateral movement as the Mp3 should be considered a critical control point. 6. All MEC platform API interfaces should require tenant-aware fine-grained authentication and authorisation (e.g.

Reference	Objective	Solution Description
		Oauth 2.0) to prevent non-repudiation and unauthorised access. 7. Platform interfaces MMx should be isolated at the network level. Access to MMx interfaces should be allowed only between MEC platform nodes (approved lists for network access) to minimise the attack surface.
EC-006	**Protecting MEC Platforms from physical attacks** (deployment in enterprise and/or area with limited access) to protect MECs that may be deployed in hostile environments with limited physical security and/or limited operator control.	1. When MEC is deployed in locations with limited access, reduced physical security risks and/or managed/controlled by untrusted 3rd parties, tamper resistance security controls should be built into the MEC platform solution. 2. When the MEC is deployed in locations where the physical security is managed/controlled by a 3rd party tamper resistant controls should securely log and report all access attempts. 3. When the MEC is deployed in locations with limited access, reduces physical security and/or is managed/controlled by untrusted 3rd parties, automatic secure deletion policies should be implemented as the MEC platform may store significant amounts of sensitive data including application code, images, configuration data and secrets in addition to user data. Encrypted data, both in live memory and storage, is vulnerable to various types of attacks, especially when the device is powered. As MEC workloads and data is ephemeral when physically compromised, secure deletion offers the best defensive measure against further damage.
EC-007	**MEC platform monitoring**, logging and accounting to provide detailed accounting of access and usage of resources and services for regulatory compliance and root-cause analysis.	1. MNOs should deploy monitoring at the network, host, virtualisation, MEC platform and MEC application layers. 2. Resource and activity monitoring should provide correlation between the various layers from physical up to the application layer. Correlation with external sources and other monitoring points increases detection quality. 3. All human or machine access to the MEC platform, underlying infrastructure (NFV, Physical), MEC APIs, MEC Platform and MEC Applications (Mx,

Reference	Objective	Solution Description
		MM, Mp) should be logged locally and sent remotely in near real-time over a secure channel which provides confidentiality, integrity and replay-protection. Logs should contain, at least, detailed information about the time, source, target resources, the type of action, success or failure, failure cause. 4. Logs should be tamper resistant e.g. append-only, integrity protected, encrypted at rest and access protected. 5. Tenant-Aware Monitoring alerts and Logs should be created containing only the information relevant for the specific tenant as customers may require monitoring logs to comply with regulations and standardisation requirements.

2.2.8.2 Network Exposure Functions

Reference	Objective	Solution Description
NEF-001	**NEF availability** is a key concern as NEF may be a single point of failure. When deploying a single NEF instance accessible by multiple AFs in different trust domains, operators increase the risk that one or more AFs may accidentally or deliberately perform denial of service attacks that could have an impact beyond the scope of the NEF into the domain of the 5GS or even the entire operator's network. In addition, some deployments may expose the NEF via publicly accessible networks (directly or indirectly) thereby exposing them to potential DDoS attacks. This objective targets the IP/transport layer.	1. Operators should deploy DoS and/or DDoS protection solutions in front of the NEF based on the type of access exposure the NEF would have. e.g. NEF deployed with direct or indirect public access should always be protected behind an IP/transport layer DDoS protection solution. NEFs deployed with access only to AFs in 3GPP trusted domains do not require such protection against malicious DDoS, but still may wish to deploy such protection for overload protection, misconfigurations or accidental DoS. It is expected that the NEF itself should implement some level of DoS protection for the AF-NEF exposed interfaces, at least at the network level. 2. NEF should be deployed in high availability mode, with at least 2 NEF instances. 3. NEF should implement and enforce SBI rate control to comply with NBI rate control (2). 4. NEF should implement and enforce NBI-SBI rate limit in order to prevent attackers from using different NBI commands which satisfy the NBI/SBI

		rates but violate the combined NBI/SBI rates.
NEF-002	**Protection of NEF confidentiality and integrity** properties, preventing unauthorised access.	1. TLS shall be used to provide integrity protection, replay protection and confidentiality protection for the interface between the NEF and the Application Function. The support of TLS is mandatory. TLS 1.2 or higher should be used according to 3GPP TLS profile in TS 33.210. 2. NEF and an AF which resides outside the 3GPP operator domain and/or AF with risk levels medium or higher, should use mutual authentication based on client and server certificates between the NEF and AF using at least TLS 1.2 (see TS 33.210). 3. Authorisation of AF requests by the NEF shall use OAuth-based authorisation mechanism, the specific authorisation mechanisms shall follow the provisions defined in RFC 6749. 4. NEF access should be restricted by network level ACLs (source IP, destination IP, Port, Protocol) either directly implemented by the NEF or via inline security controls e.g. FW. 5. When NEF is exposed to AFs outside the 3GPP trust domain, dedicated network layer security should be deployed between the external AF and NEF which implements confidentiality, integrity and replay protection. e.g. IPSEC VPN, SSL-VPN. 6. AF should only be allowed to access NEF/5GS resources based on an explicit approve list i.e. an AF by default isn't allowed to access any NEF resources. 7. Security controls which enable operators to selectively block and terminate in near real-time AF access to NEF should be deployed.
NEF-003	**Protecting NEF from data leakage** is essential to prevent NEF from exposing significant amounts of services and information to various AFs. When operators are unable to control exactly what data is exposed to which AF, it may result in AFs extracting maliciously or unintentionally information they are	1. NEF authorisation tokens should support fine grained access control, and these should be designed to strictly limit the ability of AFs to retrieve system and user data, e.g. tokens should allow retrieval of specific operator-controlled attributes of 3GPP users associated with this specific AF. However, the AF will not be allowed to retrieve other attributes e.g. user

	not authorised to access, e.g. user/system data, thereby resulting in a significant data breach.	location to ensure attackers cannot leverage the NEF to extract system or user information beyond that authorised by the operator or data controller. 2. Access should only be granted to resources covered by the service level agreement. 3. Restriction of access by services or AF to NEF and NEF to 5GS should be considered (5GS service partitioning). Each NEF should only have access to a subset of the 5G services/information within the 3GPP trust domain and the separation of duties between NEF deployments should be enabled to prevent unauthorised access by AFs to internal services and / or information and to reduce the impact of a single compromised NEF on the 5GS. Separation also helps identify individual NEF abnormal behaviour e.g. when a NEF attempts to access services it is not authorised to access. 4. Restricting AFs access to specific NEFs, operators should also consider adding binding of AF to NEF, further reducing the attack surface of AFs of NEF. When implementing (2), an AF may still be allowed to have e.g. network-level access to all NEFs even those it is not currently provisioned to access but a malicious AF could still attempt to attack and compromise these NEFs. Restrict AFs at the network layer to allow them to access only specific NEFs based on ACLs or other network isolation technologies to further reduce the attack surface.
NEF-004	**NEF non-repudiation and fraud prevention** - enterprises operating AF with access to a NEF may attempt to perform fraudulent or malicious activities, given the NEF's access to the 5GS and it being, in some cases, a shared resource e.g. AF can provision a set of UEs with high QoS but if the NEF doesn't maintain the binding between the AF request and the affected UEs, the enterprise can later reject the claim and suggest the action was the result	1. NEF shall ensure that all types of access by AFs via NEF APIs/services to the operator's 5GS can be uniquely identified and mapped to the originating AF and user/account. In addition, all 5GS services which resulted from this AF interaction e.g. SBI calls are logged in a manner which uniquely identifies that these calls/actions were the result of the actions of a specific AF on the NEF. This is essential as some enterprises could deny performing specific actions or retrieving/attempting to retrieve specific

	of a different AF operated by a 2nd enterprise. Without detailed mappings, the operator would be unable to prove which AF performed actions and which should incur charges.	information. Multiple AFs from different enterprises operating on the same NEF adds complexity and unmapped actions could result in fraud, violation of agreed SLAs, or denial of malicious activities.
NEF-005	**NEF auditing, accounting and monitoring**	1. NEF should maintain detailed access logs which associate each service call (API) with a specific AF and the resulting SBI and local information changes. 2. NEF should support logging either directly or indirectly e.g. via EMS log forwarding. 3. NEF should support alerts for unauthorised NBI and SBI access and resource attempts. 4. NEF should support alerts for unauthenticated NBI and SBI access attempts. 5. NEF should support isolation and separation of logs per AF and, where a single AF supports multiple tenants, NEF should also support generation and isolation of logs per AF and tenant.
NEF-006	**NEF API Protection** is essential as NEF APIs provide access to internal 5GS components as well as to information stored within the 5GS. These APIs may be exposed to AFs within the 3GPP trust domain or outside of this domain at various exposure levels. This reduces operator access, control and visibility of the AFs and increases the ability of malicious or compromised AFs to launch attacks against the NEF thereby directly impacting internal 5GS services. Existing 3GPP specifications don't preclude deployment of NEF with public access (internet), further increasing the exposure of NEF APIs to adversaries.	1. The NEF shall provide mechanisms to hide the topology of the PLMN trust domain from the API invokers accessing the service APIs from outside the PLMN trust domain. 2. The NEF shall provide mechanisms to hide the topology of the 3rd party API provider trust domain from the API invokers accessing the service APIs from outside the 3rd party API provider trust domain.(MEC) 3. The NEF shall provide an authorisation mechanism for service APIs from the 3rd party API providers. 4. The NEF shall support a common security mechanism for all API implementations to provide confidentiality and integrity protection. 5. Privacy of the 3GPP user over the NEF northbound interfaces shall be protected. 6. NEF APIs exposing critical infrastructure services should be verified against OWASP latest ASVS release level 3 testing standards, as far as applicable to the API. Other NEF functions should be at least verified according to applicable

		OWASP latest ASVS release level 2 testing standards. 7. When the NEF is exposed allowing extended external access e.g. public access, the NEF should implement web application firewalling capabilities (WAF) or, alternatively, inline security control functions with WAF capabilities in front of the NEF. 8. NEF northbound access (APIs, services, webservers, etc.) should be regularly security/penetration tested in a deployment setup i.e. the same setup as that of the production network, every 3 months for vulnerabilities and misconfigurations as the NEF is continuously exposed to AFs and, in some deployment, scenarios may be directly accessible beyond the operator's 3GPP trust border e.g. via public access. This increases the likelihood that adversaries will continuously attempt to identify and exploit vulnerabilities and/or misconfigurations in the NEF which may result in a significant security incident given the level of access NEF to the 5GS. 9. NEF should be evaluated based on the NESAS program using relevant SCAS test cases.
NEF-007	**NEF information exposure protection** is essential to prevent access and/or leakage of core network information via NEF.	1. Internal 5G Core information such as the DNN, S-NSSAI etc., shall not be sent outside the 3GPP operator domain. 2. SUPI shall not be sent outside the 3GPP operator domain by the NEF.
NEF-008	**NEF availability** is a consideration as NEF may be a single point of failure. When deploying a single NEF instance accessible by multiple AFs in different trust domains, operators increase the risk that one or more nodes may accidentally or deliberately perform denial of service attacks on the API provided by the NEF. The impact may extend beyond the scope of the NEF into the domain of the 5GS or even the entire operator's network. In addition, some deployments may expose the NEF via publicly accessible networks (directly or indirectly) thereby	1. NEF should implement and enforce NBI API rate control, i.e. allow to define the maximum number of API calls per a specific API per AF and overall. 2. NEF should implement QoS and fairness for NEF NBIs to prevent resource exhaustion attacks. 3. When the NEF supports CAPIF for external exposure, then the CAPIF core function shall choose the appropriate CAPIF-2e security method, as defined in the sub-clause 6.5.2 in 3GPP TS 33.122, for mutual authentication and protection of the NEF – AF interface.

	exposing them to potential DDoS attacks.	4. The NEF should prevent information leakage on information element level. 5. AF should only be allowed to access NEF/5GS service resources based on an explicit approve list i.e. an AF by default is not allowed to access any NEF resources. 6. Security controls which enable operators to monitor, selectively block and terminate in near real-time AF access to NEF should be deployed.

2.2.9 Network Operations Controls

These controls are likely to be understood and managed by the network operations team.

Reference	Objective	Solution Description
NO-001 / CIS-001	Actively **manage (inventory, track, and correct) all hardware devices on the network** so that only authorised devices are given access, and unauthorised and unmanaged devices are found and prevented from gaining access.	1. Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. 2. Ensure the asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. 3. Use client certificates to authenticate assets connecting to the organisation's trusted network. 4. Utilise port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network. 5. Do not allow shared, default or hardcoded passwords
NO-002 / CIS-005 & 011	Establish, implement, and actively **manage (track, report on, correct) the security configuration of network equipment (NE), servers, and workstations, and core infrastructure** using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	1. Harden NE, and network infrastructure according to local hardening policies, if unavailable to the device manufacturer's hardening guides and/or industry accepted hardening guides [37], maintain images of these builds. 2. Confirm interfaces are only accessible to the correct external applications and/or networks, internal network

Reference	Objective	Solution Description
		elements and BSS e.g. GTP's Gp/S8 interface accessible only for roaming partners [37] 3. Close interfaces that are not required (e.g. debugging interfaces) 4. Deploy mechanisms for detecting and reporting differences between master configuration and that of network infrastructure 5. Limit ability for change to occur using account management (e.g. by use of Privileged account management (PAM) system)
NO-003	**Virtualisation/Containerisation controls should be enforced** wherever network elements are virtualised e.g. Network Function Virtualisation (NFV).	1. Use Security Orchestration technology within operation centres to control management of virtualisation 2. Harden virtualised machines or containers (NO-002) as per industry recommendations [46] 3. Isolate services, processes and tenants via name-spacing and hypervisor controls 4. NFV Infrastructure patching should deployed as a priority, the impact of a successful attacker gaining code execution rights is high.
NO-004 / CIS-009	Manage (track/control/correct) the ongoing **operational use of ports, protocols, and services** on networked devices in order to **minimise windows of vulnerability** available to attackers	1. Associate active ports, services, and protocols to the hardware assets in the asset inventory. 2. Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system. 3. Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system. 4. Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. 5. Depreciate and remove usage of: a. Insecure or deprecated cipher suites b. Unencrypted, insecure transmission protocols [47]

Reference	Objective	Solution Description
		c. Unencrypted and insecure protocols Examples include, but are not limited to: FTP, TFTP, telnet, POP3, IMAP, BGP and SNMP v1/v2. 6. NIST/3GPP recommended cryptographic algorithms shall be used whenever cryptographic services are required [48]
NO-005 / CIS-004	The processes and tools used to **track/control/prevent/correct the use, assignment, and configuration of administrative privileges** on servers, networks, and applications.	1. Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts. 2. Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. 3. Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities. 4. Limit access to scripting tools to only administrative or development users with the need to access those capabilities. 5. Use multi-factor authentication and encrypted channels for all administrative account access. For accounts that cannot use multi-factor authentication and allow privilege access, operators should consider setting: a. credential/key rotation policies b. credential/key strength requirements 6. Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges. 7. Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.
NO-006 / CIS-003	Continuously acquire, assess, and act on new information in order to **identify vulnerabilities, remediate, and**	1. Enable a centralised vulnerability and patch management programme to

Reference	Objective	Solution Description
	minimize the window of opportunity for attackers.	remediate vulnerabilities in a prioritised, timely manner 2. Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. 3. Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities. 4. Include software, open source and proprietary, in vulnerability assessment programmes. 5. Provenance of software updates should be assured. 6. Patches should be delivered over a secure channel. 7. Patches/Software updates should be integrity protected.
NO-007	**Monitor and analyse core, radio and enterprise network traffic** for potential internal or external attacks.	1. Enable audit logging and deliver data to SIEM/log server for analysis for relevant threat vectors 2. Correlate log data to allow cross referencing 3. Enable system logging to include useful key elements, such as an event source, date, user, timestamp (UTC), source addresses, destination addresses, object, action, old value, new value, etc. 4. On a regular basis, tune SIEM system to better identify actionable events and decrease event noise. 5. Ensure integrity of audit data (e.g. copy to write-once media or apply digital signatures to log collections)
NO-008	**Ensure certificate issuing authorities are managed correctly** to avoid the risk of bogus certificates being provided with access to network services.	1. Ensure root certificate issuing machines do not have access to and from the internet 2. Follow IETF RFC pertaining to PKI CA handling [49], [50], [51]
NO-009	**Ensure cryptographic key material is protected correctly** using a Cryptographic key management system (CKMS).	1. Actively manage the storage location, crypto-period and usage of all cryptographic material on the network [52] 2. Ensure HSM key management follows industry best practice, as outlined in FS.28 [19].

Reference	Objective	Solution Description
		3. Whenever possible key material should be managed via a HSM
NO-010	Ensure **database services and systems are protected** from unauthorised access and misuse.	1. Monitor database systems for unauthorised access, changes and data leakage 2. Monitor for unauthorised changes from privileged users such as administrators 3. Use transparent data encryption (TDE) to ensure data is encrypted all the way to the client, securing data both when it is at rest and in transit.
NO-011	Implement **cloud security principles** for all private, public and hybrid cloud (infrastructure, platform or software) computing based provisioning, whether operated in-house or outsourced, to provide all tenants with an effective risk management of services.	1. Data assessment before multi-tenant etc. 2. Deployment management 3. In life management 4. Procurement management 5. Isolation controls 6. Secure communications with infrastructure/service 7. Supplier security 8. User management 9. Cover in-life threat modelling as part of the ongoing risk management process 10. MNOs should evaluate their cloud deployments against CSA CCM matrix and ensure adequate and applicable cloud security controls have been properly deployed.
NO-012	**Monitor and analyse roaming network traffic** for potential internal attacks.	1. Monitor and analyse outgoing traffic for potential detection of misuse and compromise of core network. 2. Enable audit logging and deliver data to Security Incident and Event Management (SIEM) for analysis for relevant threat vectors. Ensure integrity of audit data e.g. by the use of digital signatures
NO-013	**Continuous real-time Roaming visibility to detect and stop cybersecurity threats**, attacks and vulnerability exploitation	1. Real-time monitoring of signalling traffic for potential attacks, malware, and other malicious activities. 2. Engine to detect and stop malicious traffic in compliance with local legislation.

Reference	Objective	Solution Description
NO-014	**Ensure UE and IoT traffic security** e.g. to avoid overload or malware propagation	1. Traffic monitoring e.g. according to GSMA CLP.14 [26]
NO-015	**Monitor and analyse roaming and national network traffic** for potential internal attacks.	1. Monitor and analyse outgoing traffic for potential detection of misuse and compromise of core network. 2. Enable audit logging and deliver data to Security Incident and Event Management (SIEM) for analysis for relevant threat vectors. 3. Ensure integrity of audit data e.g. by the use of digital signatures.
NO-016	MNOs should utilise centralised patching software, orchestrate and control patch deployments, and define **patch deployment** policies	1. Patching processes set the frequency and scope 2. Controlling or restricting automatic software updates. 3. Testing of patches in lab environment and ensuring that devices are updated in controlled settings before deployment.
NO-017	**Misconfiguration detection and prevention**	1. Equipment vendors should provide best practices and guidance on secure deployment and secure configuration of their products. 2. MNOs should define feasible configuration policies based on the vendors and industry best practices as well as regulatory requirements e.g. allow only use of secure communication protocols and strong cipher suites. 3. Equipment vendors and/or 3rd party security vendors should develop tools to either automate the process of misconfiguration detection and prevention or allow MNOs and 3rd party vendors to develop such tools themselves. 4. MNOs should favour the use of **automatic** tools provided by vendors and / or 3rd parties to monitor, alert and when possible, block configurations which may result in a violation of set policies (2).

2.2.10 Orchestration and VNF Security Controls

These controls are likely to be understood and managed by the Service Provisioning / Network Operations teams.

In this section the controls can be partitioned into two parts:

- Those relating to VNF LCM (Life Cycle Management);
- Those relating to the overall Orchestration.

2.2.10.1 VNF LCM Security Controls

Reference	Objective	Solution Description
VNF-LCM-001	**Protect VNF Packet Management**, ensuring no image file or template is illegally accessed, tampered, or deleted.	1. Implement a credible integrity check before upload, on-board or storage of templates or image files.
VNF-LCM-002	**Protect the VNF Instantiation process** to ensure that no illegal VNF can be instantiated through an illegal template.	1. Perform an integrity check before doing the VNF instantiation.
VNF-LCM-003	**Protect the VNF management processes** to prevent illegal acquisition of network information such as VNF status.	1. Implement a fully authenticated and role-based access control strategy.
NFVI-LCM-004	**Protect VNF scaling management** to prevent tampering thresholds of scaling, and resource exhaustion.	1. Implement a correct authentication and authorisation-based access control and perform tenant-based quota controls

2.2.10.2 Orchestrator Security Controls

Reference	Objective	Solution Description
NFV-OR-001	**Protect against unauthorised operations**, by ensuring that the source of the command is secure before processing an orchestration event.	1. Implement measures to ensure that the receiving party shall not perform any actions from received command/information before successfully identifying and verifying the source of the command/information.
NFV-OR-002	**Prevent modifications of orchestration communications** to protect against “Man in the Middle” attacks in the communication path.	1. Enable integrity protection measures such that a transmitter / receiver communication is protected from modification, deletion, insertion or replay.
NFV-OR-003	**Prevent disclosure of data to unauthorised entities** by securing the orchestration communication.	1. The data transfer between any orchestration and any orchestrated elements shall be encrypted.
NFV-OR-004	**Prevent resource hijacking** by utilisation monitoring and logging.	1. Regular full system audits have to be enabled to ensure no frozen or hijacked resources are running in the system. All events, alarms, logs and statistics shall be verified and cross-referenced with the expected level of utilisation.

2.2.11 Security Operations Controls

These controls are likely to be understood and managed by the Security Operations Centre (SOC), Computer Security and Incident Response Team (CSIRT) or ethical hacking teams.

Reference	Objective	Solution Description
SO-001 / CIS-006	**Collect, manage, and analyse audit logs** of events that could help detect, understand, or recover from an attack.	1. Collect, manage, correlate and analyse the audit logs of events that could help detect, understand or recover from an attack [3] 2. Collect, manage, correlate and analyse network traffic flows that could help detect, understand or recover from an attack
SO-002 / CIS-008	**Control the installation, spread, and execution of malicious code** at multiple points in the network, while optimizing the use of automation to enable rapid updating of defence, data gathering, and corrective action.	1. Collect and manage events triggered by enterprise, mobile network and end point device anti-virus protection [3]
SO-003	**Utilise open-source information** (OSINT) and other contextual information to increase awareness of the threat landscape.	1. Carry out Threat Intelligence integration 2. Contribute to relevant sharing communities e.g. GSMA T-ISAC [53]
SO-004 / CIS-019	Protect the organisation's information, as well as its reputation, by **developing and implementing an incident response infrastructure** (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and Systems.	1. Create and advertise an incident reporting function (external and internal), allowing suspected incidents to be reported to the appropriate team 2. Plan, prepare and practice incident response activities (including data recovery and forensic capabilities) [54] 3. Assign roles to specific teams and individuals to drive ownership and accountability during an incident 4. Develop capability to learn and improve based on historic incidents through post incident reviews (PIR) 5. Create processes for any breach notifications required, noting any deadlines included
SO-005 / CIS-020	**Perform security assessment of live systems** to test the overall strength of an organization's defence (the technology, the processes, and the people) by **simulating the objectives and actions of an attacker**.	1. Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. 2. Remediate issues located through security assessments 3. Undertake regular security assessments, e.g. pen testing, of live systems
SO-006	Implement a holistic **protective monitoring** approach that ensures there	1. Design an approach to protective monitoring that draws together the

Reference	Objective	Solution Description
	is a proactive and consistent approach to detection of abnormal behaviour on networks and systems	available sources of security events and alert when these sources fail to deliver data. 2. Appropriately tune available log sources, SIEM and behavioural analysis systems to detect abnormal behaviour. 3. Centralise reporting to consoles that are adequately manned. 4. Be able to provide forensically sound transaction audit trails. 5. Be able to trace actions (especially privileged actions) to individuals and devices. 6. Integrate into the system monitoring, audit and fraud management processes. 7. Produce regular management and performance reports. 8. Undertake regular reviews to adjust and improve practice. 9. Continuously improve processes through root cause analysis from past security incidents.

2.2.12 Roaming and Interconnect Controls

These controls are likely to be understood and managed by the roaming and interconnect team.

Reference	Objective	Solution Description
RI-001	**Protection of the roaming and interconnect messaging and customers** from attacks including location tracking, eavesdropping, denial of service and fraud over interconnect signalling protocols and links.	1. Confirm interfaces are only accessible to the correct external applications and/or networks, internal network elements and business support services (BSS) 2. Deploy Diameter proxies for each Diameter application supported by the public mobile network (PMN), through an Internetwork Packet Exchange (IPX) Diameter agent [33], [34] 3. Deploy message monitoring and filtering capabilities according to FS.21 and FS.36 [58] to identify and block malformed, prohibited and unauthorised messages i.e. SS7 for 2/3G [35], [36] Diameter for LTE and prepare for 5G SEPP deployment [57]. 4. Enable IR.77 binding security requirements for IPX Provider Networks [37] 5. Remediate inappropriate interconnect access by third parties e.g. Global Title (GT) leasing 6. Signalling message traffic filters should be implemented, only accepting incoming traffic from known peer Operators of Hubs where a roaming or interworking agreement exists [34] 7. Legacy interworking scenarios need also to be secured according to usage and protocol FS.36 [58]. 8. Deploy monitoring on incoming and outgoing traffic 9. Deploy monitoring on both international and national links.
RI-002	**Protect the roaming and interconnect network elements (NE)** from unauthorised access.	1. Assign disjoint IP address segments for each of the networks [37] 2. Disable the ability to access roaming and interconnect NE from the internet or UE IP addresses [37] 3. Keep networks separated physically by separate connections, or logically separate on layer 2 (e.g. through the use of a VPN or VLAN) [37]

Reference	Objective	Solution Description
		4. Keep networks separated in shared equipment, such as routers or switches, by having independent virtual routing and forwarding instances or VLANs [37] 5. Do not allow shared, default or hardcoded passwords
RI-003	Maintain an **accurate record of roaming information**.	1. Maintain data recorded in the Roaming Exchange (RAEX) using IR.21 [38] /IR.85 [39]

Annex A Policy Outlines

A.1 Policy Document Outline Table

Policy	Outline Description
3rd party data/supply chain security management	3rd party data and supply chain security management will control the information exchanges and remote access for 3rd party to information systems, as well as the correct operation of policy and controls to ensure that vulnerabilities are not introduced within the supply chain.
Access control	Access control policy will cover the process for internal and external access to information systems and data. This includes enrolment and movers/leavers policies, data access controls, network access controls and privilege management.
Asset management	Asset management policies; including architectural design, in life management, and decommissioning of assets, especially those that contain information and data. This ensures that the systems that process those assets can effectively protect those assets and that the data loss is prevented (e.g. following disposal).
Business continuity management	Business continuity management policies and plans are developed based on specialist impact assessments that ensure that critical business processes can be maintained regardless of eventualities (disasters, losses of key personnel and other business disruptions, e.g. industrial action).
Cloud security	Cloud security policies ensure that appropriate security controls are applied to public, private or hybrid cloud computing deployments, with particular regard for protection of assets when they are processed within a multi-tenanted environment within which the tenants are largely dependent upon the security environment delivered by the cloud services provider.
Cryptographic material management	Cryptographic material management policy ensures that there is effective and sustainable management of encryption technology within solutions. This includes proactive key management to ensure that information and data can be encrypted/decrypted as and when required (and only by the legitimate communicating parties) and also that cryptographic techniques that support integrity and trust frameworks (PKIs) operate effectively and can be relied upon.
Device, system and network asset security	Device, system and network asset security policies ensure that appropriate configurations are applied to computing and networking devices to a) help enforce access control policies and b) minimise the exposure of vulnerabilities (e.g. disablement of unused functions/application of build lockdowns).

Policy	Outline Description
Information classification and handling	The information classification and handling policy will define the approach to security classification of information in both paper and electronic forms. It is typical for a hierarchy of security classifications to be identified and for appropriate handling requirements to be defined for each classification.
Personnel security	Personnel security policies cover pre- and during employment checks and also include conditions within both contracts of employment and arrangements with agencies and other contractors. It also covers sanctions for security breaches within disciplinary or contractual processes and procedures as well as management of security clearances for working with 3rd parties (e.g. government agencies).
Physical security	It can be expected there will be applied several physical security policies and standards across the estates of Operator organisations, with appropriate and proportionate standards applied to different sites (data centres, telecommunications centres, offices, cell-sites, etc.).
Risk management	A risk management policy should embody the approach to management of risks to information risks (the confidentiality, integrity and availability of that information). This includes consideration of threats and vulnerabilities present within both physical and electronic environments. This should be integrated with the business approach to risk in order that the SLT has visibility of critical information security risks.
Security incident management	Security incident management policy and processes handles the complete lifecycle of security related incidents (including breaches), should work as a feedback loop to reduce the risk of reoccurrence and should cover all aspects: reporting (actual or suspicious behaviour, weaknesses, etc.), triage, investigation, computer forensics, breach notification (in accordance with local regulations), communication with stakeholders, collaboration with law enforcement, recovery, management reporting/escalation, critical incident management teams and post-incident reviews.
Security monitoring	Security monitoring policy and processes are used to establish the necessary skills, disciplines and framework for monitoring systems for abnormal behaviour indicative of potential cyber-attacks or security breaches. This also includes audit policies for those systems that are not monitored by electronic systems and also log management and analysis.
Software security update management	Software security update management policy defines the required parameters for application of security updates and other patches to software and firmware in

Policy	Outline Description
	equipment. It also considers the solution product lifecycles to ensure that systems are supported with security updates and that end-of-support components are replaced prior to obsolescence.
Staff training and awareness	Staff training and awareness policy covers both specialist training of security and front-line staff and also broader awareness of security matters to all staff and contractors (including induction sessions, regular refresher/update briefings/communications, posters, etc.). It also covers urgent dissemination of security notices following security breaches.
Vulnerability disclosure management	Vulnerability disclosure management policy covers the responsible reporting of vulnerabilities discovered in systems, services and solutions. This prevents details of those vulnerabilities falling into the hands of attackers who would be interested in exploiting them and times releasing of public information in order that it is in conjunction with the availability of remedies.

Annex B Network Function Virtualisation Infrastructure (NFVI) Background

B.1 Infrastructure

B.1.1 Containers

NIST SP 800-190 Application Container Security Guide [76] describes the risks and the countermeasures required to protect a system using container technology.

Figure 1**Error! Reference source not found.** presents the major components of a container-based platform which are;

- **Container Images** – a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.
- **Container Registry** – a repository of container images which may be external (public) and/or internal (private).
- **Container Orchestrator** – manages the lifecycles of containers, resource provisioning, networking services, load balancing and scaling, management and decommissioning.
- **Container Runtime / Hosts** – local process / deamons / applications that manage, deploy, configure and execute containers on a specific host**.**
- **Containers –** workloads / applications executed using lightweight virtualisation over the host machines OS (shared kernel space). Containers behave like a virtual machine however, unlike a VM, they don't create a whole virtual operating system. (See)

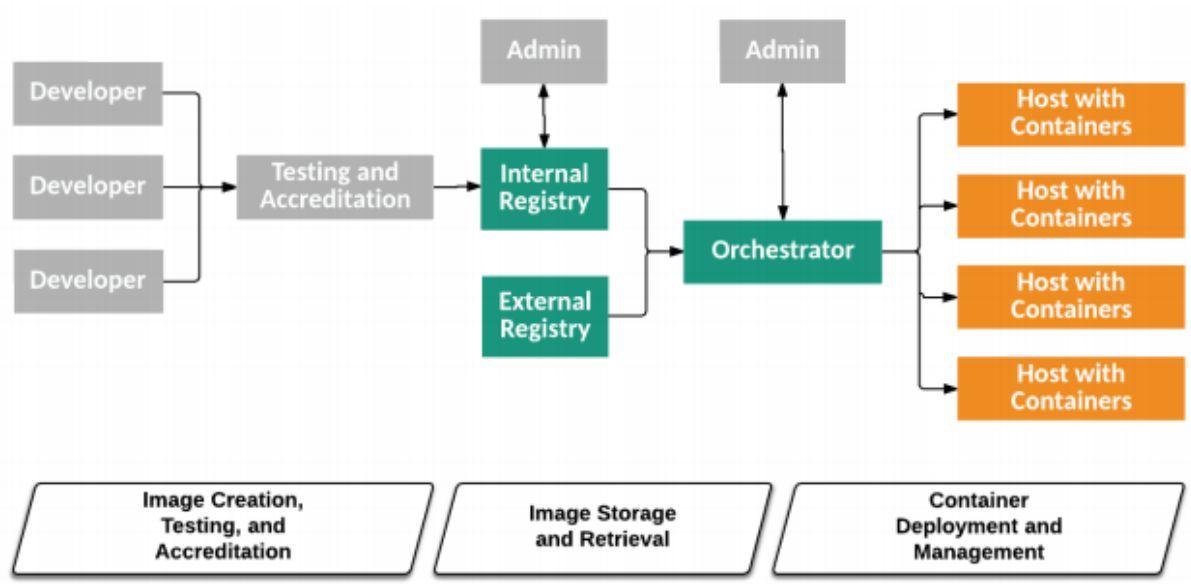


Figure 2: NIST SP.800-190 Container Technology Architecture Tiers, Components, and Lifecycle Phases

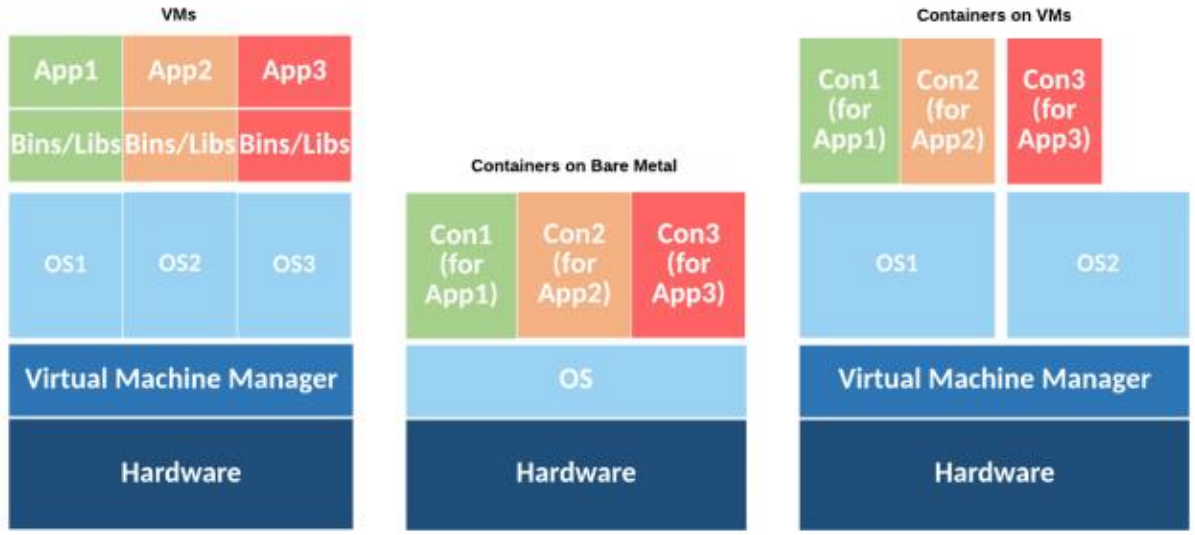


Figure 3: NIST SP.800-190 Virtual Machine and Container Deployments

Figure 3 and Figure 4 demonstrate two popular container technology platforms, which are widely used in ICT environments. *These figures provide further validation for NIST SP 800-160 components breakdown.*

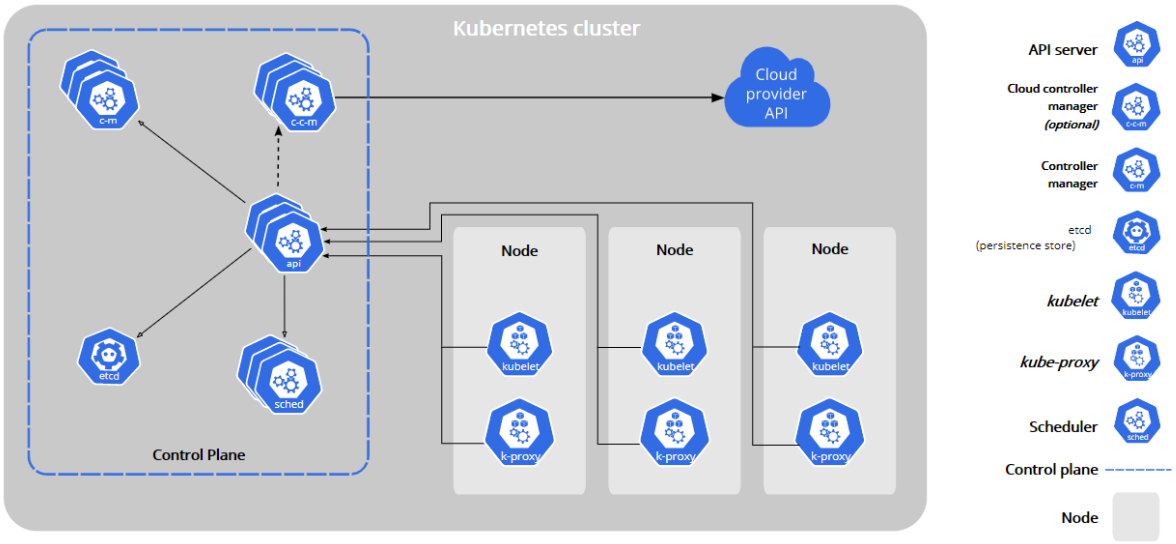


Figure 4: Kubernetes Components, src: kubernetes.io/docs/concepts/overview/components

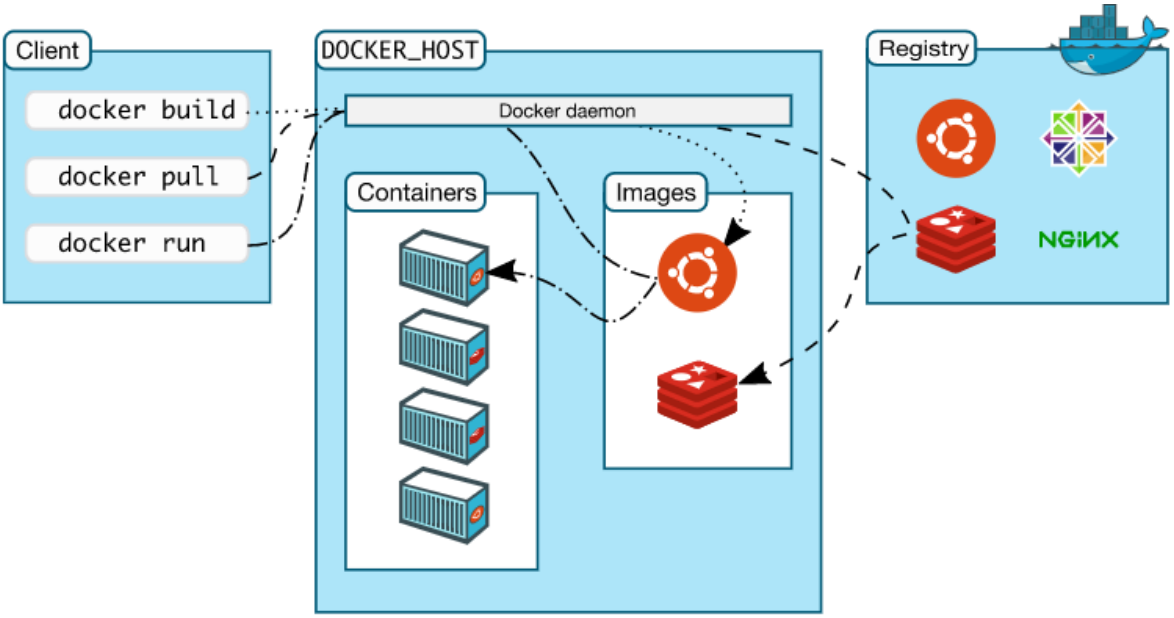


Figure 5: Docker architecture, src:docs.docker.com/get-started/overview/#docker-architecture

B.1.2 Network Exposure Function

3GPP TS 23.501 5.2 defines The Network Exposure Function (NEF) function as one that "… *supports external exposure of capabilities of network functions. External exposure can be categorized as Monitoring capability, Provisioning capability, Policy/Charging capability and Analytics reporting capability…*"

Figure 5 describes a multi-NEF deployment with two different types of Application Function (AF) deployments. The 1st are AFs deployed outside of the operator's network trust domain and the 2nd deployment type is where an AF is deployed within the operator's trust domain. When evaluating if AF is located in trusted or untrusted security domains, operators should perform a comprehensive risk assessment of each specific AF, which evaluates, at the very least, the physical and virtual deployment location, the level of control and visibility the operator maintains throughout the AF lifecycle, the ability of the operator to identify and mitigate in near real-time, in a selective manner, unauthorised and/or malicious activities performed by the AF given the level of exposure the AF has via the NEF to the operator's network i.e. the potential impact a specific compromised AF can cause the operator's network.

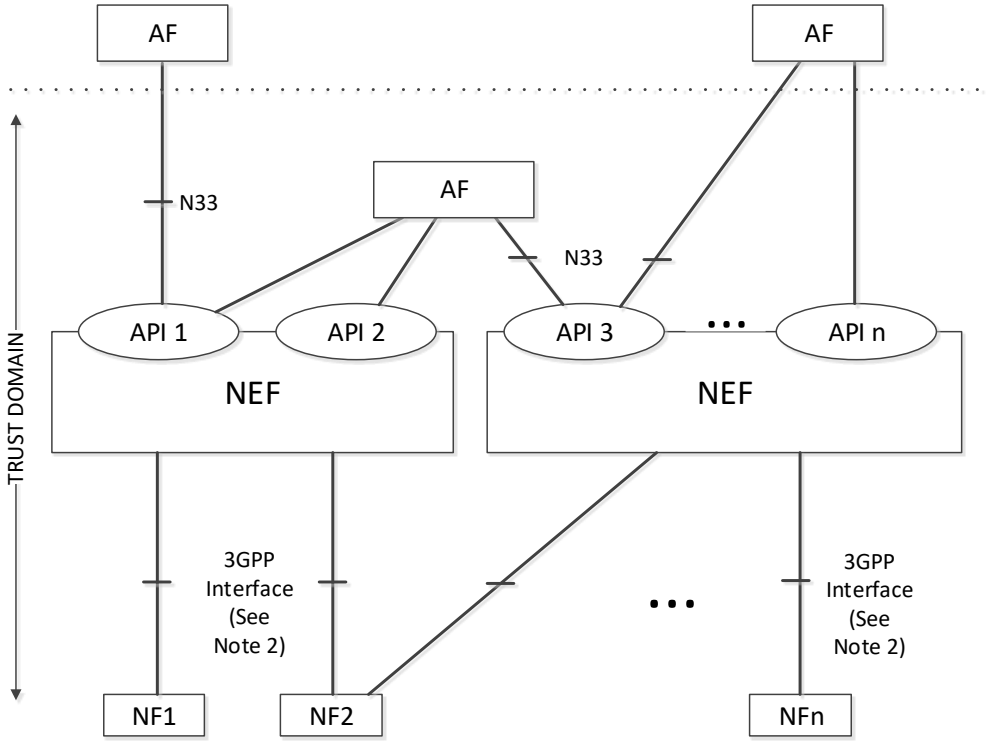


Figure 6: Non-roaming architecture for Network Exposure Function in reference point representation, src: 3GPP TS 23.501.

NOTE 1: In The figure above, The NEF Trust domain is the same as the Trust domain for SCEF as defined in 3GPP TS 23.682. 3GPP Interface represents southbound interfaces between NEF and 5GC Network Functions e.g. N29 interface between NEF and SMF, etc.

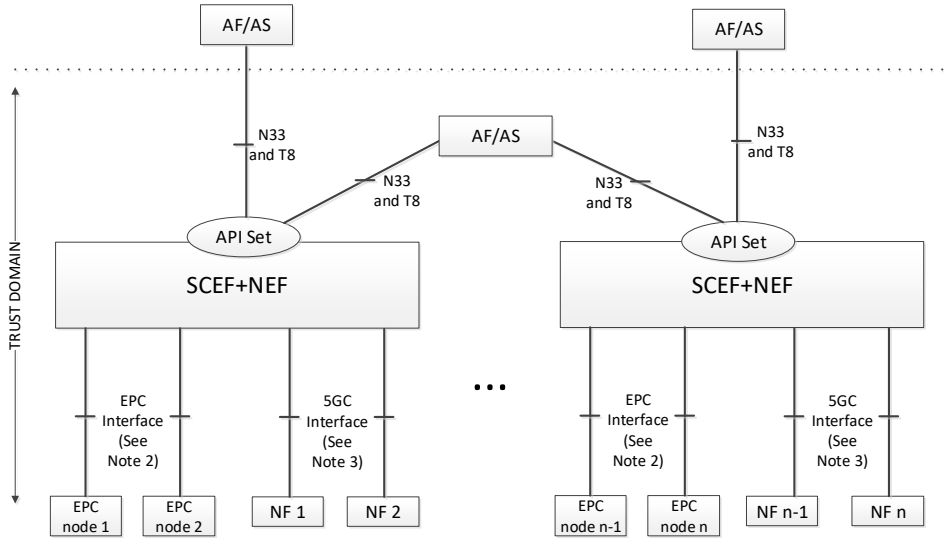


Figure 7: Non-roaming Service Exposure Architecture for EPC-5GC Interworking, src: 3GPP TS 23.501

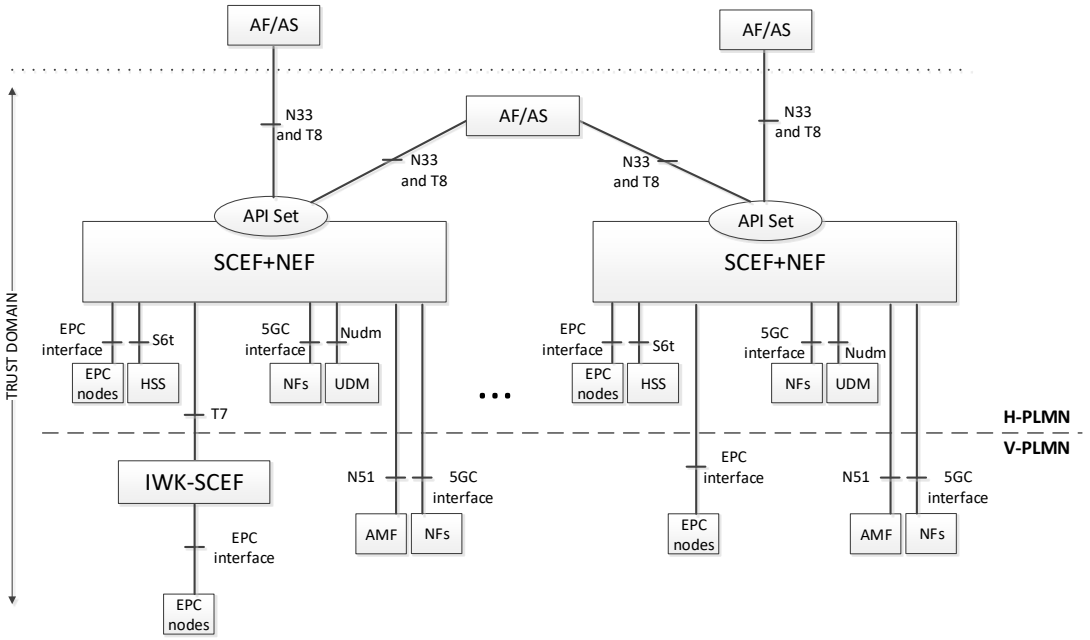


Figure 8: Roaming Service Exposure Architecture for EPC-5GC Interworking, src: 3GPP TS 23.501

B.1.3 Virtual Switch

Virtual switches are located at the core of network virtualisation and they manage layer 2 traffic with the virtual platform and carry layer 2 traffic across the VMs as well as handle layer 2 physical/virtual network traffic. Some vendors offer virtual switches which extend beyond the scope of a single host and offer centralised management of the networking configuration of all hosts associated with that switch.

In all cases, misconfiguration of security policies on the vSwitch can result in an increased attack vector and increased risk to the virtualisation platform. Attackers may attempt to directly attack the vSwitch in order to bypass network and / or host-based security controls e.g. to capture network traffic which may be directed to specific monitor VMs (e.g. Port mirroring) or undermine network isolation by circumventing VLAN security e.g. using VLAN hopping, STP poisoning, etc.

Attackers may also attempt to simply impact the performance of other VMs or to reduce the overall availability of services by performing DoS attacks against the vSwitch or simply utilise lack of rate control over the vSwitch to consume all available bandwidth.

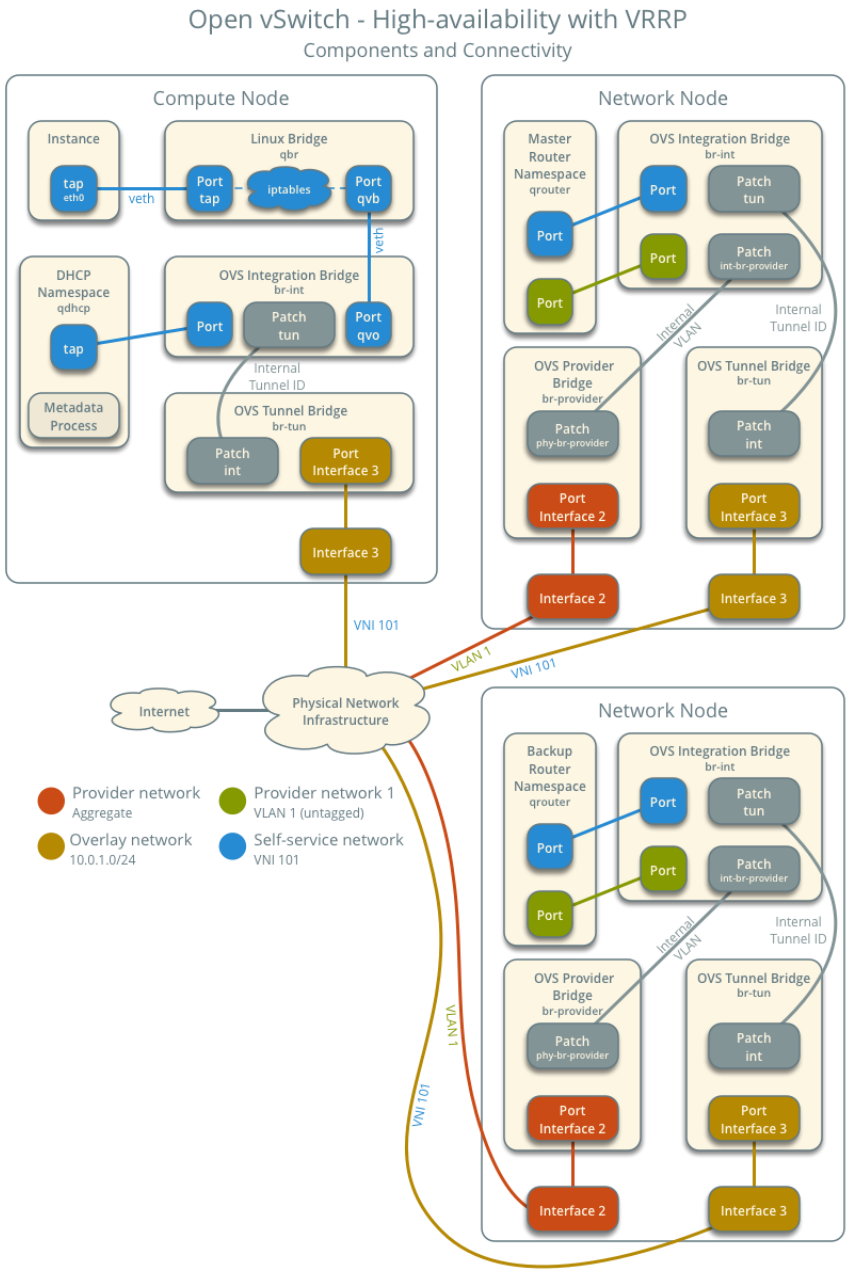


Figure 9: Open vSwitch: High availability using VRRP src: OpenStack Neutron's documentation

Figure 8 depicts a possible OpenStack high availability deployment of an Open vSwitch with VRRP, which increases the availability and resiliency of the virtualisation platform.

B.2 Services

B.2.1 Mobile Edge Computing (MEC)

MEC supports various deployment options dependent on the MEC vendor as well as the MNO deployment strategy. The ETSI MEC ISG architectural framework enables MEC deployments over virtualised hosts as well as over NFV as can be seen in Figure 9, Figure 10 and Figure 11 below. These different technology deployment stacks may introduce additional cross-layer risks.

MEC platforms may also be operated by 3rd party service providers (e.g., suppliers, cloud service providers), further reducing MNO control.

In addition to the technology deployment aspects of MEC, the physical deployment aspects provide an additional attack surface. MECs may be deployed in an enterprise environment either partly or fully controlled by the enterprise. MECs may also be deployed in remote locations or locations with limited physical security controls compared to those offered in MNO Data Centres or Central Offices.

MNOs should include in their risk-based analysis a detailed account of their specific MEC deployments and operational models and identify which security controls are suitable for their respective businesses.

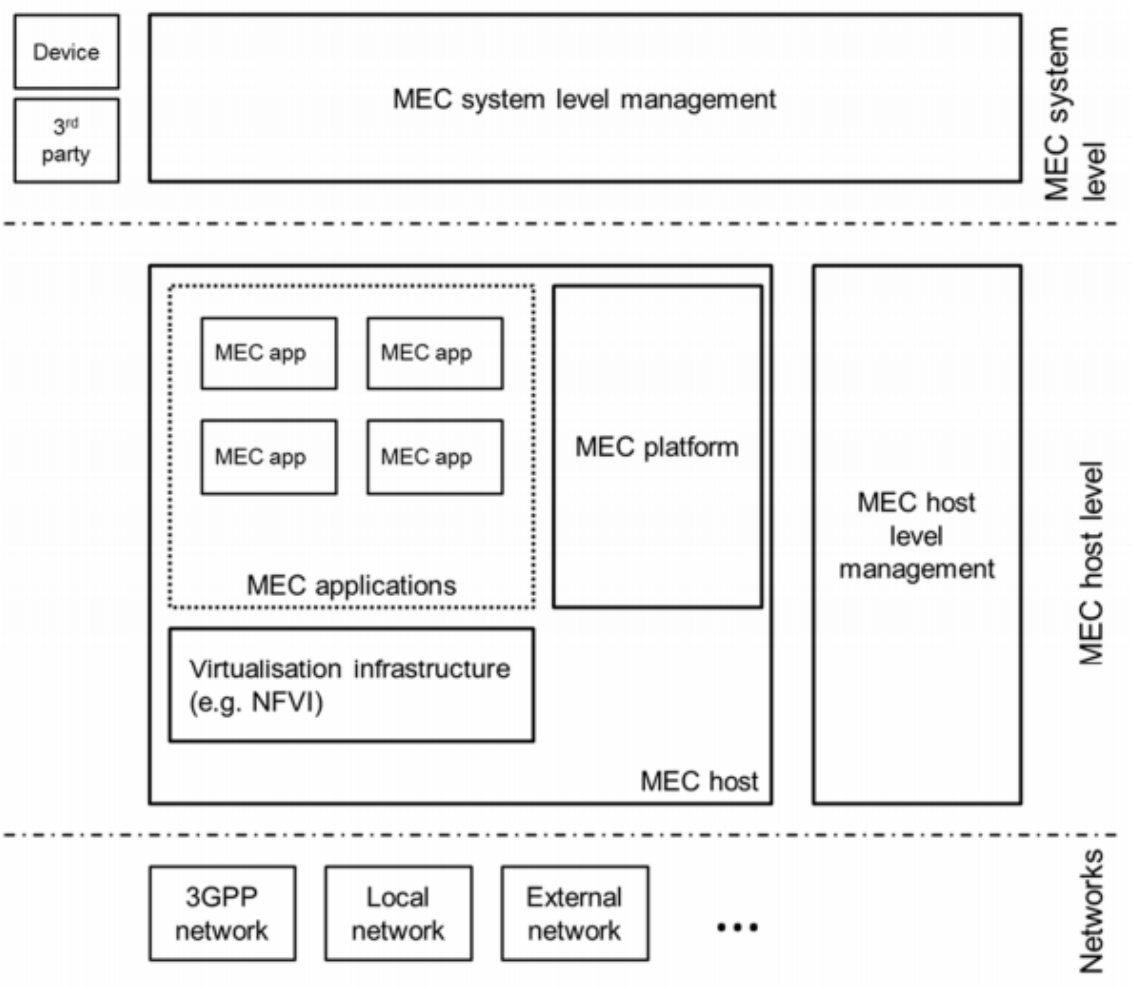


Figure 10: ETSI GS MEC 009 V2.1.1 (2019-01), Multi-access Edge Computing framework

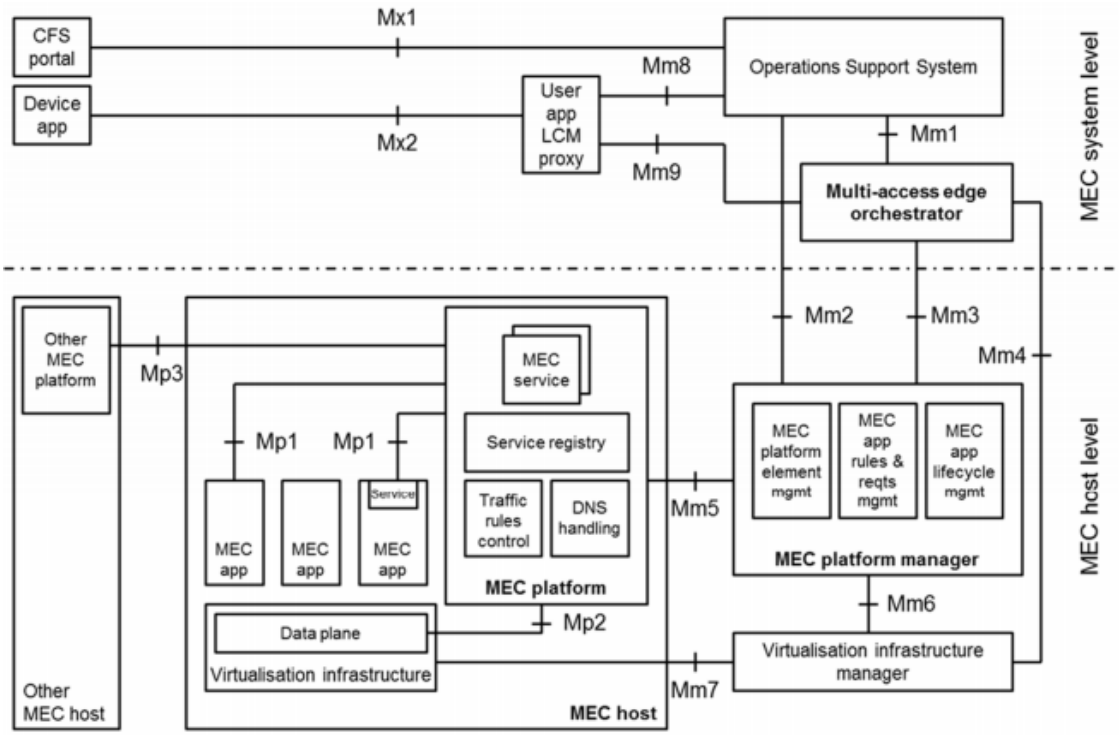
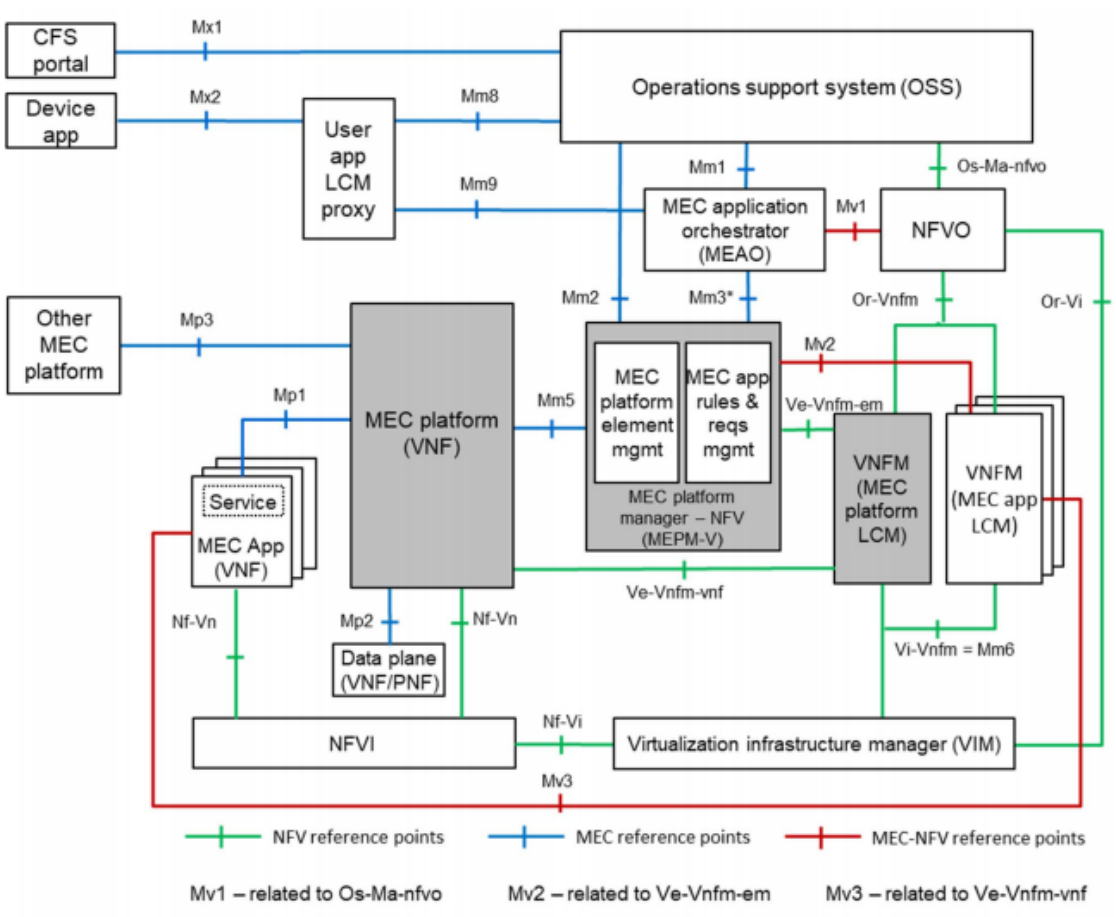


Figure 11: ETSI GS MEC 009 V2.1.1 (2019-01), Multi-access edge system reference architecture



Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	23 February 2019	Baseline security control for Mobile Network Operators.	TG	Amy Lemberger, GSMA
2.0	05 Feb 2020	Major review of controls in all sections	FASG	Amy Lemberger, GSMA
3.0	Sep 2023	Comprehensive review and update of security controls with significant additions pertaining to edge computing, network function virtualisation, network slicing and network orchestration. In total, 85 new controls have been added and guidance has been enhanced for 29 solutions. The Security Controls Checklist has been removed and will be maintained as a separate document.	FASG	James Moran, GSMA

C.2 Other Information

Type	Description
Document Owner	James Moran
Editor / Company	GSMA

It is our intention to provide a quality product for your use. This document is an early version that can be updated with subject experiences and suggested improvements or additions, or if you find any errors or omissions. You may send these via email to us at security@gsma.com