MCMC MTSFB TC G028:2021

TECHNICAL CODE

IMT-2020 (FIFTH GENERATION) - SECURITY REQUIREMENTS

Developed by

Registered by

Registered date : 24 August 2021

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd (MTSFB) as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Application Security Sub Working Group which supervised by Security, Trust and Privacy Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB) consists of representatives from the following organisations:

Celcom Axiata Berhad

CyberSecurity Malaysia

Digi Telecommunications Sdn Bhd

KPMG Management & Risk Consulting Sdn Bhd

Maxis Broadband Sdn Bhd

National Cyber Security Agency

Telekom Malaysia Berhad

Foreword

This technical code for IMT-2020 (Fifth Generation) - Security Requirements (‘this Technical Code’) was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Security, Trust and Privacy Working Group.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

IMT-2020 (FIFTH GENERATION) - SECURITY REQUIREMENTS

0. Introduction

Mobile communications provide a means for people to communicate with one another over long distance. Throughout the years, ever since it was introduced, mobile technology has been constantly evolving, from the First Generation (1G) analogue based technology, to the up and coming Fifth Generation (5G) technology or commonly known as International Mobile Telecommunications-2020 (IMT-2020). 5G technology is capable to support even higher speed than the other previous telecommunication technologies, in addition to capable of supporting low latency services and services that may have many devices connected to the network.

With 5G capability to support a wide range of services, it is crucial for the 5G network and devices to be secured from external attacks and threats, as they can compromise the confidentiality, availability and integrity of the 5G network. Mitigation controls for these threats and attacks should be in place to ensure that the network is available all the time, in addition to preventing espionages and sensitive data breach.

1. Scope

This Technical Code specifies the security architecture and requirements for 5G network and applications.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) apply.

See Annex A.

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

See Annex B.

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.
.

4.1 Applications Service Provider (ASP)

Applications Service Provider (ASP) as defined in Communications and Multimedia Act 1998.

4.2 Bandwidth

Bandwidth refers to the maximum aggregated system bandwidth.

4.3 Network Element (NE) security

Protection of endpoint devices and Network Elements (NEs) and User Equipment (UE), including the physical security for NEs and the application software, which in a cloud‐based architecture is composed of Virtual Network Functions (VNFs).

4.4 Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) restricts network access based on a person’s role within an organisation and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that employees have to the network.

4.5 Service provider

Service provider refers to Network Service Provider (NSP) or ASP as defined in Communications and Multimedia Act 1998.

4.6 Transport/interface security

Protection of communication paths.

4.7 User information security

Protection of E2E user data, related to human users but also Machine Type Communications (MTC), including the transfer of E2E control plane and user plane data.

5. 5G security overview

5.1 5G security domains

The overview of the 5G security architecture with security domains, as defined by 3GPP TS 33.501 is shown in Figure 1.

In this architecture design, there are 6 security domains defined as follows:

a) Network access security

A set of security features that allow a UE to authenticate and access both 3rd Generation Partnership Project (3GPP) and non-3GPP network services securely, along with protecting the UE against attacks on radio interfaces. In addition, it includes the security context delivery from Serving Network (SN) to Access Network (AN) for the access security.

b) Network domain security

A set of security features that allow network nodes to securely exchange signalling data and user plane data between each other.

c) User domain security

A set of security features that ensure a secured user access to Mobile Equipment (ME).

d) Application domain security

A set of security features that enable applications in the user domain and in the application service provider domain to exchange messages securely.

e) Service Based Architecture (SBA) security

A set of security features that allows network functions of the SBA architecture to securely communicate within the SN domain and with other network domains, such as network function registration, discovery, and authorisation security aspects, as well as the protection for the service-based interfaces.

f) Visibility and configurability of security

This domain defines the set of features that allows any user to be informed whether a security feature is in operation or not. This security domain is not shown in Figure 1.

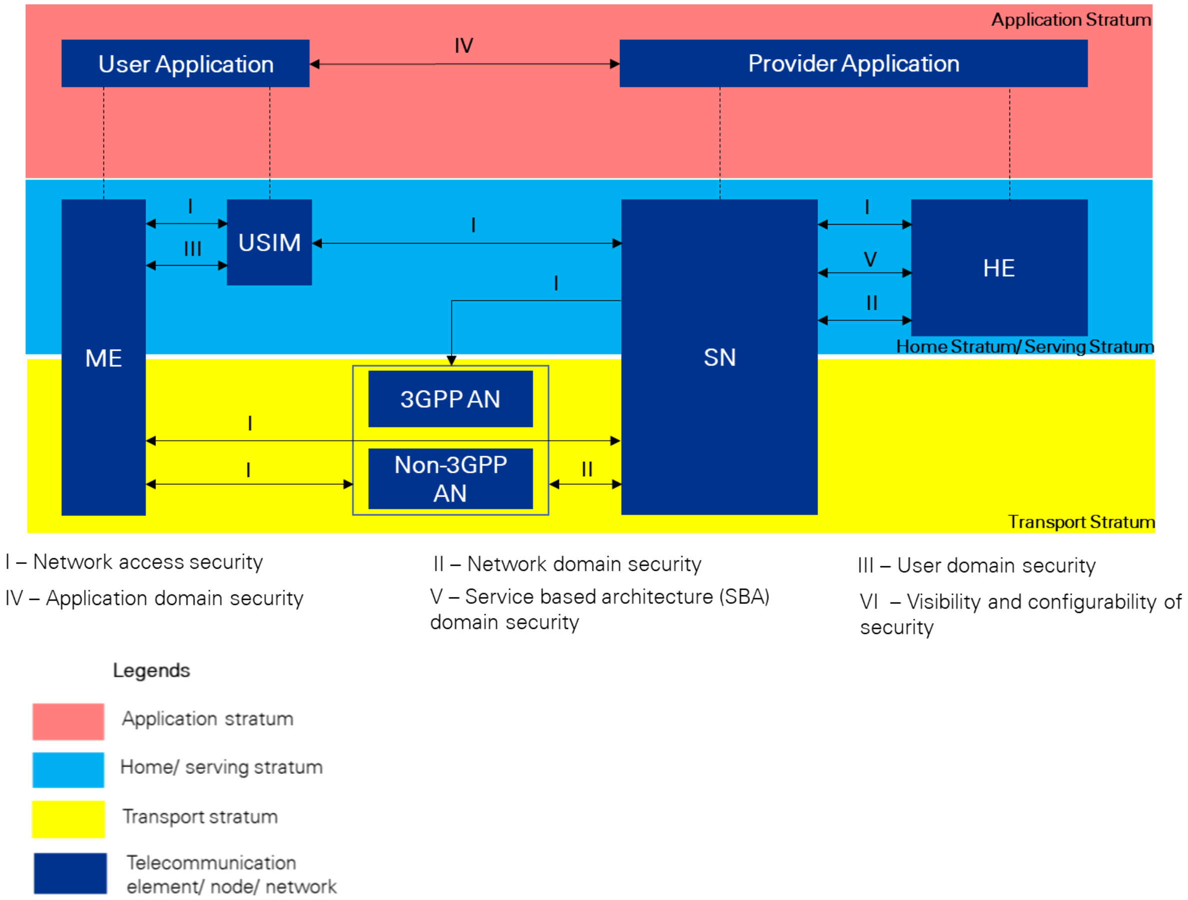

Application Stratum
User Application
IV
Provider Application
I
III
USIM
I
I
V
II
HE
ME
I
SN
Home Stratum/ Serving Stratum
3GPP AN
I
I
Non-3GPP AN
II
Transport Stratum
I – Network access security
IV – Application domain security
II – Network domain security
V – Service based architecture (SBA) domain security
III – User domain security
VI – Visibility and configurability of security
Legends
Application stratum
Home/ serving stratum
Transport stratum
Telecommunication element/ node/ network

Figure 1. Overview of 5G security architecture with security domains

Comparing with the 4G security architecture defined by 3GPP TS 33.401, the 5G security architecture design is almost similar to each other. The 2 main differences are as follows.

a) The AN in the 5G security architecture treats both 3GPP and non-3GPP access equally.

b) The introduction of the SBA security domain into the architecture, which is enforced between the SN and Home Environment (HE).

5.2 5G security planes

The 5G security architecture in Figure 2 illustrates the 3 security planes to be implemented and its interconnection with the service providers.

The 3 security planes are described as follows:

a) Management Plane - Security Plane for Management System

It will carry out service-oriented security function orchestration. During the life-cycle management of network and network slicing generation, the security function orchestration entity will carry out the following functions.

i) Modify security functions and security protection mechanisms according to the security Service Level Agreement (SLA) of service providers.

ii) Orchestrates network security functions within corresponding service slices.

iii) Efficiently deploys security functions required by slices.

In addition, this plane will also have a scalable identity management mechanism, where it will continue to inherit identity management based on Universal Serving Identity Module (USIM) cards, and supports the identity management mechanism based on the asymmetric key to uniformly manage the identities of industry customers, users, and terminals.

b) End User Plane - Security Plane for User Data

It will enforce a service-oriented differentiated security protection, where the security protection mechanism of the user plane is tailored according to the relevant security policies to meet data transmission protection requirements of various services, which may be different from one another.

c) Control Plane - Security Plane for Control Signalling

Using the security orchestration policy on the management plane, the network security function can be flexibly deployed based on the service-based architecture and virtualisation technology. Flexible security function deployment and invocation can efficiently support security capability exposure.

This plane also supports scalable authentication mechanism and remote identity management, such as tiered identity management mechanisms for enabling remote identity management of Internet of Things (IoT) terminals and wearable devices. It also supports authentication mechanisms based on symmetric keys and can be expanded to support asymmetric authentication as well.

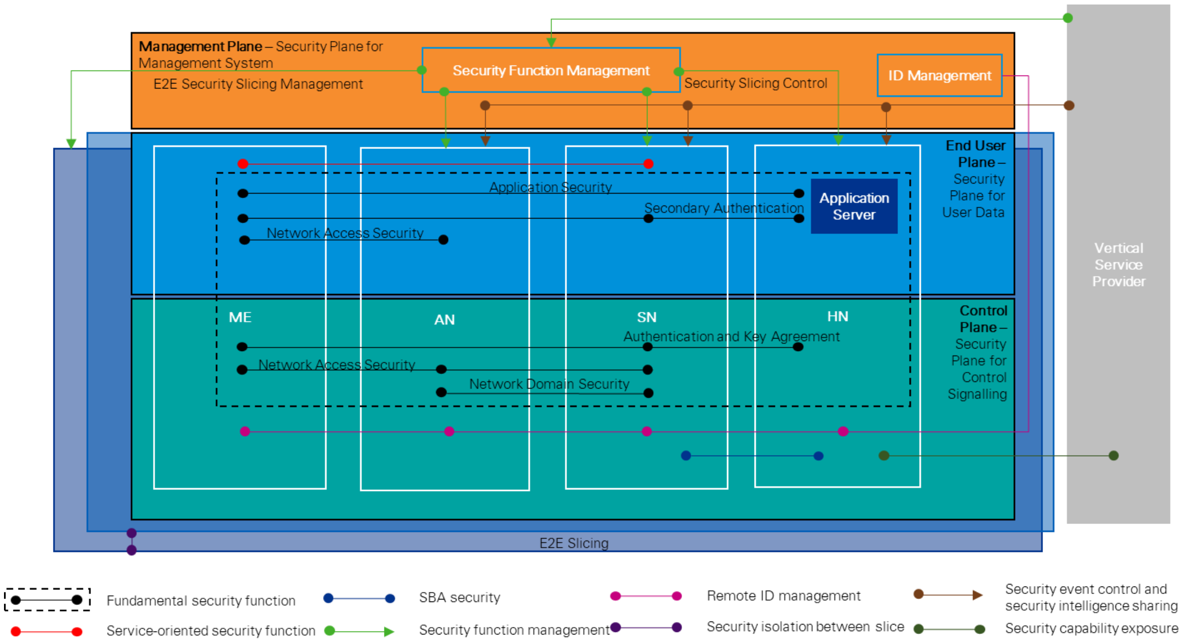

Management Plane – Security Plane for Management System
E2E Security Slicing Management
Security Function Management
Security Slicing Control
ID Management
End User Plane – Security Plane for User Data
Application Security
Secondary Authentication
Application Server
Network Access Security
ME
AN
SN
HN
Authentication and Key Agreement
Network Access Security
Network Domain Security
Control Plane – Security Plane for Control Signalling
Vertical Service Provider
E2E Slicing
Fundamental security function
SBA security
Remote ID management
Security event control and security intelligence sharing
Service-oriented security function
Security function management
Security isolation between slice
Security capability exposure

Figure 2. Overview of 5G security architecture with security planes

In addition to the 3 security planes mentioned, this security architecture also defines the following 2 security mechanisms to be implemented.

a) Slicing management security mechanism

Slicing management security mechanism shall consist of the following aspects.

i) Slicing security as a Service (SsaaS) will enable network service providers to provide customised security packages for vertical industries and monitor the performance of those packages. Network service providers may modify them and allocate resources based on the monitored results or other requirements.

ii) Slicing lifecycle security will ensure security in slice design, configuration, activation, operation and termination phases. It also protects security resources that are released from usage from being exploited by software vulnerabilities when a slice is decommissioned.

iii) Intelligent slicing security Operations and Maintenance (O&M) consists of automated slicing security function orchestration, slicing security policy control, alarm generation for slices through vulnerability scanning and anomaly detection technologies and other slicing security features.

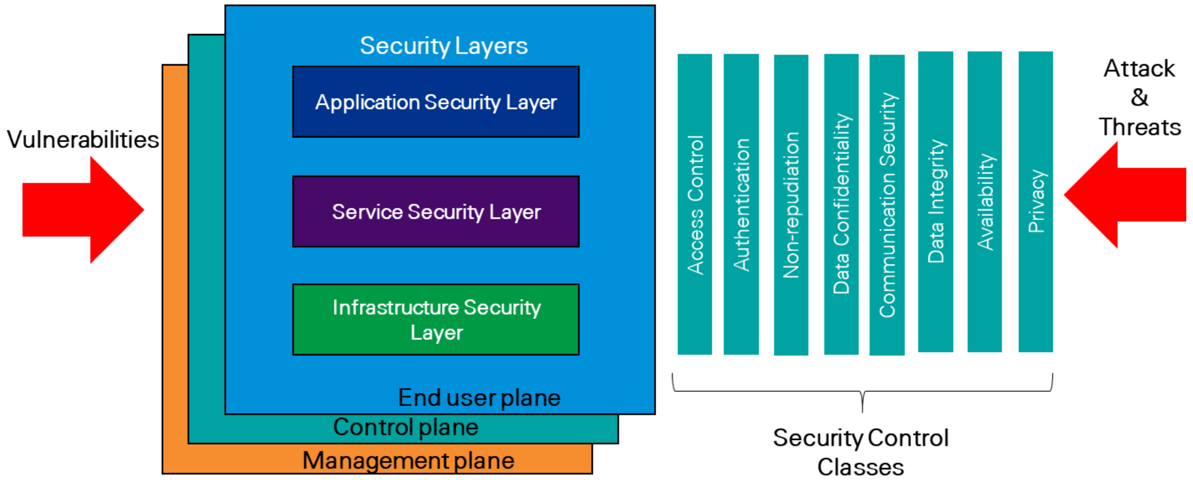
b) Proactive and intelligent security defence mechanism

The security events control and security intelligence sharing centre schedules and coordinates security components in order to implement intelligence sharing and security policy control between network service providers' networks and vertical industries based on security events. By providing a distributed deployment of security components and automatic configuration of security policies, the 5G security defence approach changes from a manual and passive response to intelligent and proactive defence approach, forming a unified collaborative security defence mechanism.

6. 5G security control classes

The End-to-End (E2E) security architecture as stipulated in ITU-T X.805 addresses security concerns for the management, control and use of network infrastructure, services and applications. This security architecture provides a comprehensive, top-down, E2E perspective of network security and can be applied to NEs, services and applications in order to detect, predict and correct security vulnerabilities.

Figure 3 shows the security control classes or dimensions that can be applied to the hierarchy of network equipment and facility groupings, which are known here as the security layers. These dimensions are also used to protect the security planes, which are the network activities in the security architecture.



End user plane - security plane for user data
Control plane - security plane for control signaling
Management Plane - service plane for management system

Figure 3. 5G E2E security architecture with security control classes

6.1 Security layers

The security layers are a series of enablers for a secured network solution. There are 3 security layers defined in Figure 3, which are described as follows:

a) application security layer

It focuses on security of the network-based applications to be accessed by service providers' customers, such as the following:

i) basic file transport;

ii) web browsing applications;

iii) fundamental applications (e.g. directory assistance, network-based voice messaging and email); and

iv) high-end applications (e.g. customer relationship management, electronic/mobile-commerce, network-based training, video collaboration and other applications).

Network-based applications may be provided by third-party ASPs, service providers (also acting as ASPs), or by enterprises hosting them in their own or leased data centres. At this layer, there are 4 potential targets for security attacks.

The targets are as follows:

i) application user;

ii) application service provider;

iii) middleware provided by third-party integrators (e.g., web-hosting services); and

iv) service provider.

b) service security layer

It addresses security of services provided by service providers such as for the following services:

i) basic transport;

ii) connectivity; and

iii) service enablers necessary for providing internet access and value-added services (e.g. freephone service, Quality of Service (QoS), Virtual Private Network (VPN), location services, instant messaging and others).

The services security layer shall be able to protect the service providers and their customers from security threats.

c) infrastructure security layer

It focuses on the securities of the network transmission facilities as well as individual NEs protected by the security dimensions. The functions of infrastructure security layer are as follows:

i) Represents the fundamental building blocks of networks, network services and applications. Examples of components that belong to the infrastructure layer are individual routers, switches and servers as well as the communication links between individual routers, switches and servers.

ii) Enables the services layer and subsequently, the services layer enables the applications layer. The security architecture addresses the fact that each layer has different security vulnerabilities and offers the flexibility of countering the potential threats in a way most suited for a particular security layer.

iii) Identify where security shall be addressed in products and solutions by providing a sequential perspective of network security. For example, first security vulnerabilities are addressed for the infrastructure layer, then for the services layer and finally for the security vulnerabilities are addressed for the applications layer.

6.2 Security planes

The security planes address specific security needs associated with network management activities, network control or signalling activities and end-user activities correspondingly. Networks should be designed in such a way that any events occurring on one security plane are completely isolated from the other security planes.

In Figure 3, the following security planes are defined.

a) Management Plane - Security Plane for Management System

It is concerned with the protection of Operations, Administrations, Maintenance and Provisioning (OAM&P) functions for NEs, transmission facilities, back-office systems and data centres. The management plane shall support the Fault, Capacity, Administration, Provisioning, and Security (FCAPS) functions.

b) Control Plane - Security Plane for Control Signalling

It is concerned with protection of the activities that enable the efficient delivery of information, services and applications across the network. It typically involves Machine-to-Machine (M2M) communications of information that allows the switches or routers to determine how to best route or switch traffic across the transport network. This type of information is sometimes referred to as control or signalling information.

c) End User Plane - Security Plane for User Data

It addresses security of access and use of the service provider’s network by customers. This plane also represents actual end-user data flows. End-users may use a network that only provides connectivity, they may use it for value-added services such as VPNs, or they may use it to access network-based applications.

6.3 Security control classes

A security control class is a set of security measures designed to address a certain aspect of network security. These security control classes are not only limited to the network, but also extended to cover applications and end-user information as well. In addition, the security control classes are also applied to cover service providers or enterprises offering security services to their customers.

Based on the ITU-T X.805, there are 8 security control classes to protect the entire E2E system from all major security threats. The security control classes are as follows:

a) access control

This security dimension shall be able to provide the following:

i) protects against unauthorised use of network resources; and

ii) ensuring only authorised personnel or devices are allowed access to NEs, stored information, information flows, services and applications.

The RBAC provides different access levels to ensure that individuals and devices can only gain access to, and perform operations on NEs, stored information and information flows that they are authorised for.

b) authentication

This security dimension shall serve to the following items:

i) confirm the identities of communicating entities;

ii) ensuring the validity of identities; and

iii) provides assurance that an entity is not attempting an unauthorised access to the communication system.

c) non-repudiation

This security dimension shall prevent an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions.

The examples of proofs are as follows:

i) proof of obligation, intent, or commitment;

ii) proof of data origin;

iii) proof of ownership; and

iv) proof of resource use.

It ensures the availability of evidence shall be presented to a third party and used as evidence to prove that some event or action has taken place by that user or device.

d) data confidentiality

This security dimension shall protect data from unauthorised disclosure and ensuring that the data content cannot be understood by unauthorised entities. Encryption, Access Control Lists (ACL) and file permissions are methods often used to provide data confidentiality.

e) communication security

This security dimension shall ensure the information flows only between the authorised end points, without getting diverted or intercepted between those points.

f) data integrity

This security dimension shall ensure the correctness or accuracy of data. The data shall be protected against unauthorised modification, deletion, creation and replication. Any attempts at those activities will be logged as an indication of these unauthorised activities.

g) availability

This security dimension shall ensure there is no denial of authorised access to NEs, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions shall be included in this category.

h) privacy

This security dimension shall ensure the protection of information that might be derived from the observation of network activities. Examples of this information include the following items:

i) visited;

ii) a user’s geographic location; and

iii) the Internet Protocol (IP) addresses and Domain Naming System (DNS) names of devices in a service provider network.

7. 5G security requirements

In general, the security implementations in 5G shall be flexible enough to accommodate the expected diversity of connected devices and systems, provide the ability to monitor their real - time status and traffic, and provide protection against the main attack vectors.

With a constantly changing threat landscape, it is crucial for network network service providers and service industries that use different part of 5G network to maintain E2E network security, which covers areas such as (but not limited to) E2E security, physical infrastructure security and virtualised resources security.

The 5G network assets to be secured are as follow:

a) user data information and user security configuration information;

b) NE security; and

c) transport/interface security.

There are many types of attacks done onto the 5G network. The example of such attacks as in the Table 1.

Table 1. Type of attacks onto 5G network

Type of attacks	Details
UEs or NEs	Stronger identity and authentication reduce the opportunity for misuse, fraudulent activity and identity theft.
Different network subsystems	Network subsystems such as Radio Access Network (RAN) and Core Network (CN) may experience resource exhaustion, terms and conditions violations such as SLA violations, or attacks on the DNS, billing, and signalling infrastructure and other systems.
End-user applications	Example of such attacks are server - side malware, application - level and protocol - specific Distributed Denial of Service (DDoS) attacks and others.

The security implementation in 5G shall not compromise the minimum performance requirements for the network as specified by the relevant technical codes or standards.

7.1 5G End-to-End (E2E) security framework

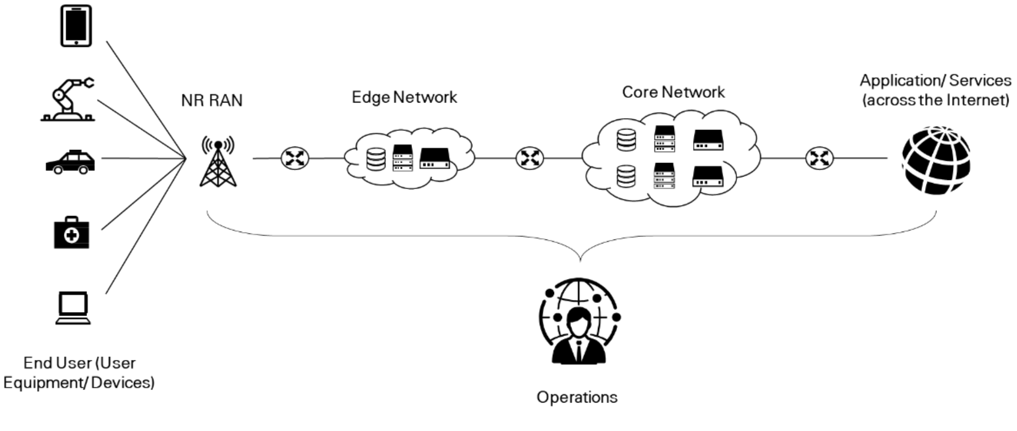

NR RAN
Edge Network
Core Network
Application/ Services (across the Internet)
End User (User Equipment/ Devices)
Operations

Figure 4. Overall 5G E2E network

Many NEs are present in the 5G E2E network, as shown in Figure 4. On the user end, the most commonly used devices in this category are ME such as mobile phones and personal computers that are connected to the 5G network. Not only that, other intelligent electronic peripherals such as smart devices and sensors, which are commonly used in IoT solutions also falls under this category.

These devices are connected to the 5G network via the wireless network, or the RAN network (base stations and gNodeB (gNB)). In 5G, edge computing, network equipment with data processing capabilities are placed closer to the user. By pushing out all of the computing capabilities to the edge network, instead of centralising it in a single location, latency between the UE and the network can be effectively reduced. Furthermore, it also helps to reduce bandwidth consumption, since only the data processing results needs to be sent to the CN.

The CN is the heart of the 5G network, where the main network devices will be located at. The network devices located here will be performing critical functions such as authentication, authorisation, policy control, resource allocation, encryption and security control and other functions. The CN will also be the gateway that connects users to various applications and services in the internet, in addition to allow smart devices to send back their data for processing.

According to ITU-T M.2083, the 5G network services can be divided into 3 categories, which are as follows:

a) enhanced Mobile Broadband (eMBB)

eMBB services are mainly be used for high bandwidth services such as 4K video streaming, augmented reality, high speed download and many other services that requires high speed.

b) Ultra Reliable Low Latency Communication (URLLC)

URLLC services consists of critical services that requires low amount of delay such as V2X, remote surgery and other mission critical applications.

c) massive MTC (mMTC)

mMTC services are mainly used for services with many connected devices such as smart city and smart home.

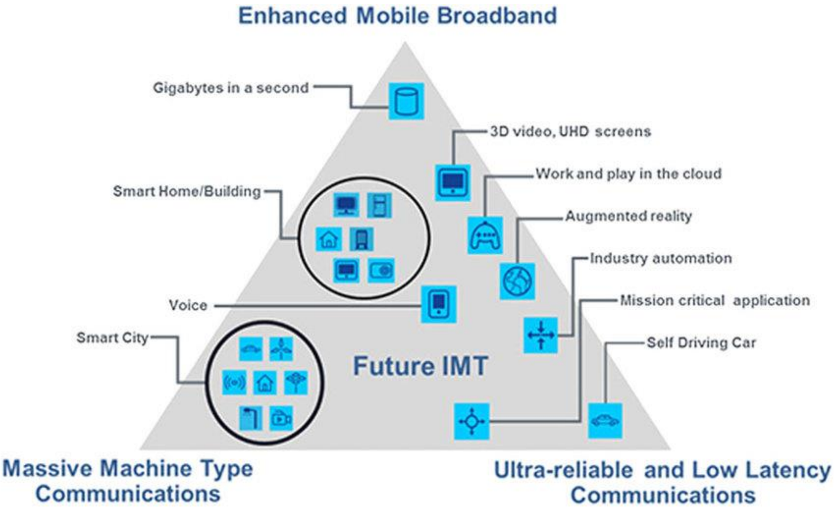

Enhanced Mobile Broadband
Gigabytes in a second
3D video, UHD screens
Work and play in the cloud
Smart Home/Building
Augmented reality
Industry automation
Voice
Mission critical application
Smart City
Self Driving Car
Future IMT
Massive Machine Type Communications
Ultra-reliable and Low Latency Communications

Figure 5. Usage scenario for 5G for IMT-2020

O&M teams shall ensure all equipment and services are being handled properly. Any new services, upgrades or rectifications that needs to be done shall to go through the right procedures before they are approved to be implemented in the network and to prevent any unwanted changes that may potentially case network disruption.

Standard Operating Procedures (SOP) and contingency plans shall need to be in place to ensure that the day-to-day operation is not affected and to minimise the duration of outages, if not outright prevent them.

The 5G E2E security framework can be viewed in 3 different perspectives as follows:

a) 5G security architecture with security domains;

b) 5G security architecture with security planes; and

c) 5G security architecture with security control classes.

7.1.1 5G security architecture with security domains

The definition of 5G security architecture with security domains is illustrated in Figure 6.

As per the 5G security architecture defined in Clause 6, the ME and SN elements (in green column in Figure 6) are located in both the transport and home/serving stratum, which is reflected in the overlap shown in Figure 6.

The strata overlaps are due to the fact that the ME and SN elements perform a common role in handling and exchanging user and control plane signals with not only between each other, but to the elements in the edge and core network as well.

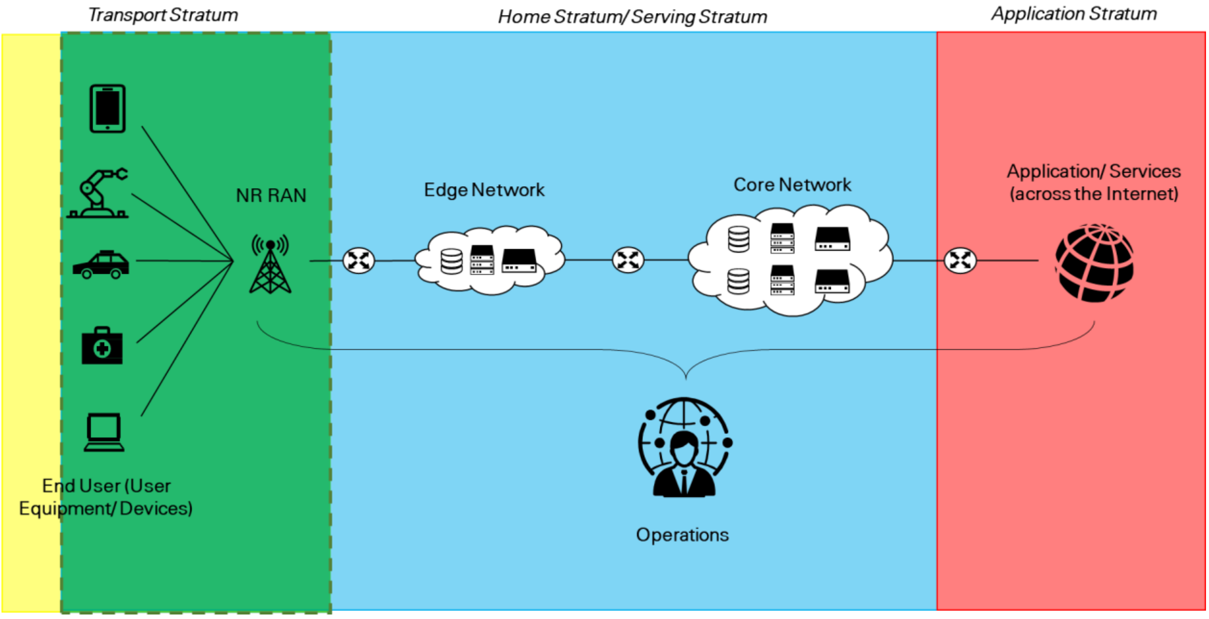

Transport Stratum
Home Stratum/Serving Stratum
Application Stratum
NR RAN
Edge Network
Core Network
Application/Services (across the Internet)
End User (User Equipment/Devices)
Operations

Figure 6. 5G security architecture with security domains

7.1.2 5G security architecture with security planes

The definition of 5G security architecture with security planes is illustrated in Figure 7.

Figure 7 highlights where the E2E elements lie in their respective security planes, based on the security planes defined in Figure 2. As the control plane and user plane signals will traverse through some common E2E elements, they will be subjected to both security controls defined in the control planes and user planes.

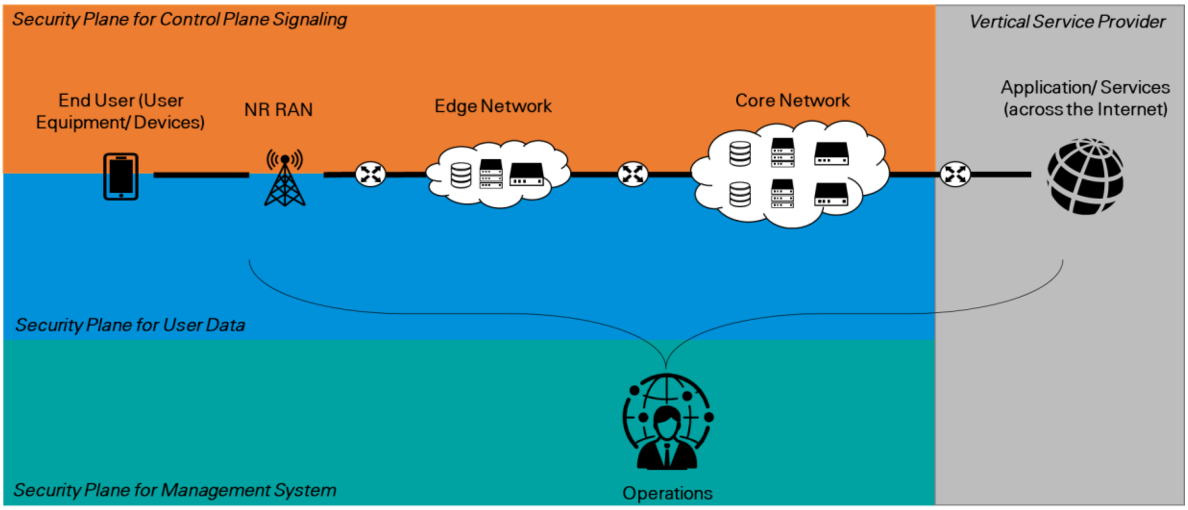

Security Plane for Control Plane Signaling
Vertical Service Provider
End User (User Equipment/ Devices)
NR RAN
Edge Network
Core Network
Application/ Services (across the Internet)
Security Plane for User Data
Security Plane for Management System
Operations

Figure 7. 5G security architecture with security planes

7.1.3 5G security architecture with security control classes

The definition of 5G security architecture with security control classes is illustrated in Figure 8.

For ease of representation, the end user plane, control plane and management plane are all consolidated into one part.

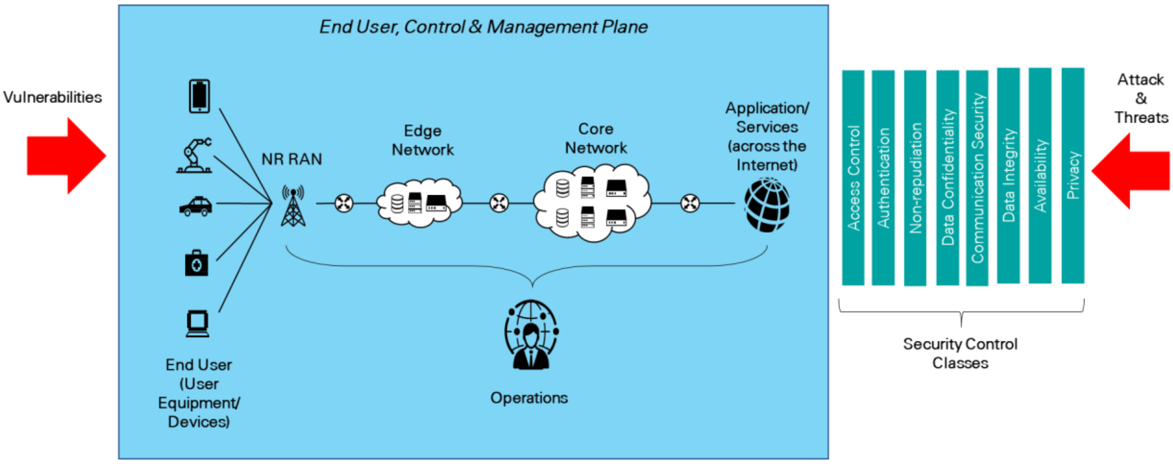


Figure 8. 5G security architecture with security control classes

7.2 5G security standards

The ITU-T has published several standards in various key security areas. The standards for key security areas as specified in Annex C shall be considered in the implementation of 5G security.

7.3 5G security infrastructure requirements

There are 17 key security areas that shall be considered for the implementation of 5G security infrastructure. The functions of each key security area are as described in Table 2.

In order to achieve the full 5G security features, the 5G services shall be deployed using a 5G Stand Alone (SA) architecture or known as Option 2 by the 3GPP. In the SA architecture, 5G core is the major component to be deployed and it has various network functions to deliver fully secured 5G services to the customers.

Table 2. Functions of each key security area

No	Key security areas	Functions
1.	Security architecture	Covers architectural aspects of security for next generation system.
2.	Authentication	Covers authentication between UE and 3GPP network which comprises of authentication framework, identifiers, credentials and authentication methods.
3.	Security context and key management	Deals with security aspects related to management of security context and security keys.
4.	RAN security	Covers security for next generation radio interface and RAN such as protection of user plane and control plane between RAN, base stations and CN, negotiation of security algorithm, handling of Access Stratum (AS) security context, protection against Denial-of-Service (DoS) attacks towards the network infrastructure or against others devices and privacy aspects.
5.	Security within Next Generation - User Equipment (NG-UE)	Covers security of sensitive data handled within the NG-UE.
6.	Authorisation	Covers authorisation of the UE to access the network and authorisation of the network to serve the UE.
7.	Subscription privacy	Covers various aspects related to the protection of subscribers' personal information, for example identifiers, location, data and other information.
8.	Network slicing security	Covers security aspects related to the network slicing concept such as service access, network function sharing and slice isolation.
9.	Relay security	Covers security of the next generation connectivity over relays, as various equipment with different network and resources capabilities may be connected to relays via 3GPP or other technologies.
10.	Network domain security	Covers security of the signalling protocols in the network domain such as authentication, integrity, and availability; that addresses issues such as overloading of control plane messages, lack of native support of authentication and integrity mechanisms in the CN signalling messages and architectural security issues coming from the interconnection network.
11.	Security visibility and configurability	Covers presentation of security information to a user of a UE and management of security configuration by users, as the users may need to be aware of the security available for a specific service so that they can choose whether this is secure enough for the service use.
12.	Credential provisioning	Covers security aspects of provisioning 3GPP credentials on equipment that will access the next generation system.
13.	Interworking and migration	Covers security aspects related to the interworking and migration scenarios between radio technologies and possible CN concepts such as roaming scenarios with other service providers that have and do not have a next generation CN.

Table 2. Functions of each key security area *(continued)*

No	Key security areas	Functions
14.	Small data	Relates to massive number of IoT UEs that usually send small amount of data sporadically while moving around. For this scenario, the UE sends data to the next generation core via a user plane path without requiring more signalling to set up and tear down dedicated bearers.
15.	Broadcast/multicast security	Covers security for broadcast services that will be used in vertical industries such as critical communication, Vehicle-to-Everything (V2X), and mMTC.
16.	Management security	Covers security related to management plane and deployment scenarios. In the next generation network, several changes can introduce difficulties into network management and deployment, such as network architecture evolution, network virtualisation, deployment location of network functions and opening of management interfaces.
17.	Cryptographic algorithms	Relates to cryptographic algorithms to be used for security mechanisms and protocols within next generation system.

In addition to the 17 key security areas mentioned in Table 2, physical security as specified in MCMC MTSFB TC G009, *Information and Network Security - Requirements* shall also be considered for 5G infrastructure such as base stations, computing systems and CNs.

7.4 5G End-to-End (E2E) threat landscape and security controls

With many elements in the 5G E2E architecture, there will be various threats for each of these elements. These threats will compromise the confidentiality, availability and integrity of the entire 5G network, leading to situation such as network disruption, confidential data leakage and unauthorised modification or even deletion of critical data and information.

To minimise these threats, or even outright prevent them, control measures shall be in place for those elements. Annex D shows the summary of the security threats and security controls for each element in the 5G E2E architecture. It is divided into the following categories.

a) End user (refer Table D.1).

b) NR RAN (refer Table D.2).

c) Edge network (refer Table D.3).

d) CN (refer Table D.4).

e) Applications/services (refer Table D.5).

f) Operations (refer Table D.6).

7.4.1 End user

7.4.1.1 Physical elements

The end user generally consists of consumer devices such as mobile phones or personal computer, or unmanned electronic devices that are usually used for IoT application. These devices are installed with the Universal Integrated Circuit Card (UICC) and embedded UICC (eUICC). To safeguard the integrity of UICCs, eUICCs with remote provisioning capabilities, and of their applications and data, it is essential that the supplier environment and processes that are used to manufacture and manage UICCs and eUICCs are secured.

For this case, Global System for Mobile Communications Association (GSMA) has Security Accreditation Scheme (SAS) that allows network service providers to access the security of their UICC and eUICC suppliers, and their eUICC subscription management service providers.

There are 2 schemes that run under SAS, which are:

a) SAS for UICC Production (SAS-UP)

UICC and eUICC manufacturers will subject their production sites and processes to a comprehensive security audit, with successful sites awarded with security accreditation for a period of one year, extending to two further years upon each successful renewal.

b) SAS for Subscription Management (SAS-SM)

In ensuring the industry confidence in the security of remote provisioning for eUICCs, a related security auditing and accreditation scheme exists for the providers of eUICC subscription management services.

For IoT devices, referring to the GSMA, the physical aspects of those devices, such as implementing a tamper resistant trust anchor should able to protect the IoT devices against Focused Ion Beam (FIB), side channel attacks and glitching. It is also recommended to implement a tamper resistant product casing to protect the internal components from being compromised, in case of any attempts in opening the device. Other security recommendations such as environmental lock out thresholds (e.g. temperature and humidity) and power warning threshold should be able to ensure the system operator is warned beforehand when reaching those thresholds, before attacks takes advantage of the situation.

7.4.1.2 Technical elements

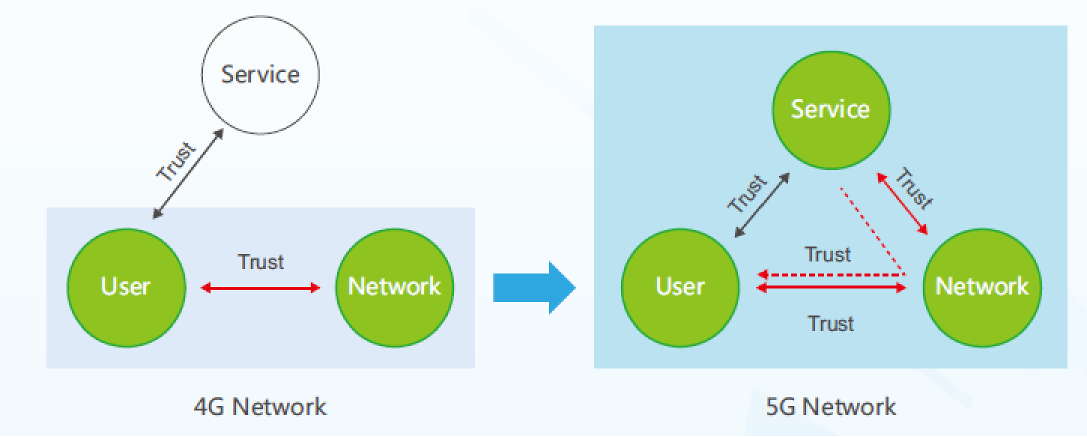


Figure 9. Comparison of trust model between 4G network and 5G network

In 5G, ME and IoT devices will be authenticating to both network providers and service providers, thus the subscriber’s identifiers and credentials shall be validated. Previously in 4G networks, any devices only need to authenticate with the network service provider only, however, this is not the case in 5G. With both network and service providers playing an essential role in authentication of the user devices and endpoints, a new trust model shall be created, where the user devices, network providers and service providers has a trust relationship with one another, allowing an even secured and efficient identity management system as in Figure 9.

With many devices connected simultaneously to the network, it is essential to ensure that only the verified devices and endpoints can use the services provided. A hybrid authentication model can be used in this situation to make authentication procedures simpler and cost effective.

A user device or endpoints can choose the following options:

a) authenticated by the network service provider only;

b) authenticated by the applications service provider only; or

c) authenticated by both network service provider and applications service provider.

Management of the user identity can also be made more effective by using an identity that is a combination of device identity and service identity, where the devices can have more than one service identities, assigned by the service providers.

For mutual authentication between the UE and the network, the Authentication Key Agreement (AKA) procedure is used during the attach procedure. There are 2 types of AKA procedures, which are 5G-AKA and Extensible Authentication Protocol-AKA (EAP-AKA). In these 2 authentication procedures, key hierarchy is defined for authentication purposes, where the keys at the top of the pyramid is used to define the keys at the lower levels of the hierarchy, as shown in Figure 10.

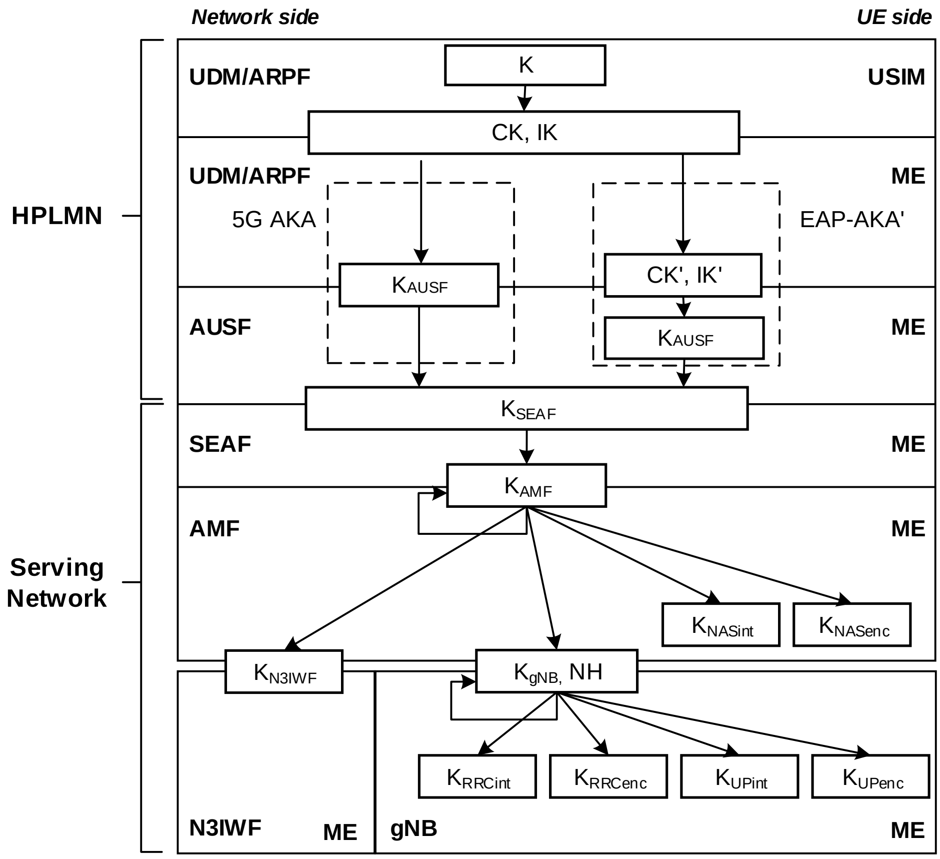


Figure 10. Key hierarchy in 5G

To prevent the hijacking of 5G devices, identities in telecommunication and Information Technology (IT) domains shall be made visible to Identity Access Management (IAM) systems, even while roaming. These systems are considered to have a Federated Identity and Access Management Models (FidAM) with each other.

7.4.1.3 Administrative elements

It is crucial that the subscriber’s privacy is preserved in the 5G network. Without any mechanisms to ensure the subscriber’s privacy, sensitive information can be extracted by attackers by intercepting transmitted messages. To ensure the subscriber’s privacy is preserved, the 5G network uses something like Packet domain Temporary Mobile Subscriber Identity (P-TMSI) in the 4G network, which is the Subscription Concealed Identifier (SUCI).

This temporary identity shall able to mask the Subscription Permanent Identifier (SUPI), and prevent the SUPI from being visible in the messages in case of interception. The SUCI is used during authentication purposes, and it is resolved into the original SUPI by the Unified Data Management (UDM), using the Security Identifier Deconcealment Function (SIDF) built within the UDM.

7.4.2 New Radio RAN (NR RAN)

7.4.2.1 Physical elements

As the New Radio RAN (NR RAN) elements will be placed in various locations, it is important that those elements are physically secured. The following physical security elements (but not limited to) shall be implemented at the RAN site.

a) Fencing and locks

All sites on vacant land comes with fencing and locks. However, for in-building and roof-top sites, fencing is not applicable but instead they are all secured and locked using cabinets or cabin doors.

b) Alarms and security camera

Intruder alarms sensors are installed and monitored real time for all sites. Security cameras are to be installed only on designated hotspot sites with high frequency of theft incidents (this is a very small number in proportion compare to all 5G sites nationwide). Installing security cameras for every 5G sites are impractical and should be based on the jurisdiction of the 5G network service providers.

c) Disable port

Ports that are not used for RAN devices shall be disabled to prevent attackers from having a means to access the network.

7.4.2.2 Technical elements

In 5G, the SUPI is concealed or encrypted into the SUCI using a public key. This SUCI shall be decrypted using a private key stored in the SIDF. However, with technology constantly evolving, the public security key can be eventually broken. This is further shown with Moore’s Law, where the increase in computing power for hacking devices makes it easier to crack these security keys, allowing attackers to gain access to the network devices in a shorter time.

In addition to that, there are also quantum computing devices which can decipher these public security keys in a much shorter time as compared to traditional computer devices. Some symmetric key ciphers such as Advanced Encryption Standard (AES) may considered to be quantum-safe.

To ensure that the symmetric keys can be safely distributed between various parties, quantum key distribution shall be used, where the functions are as follows:

a) uses quantum physics to secure the distribution of symmetric keys;

b) allows the sender and receiver to know if an attacker tries to intercept the information within the message sent; and

c) ensures the security of key exchanges and security keys can be safely used with conventional cryptography algorithms.

However, it is to note that powerful quantum computers capable of breaking any types of cryptography, including quantum cryptography. The possibility of building a computer with such capability is highly unlikely anytime soon, nevertheless the public need to embrace the standards of protection against quantum computers.

One of the threats faced by NR RAN is DDoS attacks by botnets. In order to detect them, detection functions shall be installed in the RAN equipment, specifically the Central Unit Control Plane (CU-CP), since it will be handling most of the Radio Resource Control (RRC) connections. These detection functions will have adjustable threshold for RRC connection requests, along with analytic algorithms to determine whether an event is a DDoS event or not. These functions should also be able to get updates from external machine learning and artificial intelligence. Do note that such protection relies on the Network Functions Virtualisation Infrastructure (NFVI) layer for support.

It is also necessary to ensure that the air interface has protection from jamming attempts, which is related with DDoS attacks mentioned earlier. Overload control mechanisms should be in place to ensure that the network is available when handling any number of requests. Pseudo-random time hopping spread spectrum was also proposed to improve the performance of the system on jamming, error and switching probability. Anti-jamming offloading mechanisms also helps to ensure that radio resources can be offloaded even under jamming scenarios. It is to note that on-going studies on protection against jamming attacks within 3GPP are still being carried out, thus the specifications on this matter have not been finalised yet.

Network slicing plays an important role in NR RAN, since various applications need different types of performance criteria, for example, URLLC services require very low latency performance. With the use of network slicing technology, isolation is a very important aspect. There are 2 categories of isolation such as follows:

a) resource isolation

Refers as the resources that were assigned to a slice, for example memory, compute and storage. The resource isolation shall not be taken away by another network slice to ensure that the resources provided to a slice is always available all the time.

b) security isolation

Security isolation ensures that information contained within a network slice cannot be accessed or modified by other slices.

Each network slice shall have various security measures to ensure the network isolation is properly done. These security measures include (but not limited to) the following mechanisms:

a) virtual firewalls;

b) traffic filtering mechanisms (e.g. Virtual Local Area Network (VLAN) or Virtual Extensible Local Area Network (VXLAN) partitioning and ACL);

c) intrusion and anomaly detection systems;

d) cryptographic traffic protection; and

e) other mechanisms.

In addition to slice isolation, slice quarantine shall be implemented to ensure inter-slice and intra-slice security. This mechanism ensures that any compromised slices is immediately isolated from the network and other slices, so that any attacks are confined to that compromised slices only. The implementation of the quarantine slice is made possible in transport by segment routing and in the data centre by segmentation technology. By combining these 2 segmentation methods, it will create an architecture capable delivers E2E, segmented network delivering visibility and agility in threat detection and management.

The fronthaul and backhaul security shall also be considered to ensure that the transport network is not compromised from link failures and interferences. Link redundancy shall be implemented too so that traffic can be rerouted in case of link failures or overload conditions. DDoS and DoS detection shall be implemented, in addition to the cryptographically secured IP Security (IPSec) or Media Access Control Security (MACSec) links for transmission of data between network equipment.

7.4.2.3 Administrative elements

In 5G, the hardware and software infrastructure used could be in a multi-vendor environment. With a multi-vendor environment, there would be many identities required to access these devices for day-to-day operations. It is crucial that an IAM system shall be in place to provide the users with the required roles and access policies. This is to prevent unauthorised users from accessing to NEs, where they may cause changes to the system configurations or sabotages, whether intentionally or unintentionally. An identity federation would also be recommended for a multi-vendor environment, as a means of unifying all the users and roles under one management umbrella, making it easier and more efficient in managing them.

In addition to that, a logging and monitoring system or Security Information and Event Management (SIEM) solution should be implemented. Threshold for critical performance parameters shall be set, such that in any event where the threshold for those parameters has been exceeded, the system will alert the network service providers on such event. The event logs for this event will be generated for analysis purposes. The SIEM solution should also be able to generate the report on the overall system performance on a regular basis.

7.4.3 Edge network

7.4.3.1 Physical elements

In the edge network, some of the core functions are moved to the edge, so that processing of those functions is done at the edge network instead of the CN, which allows the following process to be executed.

a) Help to reduce computing resources required at the CN.

b) Reduce the latency between the user and the CN, due to its close proximity to the user.

As the edge equipment is placed in a relatively open environment, the equipment is more vulnerable to physical damage and requires physical security measures. The control elements shall be implemented according to 7.4.2.1.

7.4.3.2 Technical elements

As 5G is based on Network Functions Virtualisation (NFV) technology, it is imperative that the edge network shall implement NFV security controls. Virtualised security solutions such as virtual machine security and container security should be implemented in the edge network. This is to ensure the virtual machines running in the NFV network is secured from intrusions and attacks.

VNF software packages shall have signature verification to ensure the security of the software running in the edge network. Such protection also requires dependency with the NFVI for support.

The network slice security plays an important part in the NR RAN, edge network and CN. Resource and security isolations shall ensure the slice is not affected by any events in the network, such as network scaling or security threats. Any compromised slice shall be quarantined to prevent from affecting other unaffected slices and confine any threats to that affected slice only.

Software defined segmentation enables policies to be enforced for users, applications and devices (IoT, M2M and enterprise network devices). In the data centre part of the 5G architecture, software defined segmentation leverages segment routing. When software defined segmentation is used, the security group tags should be defined and managed by an identity and segmentation policy controller. The controller should share group information with other group-based policy schemes to allow segmentation of the traffic and restriction of communication between defined network interfaces. This security approach shifts the network security away from reliance on long lists of IP address to a flexible and automated model which is better managed and more effective against new and expanding threat vectors.

As the NEs are placed closer to the edge network, the risk of data theft and leakage are high. Thus, a higher emphasis on data security is required. All user data assets, including access control and user identification shall be identified. Highly sensitive data also shall be encrypted and sent over secured communication channels that are secured with IPSec, Transport Layer Security (TLS) or other security algorithms to prevent data loss or leakage. All data processing, analysis and usage shall also comply with privacy laws and regulations in combination with data operation object authentication and authorisation.

As the edge network will be connected to the NR RAN and CN, the fronthaul and backhaul security shall be secured from link failures and interferences. The controls elements for fronthaul and backhaul security should be implemented according to 7.4.2.2.

7.4.3.3 Administrative elements

The controls elements as stipulated in 7.4.2.3 should be applied to the edge computing nodes, in order to ensure the following conditions:

a) only the right people are able to access the edge nodes;

b) the correct roles and access policies are assigned to the right people; and

c) the system is constantly under watch and monitoring for any anomalies and attack attempts.

7.4.4 Core Network (CN)

7.4.4.1 Physical elements

The 5G CN elements will usually be placed in a centralised data centre, unlike the NR RAN and edge NEs, which are placed at various locations that are close with the users. The data centre shall be thoroughly secured physically from unauthorised access, since the CN elements will be handling the critical functions of the entire 5G network. The control elements shall be implemented according to 7.4.2.1.

7.4.4.2 Technical elements

The CN uses NFV technology, the controls as stipulated in 7.4.3.2 should be applied to this area as well. Network slice isolation shall ensure that any resources allocated to a slice is not affected by any other slice, or the safety of network slices are not compromised by hacked network slices. Software defined segmentation policies provides efficient method of managing network traffic and network interfaces.

The CN will be handling a lot of sensitive data such as user information, location, services and other data, the data security policies shall be implemented here to minimise data loss and data leakage. The CN will be the final gateway before data is transmitted over the internet to vertical industries. It is crucial that transport security shall be enforced with IPSec and TLS security algorithms being used along with link redundancy options and DDoS protection.

Network network service providers are connected via the Security Edge Protection Proxy (SEPP) for interconnect security or security between different network service providers. All signalling traffic between network service providers will be passed through this NE via the N32 interface and authentication between SEPPs are required to filter the traffic passing through them. In the N32 interface, an application layer security solution shall be implemented to provide protection of sensitive data attributes while still allowing services throughout the interconnect.

Stronger security is required for the protocol layers such as application and transport layers when SBA is used, in addition to the protection of the communication between the CN elements at the IP layers (e.g. IPSec). OAuth 2.0 framework is required to protect the application layer to support TLS 1.2 and TLS 1.3 for the protection of the communication layer. By using OAuth 2.0, any network function needs to authenticate with the Network Repository Function (NRF) before being able to use any of the services offered by the NRF.

7.4.4.3 Administrative elements

The controls as stipulated in 7.4.2.3 should be applied to the CN elements, in order to ensure the following conditions:

a) only the right people are able to access the CN elements;

b) the correct roles and access policies are assigned to the right people; and

c) the system is constantly under watch and monitoring for any anomalies and attack attempts.

7.4.5 Application/Services

7.4.5.1 Physical elements

With the emergence of cloud technology, most of the services and applications will be hosted fully on cloud, instead of being hosted on premise. Nevertheless, the cloud data centre hosting those services and applications shall be thoroughly secured physically from unauthorised access.

The control elements shall be implemented according to 7.4.2.1.

7.4.5.2 Technical elements

The services and applications running on 5G network may be very critical to vertical industries. It is crucial that safeguards for them are in place to prevent attackers from gaining access and perform acts of malicious intents. Application security measures such as (but not limited to) encryption of data, hardening of application interfaces and Applications Programming Interface (API) security shall be enforced so that the application does not have loophole that can be exploited by attackers.

Segmentation of application traffic from management traffic is recommended as well, so that attacks in one area cannot be used as a method to gain access into another area.

Security policies shall be enforced to ensure the services and applications are securely hosted in the cloud environment.

Isolation between applications also shall be enforced, so that no compromised application can affect other running applications, potentially disruption the entire system.

Data flowing within and out of the network should be encrypted. Data policies also shall be established for treating data at rest, in motion and has reached end of their lifecycle.

For voice calls, it is necessary to ensure that controls against spam calls are implemented, as spam calls can lead to fraud cases and call abuse.

7.4.5.3 Administrative elements

The controls as stipulated in 7.4.2.3 should be applied to the services and applications, in order to ensure the following conditions:

a) only the right people are able to access them;

b) correct roles and access policies are assigned to the right people; and

c) the system is constantly under watch and monitoring for any anomalies and attack attempts.

7.4.6 Operations

7.4.6.1 Physical elements

The operations team shall perform the day-to-day activities of the 5G system. Thus, the control elements shall be implemented according to 7.4.2.1.

In addition, they shall monitor and detect if there are any indication of hardware or equipment failure, and replace them as soon as possible. This is to avoid any potential service interruption.

Critical software patches and security upgrades also shall be done as soon as possible to ensure that the software for the network equipment are up-to-date and any security vulnerabilities are resolved.

7.4.6.2 Technical elements

The SIEM solution shall be in place for day-to-day operations for logging and monitoring purposes. Any anomalies in system performance or indication of a system breach shall be detected and logged for analysis purposes.

Furthermore, alarms for system performance shall be set to trigger when the performance reaches the threshold level. All the logs and event files shall be stored in a centralised storage centre for audit purposes in a fixed period before being properly disposed.

It is also crucial to have a system with a secured booting mechanism, to ensure that no important files are tampered and modified during system start up. The system should also have an integrity check on important software files and running code to prevent tampering during runtime.

The NIST Identify, Protect, Detect, Response and Recover (IPDRR) framework is recommended to manage cybersecurity risk at a high level and enabling risk management decisions.

7.4.6.3 Administration elements

The IAM control shall be implemented to assist the operation team for day-to-day operations in handling users. Each user will have their own account with certain amount of privilege and access which only able to access to certain elements. This is to ensure no users can access unauthorised network equipment, nor are they able to perform unauthorised changes to the system. If there is a multi-vendor environment, an identity federation is recommended to synchronise all identities across the entire infrastructure under one identity platform.

The security standards and procedures shall be available as part of the compliance for privacy laws and regulations when troubleshooting a network slice that contain sensitive data. Security rules also shall be enforced when performing day-to-day O&M routines, so that human errors can be minimised. This is to ensure no safety procedures are breached, which may potentially cause harm to the network or in severe cases, to individuals as well.

It is recommended to have a third party to perform a system wide audit. Its purposed is to detect any vulnerability present in the system and loopholes in standard operating procedures.

8. 5G security elements severity

According to 3GPP TS 33.501, the 5G security architecture consists of 3 stratums (see Figure 1) as follows:

a) application stratum;

b) home/serving stratum; and

c) transport stratum.

The home/serving and transport stratums have different levels of security sensitivity, where the transport stratum has the lowest security sensitivity. It does not involve sensitive data such as SUPI, which is the main identifier used in 5G and user root keys. Only low-level keys in the key hierarchy are used here (e.g. user access keys). This stratum consists of some UE functions, all RAN functions and some CN functions such as the User Plane Function (UPF).

The serving stratum consists of Access and Mobility Management Function (AMF), NRF, SEPP, and Network Exposure Function (NEF) of the home service provider. This stratum has a relatively high security sensitivity as it handles mid-level keys in the key hierarchy, such as the AMF keys.

On the other hand, the home stratum, which consists of the Authentication Server Function (AUSF) and UDM of the home service provider, has a high security sensitivity as it handles sensitive data such as SUPIs, user root keys and high-level keys.

In accessing the severity of the network assets in 5G, 2 factors shall be considered are as follows:

a) type of impact

Whether a threat leads to compromised confidentiality, availability and/or integrity of the 5G network.

b) scale of the impact

The impact is evaluated in terms of number of users affected, duration of outages, number of base stations or cells affected and severity of the information altered or accessed.

Table 3 shows the network functions on their severity levels and justification for being placed at that level of sensitivity. The sensitivity level is classified as follows:

a) critical

These network elements perform extremely vital network functions regarding the operations and security of the entire network, in addition to processing and storing sensitive information. Any attacks to these network functions will severely cripple the network, if not outright, bring the entire network down completely.

b) high

These network elements perform important network functions regarding the operations and security of the network. These network functions may carry sensitive information. Any attack here will affect the network functionality, but it may not bring the network down completely.

c) medium

These network elements perform relatively important network functions regarding the operations and security of the network. These network functions may carry sensitive information. Any attack here will slightly affect the network functionality, but it will not bring the network down completely.

d) low

These network elements network functions that may be deemed as optional network functions for certain network service providers. These network functions are supplementary to the other important network functions. Any attack here will be deemed as a minor hinderance to the network functionality and it will not bring the network down completely.

Table 3. Severity level of the NEs and functions

Category of network function / elements	Example of key elements	Description	Severity level
CN functions	a) UE authentication, roaming and session management functions b) UE data transport functions c) Access policy management d) Registration and authorisation of network services e) Storage of end-user and network data f) Link with third-party mobile networks g) Exposure of CN functions to external applications h) Attribution of end-user devices to network slices	Threat affecting the CN will affect the entire network's confidentiality, integrity and availability, in addition to potential sensitive data leakage, as sensitive data are being transmitted through the CN components.	Critical
NFV Management and Network Orchestration (MANO)	N/A	There are many NEs and functions in this category that performs important functions such as core access and control functions, lawful interceptions, security and cryptographic functions. Any attacks to the NEs and functions in this category will affect functions necessary to operate the 5G network.	Critical
Management systems and supporting services (other than MANO)	a) Security management systems b) Billing and other support systems such as network performance	Despite not carrying network traffic, there are many important network functions in this category. Any threat attacks to this area can put the entire network at risk. Sabotages and malicious attacks could potentially disrupt the entire 5G network function.	High

Table 3. Sensitivity level of the NEs and functions *(continued)*

Category of network function / elements	Example of key elements	Description	Sensitivity level
RAN	Base stations	Generally, AN function is classified as relatively high sensitivity network functions, though the degree of sensitivity those functions varies according to various factors. Some network functions, which are considered less sensitive in the traditional network, will become more sensitive in the 5G network due to them handling user data or performing smart and sensitive function. With the introduction of Mobile Edge Computing (MEC), more sensitive network functions are physically moved from the CN to be closer to the edge network.	Medium
Transport and transmission functions	a) Low-level network equipment (routers, switches, etc) b) Filtering equipment (e.g. firewalls, Intrusion Prevention System (IPS))	The assessment of the sensitivity of the transport and transmission functions depends various factors, such as their role in the transmission network.	High
Internetwork exchanges	a) IP networks external to Mobile Network Service Provider (MNSP) premises b) Network services provided by third parties	The assessment of the sensitivity of the internetwork exchanges depends various factors, such as their interconnection role between various network network service providers.	High

Annex A
(normative)

Normative references

MCMC MTSFB TC G009, *Information and Network Security - Requirements*

ITU-T X.680 | ISO/IEC 8824-1, *Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ITU-T X.681 | ISO/IEC 8824-2, *Information technology - Abstract Syntax Notation One (ASN.1): Information object specification*

ITU-T X.682 | ISO/IEC 8824-3, *Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification*

ITU-T X.683 | ISO/IEC 8824-4, *Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*

ITU-T X.690 | ISO/IEC 8825-1, *Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*

ITU-T X.691 | ISO/IEC 8825-2, *Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*

ITU-T X.693 | ISO/IEC 8825-4, *Information technology - ASN.1 encoding rules: XML Encoding Rules (XER)*

ITU-T X.694 | ISO/IEC 8825-5, *Information technology - ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1*

ITU-T X.695 | ISO/IEC 8825-6, *Information technology - ASN.1 encoding rules: Registration and application of PER encoding instructions*

ITU-T X.509 (10/19), *Information technology* - *Open Systems Interconnection* - *The Directory: Public-key and attribute certificate frameworks*

ITU-T X.805*, Security architecture for systems providing end-to-end communications*

ITU-T X.1141, *Security Assertion Markup Language (SAML 2.0)*

ITU-T X.1142, *eXtensible Access Control Markup Language (XACML 2.0)*

ITU-T X.1144, *eXtensible Access Control Markup Language (XACML 3.0)*

ITU-T X.1205, *Overview of cybersecurity*

ITU-T X.1243, *Interactive gateway system for countering spam*

ITU-T X.1254, *Entity authentication assurance framework*

ITU-T X.1303, *Common alerting protocol (CAP 1.1)*

ITU-T X.1500, *Overview of cybersecurity information exchange - Structured cybersecurity information exchange techniques*

ITU-T X.1520, *Common vulnerability enumeration*

ITU-T X.1521, *Common vulnerability scoring system*

ITU-T X.1524, *Common weakness enumeration*

ITU-T X.1525, *Common weakness scoring system*

ITU-T X.1526, *Language for the open definition of vulnerabilities and for the assessment of a system state*

ITU-T X.1528, *Common platform enumeration*

ITU-T X.1546, *Malware attribute enumeration and characterization*

3GPP TS 33.401 v16.2.0, *Technical Specification Group Services and System Aspects - 3GPP Generation System Architecture Evolution (SAE) - Security architecture*

3GPP TS 33.501 v16.2.0, *Technical Specification Group Services and System Aspects - Security architecture and procedures for 5G system*

Annex B
(informative)

Abbreviations

1G	First Generation
3GPP	3rd Generation Partnership Project
5G	Fifth Generation
ACL	Access Control List
ACML	Access Control Markup Language
AES	Advanced Encryption Standard
AKA	Authentication Key Agreement
AMF	Access and Mobility Management Function
AN	Access Network
API	Applications Programming Interface
AS	Access Stratum
ASN.1	Abstract Syntax Notation One
ASP	Applications Service Provider
AUSF	Authentication Server Function
BER	Basic Encoding Rule
CAP	Common Alerting Protocol
CCTV	Closed-Circuit Television
CN	Core Network
CU-CP	Central Unit Control Plane
CVL	Certificate Revocation Lists
CYBEX	Cybersecurity Information Exchange
DDoS	Distributed Denial of Service
DNS	Domain Naming System
DoS	Denial-of-Service
E2E	End-to-End
EAP-AKA	Extensible Authentication Protocol-Authentication Key Agreement
eMBB	enhanced Mobile Broadband
eSIM	embedded Serving Identity Module
eUICC	embedded Universal Integrated Circuit Card
FCAPS	Fault, Capacity, Administration, Provisioning, and Security
FIB	Focused Ion Beam
FidAM	Federated Identity and Access Management Models
gNB	gNodeB

GSMA	Global System for Mobile Communications Association
HE	Home Environment
IAM	Identity Access Management
IMSI	International Mobile Subscriber Identity
IMT-2020	International Mobile Telecommunications-2020
IoT	Internet of Things
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning Systems
IPDRR	Identify, Protect, Detect, Response and Recover
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
M2M	Machine-to-Machine
MACSec	Media Access Control Security
MANO	Management and Network Orchestration
ME	Mobile Equipment
MEC	Mobile Edge Computing
MitM	Man-in-the-Middle
mMTC	massive Machine Type Communication
MNSP	Mobile Network Service Provider
MTC	Machine Type Communication
NB-IoT	Narrowband Internet of Things
NE	Network Element
NEF	Network Exposure Function
NFV	Network Functions Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NG-UE	Next Generation - User Equipment
NIST	National Institute of Standards and Technology
NR RAN	New Radio RAN
NRF	Network Repository Function
NSP	Network Service Provider
O&M	Operations and Maintenance
OAM&P	Operations, Administration, Maintenance and Provisioning
PER	Packet Encoding Rule
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
P-TMSI	Packet domain Temporary Mobile Subscriber Identity
QoS	Quality of Service

RAN	Radio Access Network
RBAC	Role-Based Access Control
RRC	Radio Resource Control
SA	Stand Alone
SAML	Security Assertion Markup Language
SAS	Security Accreditation Scheme
SAS-SM	Security Accreditation Scheme for Subscription Management
SAS-UP	Security Accreditation Scheme for UICC Production
SBA	Service Based Architecture
SDN	Software Defined Networking
SEPP	Security Edge Protection Proxy
SIDF	Security Identifier Deconcealment Function
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SN	Serving Network
SOP	Standard Operating Procedures
SsaaS	Slicing security as a Service
SSO	Single Sign On
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDM	Unified Data Management
UE	User Equipment
UICC	Universal Integrated Circuit Card
UPF	User Plane Function
URLLC	Ultra Reliable Low Latency Communication
USIM	Universal Serving Identity Module
V2X	Vehicle-to-Everything
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
VPN	Virtual Private Network
VXLAN	Virtual Extensible Local Area Network
XACML	eXtensible Access Control Markup Language
XER	XML Encoding Rules
XML	eXtensible Markup Language
ZTA	Zero-Trust Architecture

Annex C
(normative)

Security standards per security area

Table C.1. Security standards per 11 key security areas

No	Key security area	ITU standards	Descriptions
1.	Public Key Infrastructure (PKI)	ITU-T X.509, *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*	a) Provides a security framework for both PKI and Privilege Management Infrastructure (PMI). b) Used for services such as authentication, encryption and confidentiality, digital signatures, nonrepudiation, and authorisation. c) Applicable to any vendors providing security solutions, profiling and products that are based on PKI and PMI. d) Defines the framework for both PKI and PMI, which includes infrastructure models, certificate and Certificate Revocation Lists (CVL) syntax definitions, directory schema object definitions and certificate path processing procedures.
2.	Cybersecurity overview	ITU-T X.1205, *Overview of cybersecurity*	a) Applicable to any party involved in providing security solutions, profiling and products for various organisations. b) Provides insight on various cybersecurity threats from an organisational point of view across various network layers, along with threat countermeasures, network protection principles and risk management strategies and techniques.
3.	Security architecture for systems providing E2E communications	ITU-T X.805 NOTE: Further details, please refer Clause 8.	a) Required for any party that is performing comprehensive network security assessment and planning. b) Addresses complex security problems in Next Generation Networks with their division into layers and planes and elements and the need to have at hand a holistic security methodology to systematically engineer security for such systems. c) Provides a comprehensive, multi-layered, E2E network security framework across 8 security dimensions in order to combat network security threats and to achieve E2E security.
4.	Security Assertion Makeup Language (SAML)	ITU-T X.1141, *Security Assertion Markup Language (SAML 2.0)*	a) Extensible Markup Language (XML) based framework used to facilitate the exchange of security information among different organisations with different security domain. b) Ensure a secured exchange of authentication and authorisation information. c) Enables Single Sign On (SSO) capabilities, where organisations can share information about user identities and access privileges in a safe, secure and standardised manner.

Table C.1. Security standards per 11 key security areas *(continued)*

No	Key security area	ITU standards	Descriptions
5.	Entity authentication assurance framework	ITU-T X.1254, *Entity authentication assurance framework*	a) Affects organisations that are provides security-based products, profiling application and security solutions that requires authentication. b) 4 levels of entity authentication assurance are defined along with the criteria and threats for each of the four levels. c) Provides guidance concerning control technologies to be used to mitigate the threats. d) Provides guidance for mapping the 4 levels of assurance to other authentication assurance schemas and for exchanging the results of authentication based on the four levels of assurance.
6.	Common Alerting Protocol (CAP)	ITU-T X.1303, *Common alerting protocol (CAP 1.1)*	a) Affects Integrated Public Alert and Warning Systems (IPAWS), as they are based on CAP. b) Exchange all-hazard emergency alerts and public warnings over all kinds of networks. c) Allows a consistent warning message to be disseminated simultaneously over many different warning systems. d) Increase warning effectiveness while simplifying the alerting task.
7.	Access Control Markup language (ACML)	ITU-T X.1142, *eXtensible Access Control Markup Language (XACML 2.0)*	a) Covers the eXtensible Access Control Markup Language (XACML). b) XACML defines an attribute-based access control policy language, architecture and a processing model. c) Describes how access requests are evaluated according to some rules defined in an enterprise policy. d) Plays important role within an organisation to provide real time RBAC to protect access to all types of resources within any organisation.
		ITU-T X.1144, *eXtensible Access Control Markup Language (XACML) 3.0*	

8.	Information security management guidelines for telecommunications organisations based on ISO/IEC 27002	ITU-T X.1051, *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*	a) General principles for initiating, implementing, maintaining and improving information security management in telecommunications organisations.
			b) Provides an implementation baseline for information security management to help ensure the confidentiality, integrity and availability of telecommunications facilities and services.
			c) Covers several areas in the telecommunication sector such as:
			i) information security policies;
			ii) organisation of information security;
			iii) asset management;
			iv) access control;
			v) cryptography;
			vi) physical and environmental security;
			vii) operations security;
			viii) communications security;
			ix) systems acquisition, development and maintenance;

Table C.1. Security standards per 11 key security areas *(continued)*

No	Key security area	ITU standards	Descriptions
8.	Information security management guidelines for telecommunications organisations based on ISO/IEC 27002	ITU-T X.1051, *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*	x) supplier relationships; xi) information security incident management; xii) information security aspects of business continuity management; and xiii) compliance. d) Addresses several security concerns such as protection of information from unauthorised disclosure, controlled installation and use of telecommunication facilities and provision of authorise access to telecommunication facilities when necessary.
9.	Interactive gateway system for countering spam	ITU-T X.1243, *Interactive gateway system for countering spam*	a) Enables spam notification among different domains and prevents spam traffic from passing from one domain to another. b) Specifies the architecture for the gateway system and describes basic entities, protocols and functions of the system. c) Specifies mechanisms for spam detection, information sharing and specific actions for countering spam.
10.	Abstract Syntax Notation One (ASN.1)	ASN.1 specific recommendation: ITU-T X.680 - X.683 and ISO/IEC 8824, *Information technology - Abstract Syntax Notation One (ASN.1)* Basic encoding rules (BER), packed encoding Rules (PER), and XML encoding rules (XER) recommendations: ITU-T X.690 - X.695 and ISO/IEC 8825, *Information technology - ASN.1 encoding rules*	a) Used for a wide range of other applications, such as network management, secure email, cellular telephony, air traffic control, and voice and video over the Internet. b) Covers various aspects such as the definition of data types and values, BER and PER. c) Applies to various data types under the ASN.1 notation and rules for encoding ASN.1 data value using XML.

Table C.1. Security standards per 11 key security areas*(concluded)*

No	Key security area	ITU standards	Descriptions
11.	Cybersecurity Information Exchange (CYBEX) framework	ITU-T X.1500, *Overview of cybersecurity information exchange*	a) Consists of a basic exchange framework with the following extensible functions which are as follows: i) structuring cybersecurity information for exchange purposes; ii) identifying and discovering cybersecurity information and entities; iii) requesting and responding with cybersecurity information; iv) exchanging cybersecurity information; and v) enabling assured cybersecurity information exchange. b) Creates a common global means for cybersecurity entities to exchange cybersecurity information. c) Allows cybersecurity information to be exchanged between various organisations for enhanced cybersecurity and infrastructure protection, as well as accomplishing the principal functions performed by cyber security teams.
		ITU-T X.1520, *Common vulnerabilities and exposures*	
		ITU-T X.1521, *Common vulnerability scoring system*	
		ITU-T X.1524, *Common weakness enumeration*	
		ITU-T X.1525, *Common weakness scoring system*	
		ITU-T X.1526, *Language for the open definition of vulnerabilities and for the assessment of a system state*	
		ITU-T X.1528, *Common platform enumeration*	
		ITU-T X.1546, *Malware attribute enumeration and characterization*	

Annex D
(normative)

End-to-End (E2E) threat and mitigation control

Table D.1. E2E threat and mitigation control for end user category

Elements		Security control	Security threats
Physical	Secured hardware	SAS of UICC or embedded Serving Identity Module (eSIM)	Device tampering
Technical	a) Subscriber device identifiers and credentials b) Authentication/AKA c) Security negotiation, key hierarchy	a) Trust model between telco network, vertical service network and user b) Hybrid authentication management with either/ both network service provider and service provider c) EAP-AKA and 5G-AKA authentication for attach procedure	a) Malware b) Trivial File Transfer Protocol (TFTP) Man-in-the-Middle (MitM) attacks c) Bots DDoS d) Firmware hacks e) User identity theft
Administration	Enhanced subscriber privacy	Concealment of subscriber identity via SUCI	Privacy breach

Table D.2. E2E threat and mitigation control for NR RAN category

Elements		Security control	Security threats
Physical	Secured hardware	Implementation of physical security measures at RAN site (security fence, Closed-Circuit Television (CCTV), physical locks, etc.)	a) Device tampering b) Damage to RAN NEs
Technical	a) Cryptographic algorithms b) Air interface jamming protection c) Fronthaul and backhaul security	a) Detection mechanism for DDoS attacks (e.g. threshold-based detection of RRC requests) b) Quantum key distribution for signalling encryption c) Anti-jamming mobile offloading mechanisms d) Search Results e) Featured snippet from the web f) IPSec tunnel security for transport links	a) MitM attack b) Jamming c) International Mobile Subscriber Identity (IMSI) catching d) Flooding attacks e) Rogue nodes f) Signalling fraud g) Signalling storm
Administration	Secured user access	User access control	a) Unauthorised access b) Data/ information exfiltration

Table D.3. E2E threat and mitigation control for edge network category

Elements		Security control	Security threats
Physical	Secured hardware	Implementation of physical security measures for MEC elements (anti-theft, anti-damage, access control etc)	a) Device tampering b) Damage to MEC elements
Technical	a) NFV/Software Defined Networking (SDN) security b) Network slicing security c) MEC security d) Cloud security e) Fronthaul and backhaul security	a) Resource isolation and multi-layer isolation (zoning isolation) b) Security isolation mechanism and policy c) Software defined segmentation d) Encryption of sensitive security assets e) IPSec tunnel security for transport links f) Authentication and transport protection between functions using TLS	a) DDoS and DoS attacks b) CP/UP sniffing c) MEC backhaul sniff d) MEC server vulnerability e) Slice/resource theft f) Rogue MEC gateway g) API vulnerability exploit h) Side channel attack i) Roaming partner vulnerabilities j) Signalling fraud
Administration	Secured user access	User access control	a) Improper access control b) Data/ information exfiltration

Table D.4. E2E threat and mitigation control for CN category

Elements		Security control	Security threats
Physical	Secured hardware	Implementation of physical security measures for core elements (anti-theft, anti-damage, access control etc)	a) Device tampering b) Damage to core elements
Technical	a) NFV/SDN security b) Network slicing security c) Cloud security d) SBA security e) Fronthaul and backhaul security f) Inter-networking security g) Network capability exposure security	a) Resource isolation and multi-layer isolation (zoning isolation) b) Security isolation mechanism and policy c) Software defined segmentation d) Authentication framework for SBA using OAuth 2.0 e) Authentication and transport protection between functions using TLS f) Usage of SEPP for interconnection security g) Securing east-west traffic	a) DDoS & DoS attacks b) CP/UP sniffing c) Slice/resource theft d) API vulnerability exploit e) Side channel attack f) Roaming partner vulnerabilities g) Signalling fraud
Administration	Secured user access	User access control	c) Improper access control d) Data/ information exfiltration

Table D.5. E2E threat and mitigation control for applications/services category

Elements		Security control	Security threats
Physical	Secured hardware	a) Implementation of physical security measures for NEs (anti-theft, anti-damage, access control etc) b) Physically secured IoT endpoints	a) Device tampering b) Damage to NEs
Technical	a) Vertical industries applications b) Narrowband Internet of Things (NB-IoT)	a) Securing third party application interfaces b) Enforcing cloud security policies c) Enforcing API security d) Root of trust for IoT endpoints	a) API vulnerabilities b) Application server vulnerabilities c) Application vulnerability exploits d) DDoS and DoS attacks e) Hacking of IoT endpoints
Administration	Secured user access	User access control	e) Improper access control f) Data/ information exfiltration

Table D.6. E2E threat and mitigation control for operations category

Elements		Security control	Security threats
Physical	Secured hardware	Implementation of physical security measures for NEs (anti-theft, anti-damage, access control etc)	a) Device tampering b) Damage to NEs
Technical	NIST's IPDRR framework	a) System security monitoring, auditing and traceability b) System integrity protection via secure boot	a) DDoS and DoS attacks b) MitM c) Hacking
Administration	a) Change management b) Business continuity c) Incident management d) Operation resiliency e) Secured user access	a) Privacy procedures for handling user data during network O&M routines b) Enforcement of security rules for O&M tasks c) Enforce in house / third party audit d) User access control	a) Privacy breach b) Improper access control c) Vulnerable network and systems d) Data/information exfiltration

Bibliography

[1] ITU-T X.696 | ISO/IEC 8825-7, *Information technology - Specification of Octet Encoding Rules (OER)*

[2] ITU-T X.1544, *Common attack pattern enumeration and classification*

[3] ITU-R M.2083-0*, IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond*

[4] ITU-T Technical Report XSTR-SUSS, *Successful use of security standards*

[5] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*

[6] ETSI TS 129 510 V15.6.0, *5G; 5G System; Network function repository services; Stage 3*

[7] ITU Workshop on 5G Security*, 5G Security Overview: Security for Programmable Cloud-Based Mobile Networks*

[8] ITU Workshop on Future Network 2030, *Quantum Safe Communication - Cybersecurity for 5G era*

[9] IEEE TrustCom-15, *Towards 5G Security, Günther Horn*

[10] IEEE, *Security for 5G Mobile Wireless Networks*

[11] IEEE, *Security in Mobile Edge Caching with Reinforcement Learning*

[12] *5G Security: Forward Thinking Huawei White Paper*

[13] Huawei, *5G Security Architecture Whitepaper*

[14] Huawei, *The Cybersecurity Framework and 5G RAN*

[15] Huawei White Paper, *Partnering with the Industry for 5G Security Assurance*

[16] ZTE, *5G Security White Paper Security Makes 5G Go Further, May 2019*

[17] WILEY, *5G System Design: Architectural and Functional Considerations and Long Term Research*

[18] CLP.13, *IoT Security Guidelines for Endpoint Ecoystems Version 2.2*

[19] Trend Micro, *Securing 5G Through Cyber-Telecom Identity Federation*

[20] 5G Americas White Paper, *The Evolution of Security in 5G - A “Slice” of Mobile Threats*

[21] Cloud Security Alliance, *Cloud Controls Matrix v3.0.1*

[22] *5G Network Architecture and Security: A collaborative paper DCMS Phase 1 5G Testbeds & Trials Programme*

[23] Ericsson, *Creating the next generation edge-cloud ecosystem*
https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/next-generation-cloud-edge-ecosystems?gclid=EAIaIQobChMI4L67gZDV6AIVj4WPCh2wsQnJEAAYASAAEgJJK_D_BwE&gclsrc=aw.ds

[24] Ericsson, *A guide to 5G network security*
https://www.ericsson.com/en/security/a-guide-to-5g-network-security

[25] Ericsson, *An overview of the 3GPP 5G security standard*
https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview

[26] Ericsson, *What next in the world of post-quantum cryptography?*
https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorithms

[27] GSMA, *Security Accreditation Scheme*
https://www.gsma.com/security/security-accreditation-scheme/

[28] NIS Cooperation Group, *EU coordinated risk assessment of the cybersecurity of 5G networks*

Acknowledgements

Members of the Application Security Sub Working Group

Mr Azlan Mohamed Ghazali (Chairman)	KPMG Management & Risk Consulting Sdn Bhd
Mr Mohd Fairuz Ismail (Vice Chairman)	KPMG Management & Risk Consulting Sdn Bhd
Ms Norkhadhra Nawawi/	Malaysian Technical Standards Forum Bhd
Mr Ahmad Syazilie Shamsuddin (Secretariat)	
Mr Irwan Kurnawan Amat Sapuan/	Celcom Axiata Berhad
Mr Sazali Musa/	
Mr Zef Zalmi Mohamed	
Mr Ahmad Dahari Jarno/	CyberSecurity Malaysia
Mr Farhan Arif Mohamad/	
Mr Muhammad Ashraff Ruzaidi/	
Ms Norahana Salimin/	
Mr Shahrin Baharom	
Mr Hanaffy Goeffery Ramli/	Digi Telecommunications Sdn Bhd
Mr Yuwanthiran Sukalingam	
Mr Mohd Edymainoe Mohd Noh/	Maxis Broadband Sdn Bhd
Mr Syahril Hafiz Abu Hassan/	
Mr Wong Chup Woh	
Mr Ahmad Fairuz Mohamed Noor/	National Cyber Security Agency
Ms Azleyna Ariffin/	
Ms Siti Hajar Roslan	
Mr Muhamad Hasyimi Shaharuddin/	Telekom Malaysia Berhad
Mr Shahril Azwar Abas/	
Mr Thaib Mustafa	