International Telecommunication Union

ITU-T Technical Paper

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(05/2022)

XSTP-5GsecRM
5G security standardization roadmap

Summary

This technical paper provides the standardization roadmap for fifth generation (5G; also known as International Mobile Telecommunications-2020) security. This roadmap is prepared to assist in developing 5G security standards by providing information on existing standards and those under development from key standards development organizations (SDOs). In addition, it describes the overviews of 5G security from standards perspective and gap analysis.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Keywords

5G security, 5G security standardization, roadmap.

Change log

This document contains Version 1.0 of the ITU-T Technical Paper on "5G security standardization roadmap" approved at the ITU-T Study Group 17 virtual meeting, 2022-05-10/20.

Table of Contents

Technical Paper ITU-T XSTP-5GsecRM

5G security standardization roadmap

1 Scope

This Technical Paper provides the standardization roadmap for fifth generation (5G) security. It addresses the following subjects:

– overview of 5G security from the perspective of standards development;

– 5G security-related activities in standards development organizations (SDOs);

– existing and approved, standards, and those under-development;

– 5G security-related documents published by fora, associations, research institutes and governments;

– gap analysis on 5G security standardization;

– direction of 5G-related security standardization works in ITU-T.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Technical Paper

None.

4 Abbreviations and acronyms

This Technical Paper uses the following abbreviations and acronyms:

4G	fourth Generation
5G	fifth Generation
5GC	fifth Generation Core
5GS	fifth Generation System
AKMA	Authentication and Key Management for Applications
AMF	Access and Mobility Management Function
API	Application Programming Interface
ARPF	Authentication Credential Repository Processing Function
AUSF	Authentication Server Function
CIoT	Cellular Internet of Things
E2E	End to End
EECC	European Electronic Communications Code
eNA	enablers for Network Automation

ENISA	European Network and Information Security Agency
EGPRS	Enhanced General Packet Radio Service
FMC	Fixed Mobile Converged
GSMA	GSM Association
GTP-U	General packet radio service Tunnelling Protocol for User
IAB	Integrated Access and Backhaul
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
LAN	Local Area Network
LI	Lawful Interception
LTE	Long-Term Evolution
MANO	Management and Network Orchestration
MBS	Multicast-Broadcast Services
MEC	Multi-access Edge Computing
MNO	Mobile Network Operator
MSGin5G	Message Service for MIoT over 5G
MTC	Machine Type Communication
N3IWF	Non-3GPP Interworking Function
NEF	Network Exposure Function
NESAS	Network Equipment Security Assurance Scheme
NFV	Network Function Virtualization
NGMN	Next Generation for Mobile Network
NIST	National Institute of Standards and Technology
NPN	Non-Public Network
NR	Next Radio
NRF	Network Repository Function
NSWO	Non-Seamless WLAN Offload
NWDAF	Network Data Analytics Function
PKI	Public Key Infrastructure
SBA	Service-Based Architecture
SCAS	Security Assurance Specification
SCP	Service Communication Proxy
SDN	Software-Defined Networking
SDO	Standards Development Organization
SECAM	Security Assurance Methodology
SEPP	Security Edge Protection Proxy

SIM	Subscriber Identification Module
SIP	Session Initiation Protocol
SMF	Session Management Function
SS7	Signalling System No. 7
UAS	Unmanned Aerial System
UDM	Unified Data Management
UP	User Plane
UPF	User Plane Function
URLLC	Ultra-Reliable and Low Latency Communication
UTRAN	Universal Terrestrial Radio Access Network
V2X	Vehicle to Everything
VNF	Virtualized Network Function
WLAN	Wireless Local Area Network
ZSM	Zero-touch Network and Service Management

5 Overview of 5G security standardization roadmap

Because the 5G network has changed from the fourth generation/long-term evolution (4G/LTE) era by including new functions, new technologies and new platform architecture, new threats and risks should be considered. Because 5G networks have become complicated and include many aspects, their security has been discussed by many SDOs, fora or associations and governments. The purpose of this Technical Paper is to recognize 5G security activities at the corresponding SDOs and other organizations, and to identify how security standardization work relates to 5G in ITU-T SG17.

6 Developing standards for 5G security in standards development organizations

6.1 ITU-T SG17

6.1.1 Published documents as Recommendation, Supplement and Technical Report

Table 6-1 lists the ITU-T Recommendations, Supplements and Technical Reports related to 5G security in ITU-T SG17.

Table 6-1 – ITU-T SG17 Recommendations, Supplements and Technical Reports

Study group	Number	Title	Date
SG17	ITU-T X.1038	*Security requirements and reference architecture for software-defined networking*	10/2016
SG17	ITU-T X.1042	*Security services using software-defined networking*	01/2019
SG17	ITU-T X.1043	*Security framework and requirements for service function chaining based on software-defined networking*	03/2019
SG17	ITU-T X.1044	*Security requirements of network virtualization*	10/2019
SG17	ITU-T X.1045	*Security service chain architecture for networks and applications*	10/2019

Table 6-1 – ITU-T SG17 Recommendations, Supplements and Technical Reports

Study group	Number	Title	Date
SG17	ITU-T X.1046	*Framework of software-defined security in software-defined networks/network functions virtualization networks*	12/2020
SG17	ITU-T X.1047	*Security requirements and architecture for network slice management and orchestration*	10/2021
SG17	ITU-T X.1811	*Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*	04/2021
SG17	ITU-T X.1812	*Security framework based on trust relationship for the IMT-2020 ecosystems*	05/2022
SG17	ITU-T X.1813	*Security requirements for the operation of vertical services supporting ultra-reliable and low latency communication (URLLC) in the IMT-2020 private networks*	
SG17	ITU-T X.1814	*Security guidelines for IMT-2020 communication system*	

6.1.2 Work items

Table 6-2 lists the on-going work items related to 5G security in ITU-T SG17.

Table 6-2 – Status of work items in ITU-T SG17

Q	Acronym	Title	Start of work	Timing of approval
2/17	X.5Gsec-ecs*	Security framework for 5G edge computing services	2019-01	2022-09
2/17	X.5Gsec-netec*	Security capabilities of network layer for 5G edge computing	2019-09	2022-09
2/17	X.5Gsec-ssl	Guidelines for classifying security capabilities in 5G network slice	2020-09	2022-09
2/17	X.5Gsec-message	Security requirements for 5G message service	2021-04	2023-03
13/17	X.itssec-5*	Security guidelines for vehicular edge computing	2019-09	2023-09

6.2 Other study groups in ITU-T

None.

6.3 3rd Generation Partnership Project

Table 6-3 lists the standardization items related to 5G security from the 3rd Generation Partnership Project (3GPP).

Table 6-3 – Security related documents in the 3rd Generation Partnership Project

Group	3GPP number	Title
TSG SA3	TS 33.122	*Security aspects of common API framework (CAPIF) for 3GPP northbound APIs*
TSG SA3	TS 33.126	*Security; Lawful interception requirements*
TSG SA3	TS 33.127	*Security; Lawful interception (LI) architecture and functions*
TSG SA3	TS 33.128	*Security; Protocol and procedures for lawful interception (LI); Stage 3*
TSG SA3	TS 33.501	*Security architecture and procedures for 5G system*
TSG SA3	TS 33.503	*Security aspects of proximity based services (ProSe) in the 5G system (5GS)*
TSG SA3	TS 33.511	*Security assurance specification (SCAS) for the next generation node B (gNodeB) network product class*
TSG SA3	TS 33.512	*5G security assurance specification (SCAS); Access and mobility management function (AMF)*
TSG SA3	TS 33.513	*5G security assurance specification (SCAS); User plane function (UPF)*
TSG SA3	TS 33.514	*5G security assurance specification (SCAS) for the unified data management (UDM) network product class*
TSG SA3	TS 33.515	*5G security assurance specification (SCAS) for the session management function (SMF) network product class*
TSG SA3	TS 33.516	*5G security assurance specification (SCAS) for the authentication server function (AUSF) network product class*
TSG SA3	TS 33.517	*5G security assurance specification (SCAS) for the security edge protection proxy (SEPP) network product class*
TSG SA3	TS 33.518	*5G security assurance specification (SCAS) for the network repository function (NRF) network product class*
TSG SA3	TS 33.519	*5G security assurance specification (SCAS) for the network exposure function (NEF) network product class*
TSG SA3	TS 33.520	*Security assurance specification for non-3GPP interworking function (N3IWF)*
TSG SA3	TS 33.521	*5G security assurance specification (SCAS); Network data analytics function (NWDAF)*
TSG SA3	TS 33.522	*5G security assurance specification (SCAS); Service communication proxy (SCP)*
TSG SA3	TS 33.535	*Authentication and key management for applications (AKMA) based on 3GPP credentials in the 5G system (5GS)*
TSG SA3	TS 33.536	*Security aspects of 3GPP support for advanced vehicle-to-everything (V2X) services*
TSG SA3	TR 33.738	*Study on security aspects of enablers for network automation for 5G –Phase 3*
TSG SA3	TR 33.739	*Study on security enhancement of support for edge computing – Phase 2*
TSG SA3	TR 33.740	*Study on security aspects of proximity based services (ProSe) in 5G system (5GS) phase 2*
TSG SA3	TR 33.805	*Study on security assurance methodology for 3GPP network products*
TSG SA3	TR 33.807	*Study on the security of the wireless and wireline convergence for the 5G system architecture*
TSG SA3	TR 33.808	*Study on KDF negotiation for 5G system security*
TSG SA3	TR 33.809	*Study on 5G security enhancement against false base stations (FBS)*

Table 6-3 – Security related documents in the 3rd Generation Partnership Project

Group	3GPP number	Title
TSG SA3	TR 33.811	*Study on security aspects of 5G network slicing management*
TSG SA3	TR 33.813	*Security aspects; Study on security aspects of network slicing enhancement*
TSG SA3	TR 33.814	*Study on the security of the enhancement to the 5G Core (5GC) location services*
TSG SA3	TR 33.818	*Security assurance methodology (SECAM) and security assurance specification (SCAS) for 3GPP virtualised network products*
TSG SA3	TR 33.819	*Study on security enhancements of 5G System (5GS) for vertical and local area network (LAN) services*
TSG SA3	TR 33.824	*Study on security for next radio (NR) integrated access and backhaul (IAB)*
TSG SA3	TR 33.825	*Study on the security of ultra-reliable low-latency communication (URLLC) for the 5G system (5GS)*
TSG SA3	TR 33.835	*Study on authentication and key management for applications based on 3GPP credential in 5G*
TSG SA3	TR 33.836	*Study on security aspects of 3GPP support for advanced vehicle-to-everything (V2X) services*
TSG SA3	TR 33.839	*Study on security aspects of enhancement of support for edge computing in the 5G core (5GC)*
TSG SA3	TR 33.840	*Study on security aspects of the disaggregated gNB architecture*
TSG SA3	TR 33.841	*Security aspects; Study on the support of 256-bit algorithms for 5G*
TSG SA3	TR 33.842	*Study on lawful interception (LI) service in 5G*
TSG SA3	TR 33.845	*Study on storage and transport of 5G core (5GC) security parameters for authentication credential repository processing function (ARPF) authentication*
TSG SA3	TR 33.846	*Study on authentication enhancements in the 5G system (5GS)*
TSG SA3	TR 33.847	*Study on security aspects of enhancement for proximity based services in the 5G system (5GS)*
TSG SA3	TR 33.848	*Security aspects; Study on security impacts of virtualisation*
TSG SA3	TR 33.849	*Study on subscriber privacy impact in 3GPP*
TSG SA3	TR 33.850	*Study on security aspects of enhancements for 5G multicast-broadcast services (MBS)*
TSG SA3	TR 33.851	*Study on security for enhanced support of industrial Internet of things (IIoT)*
TSG SA3	TR 33.853	*Study on key issues and potential solutions for integrity protection of the user plane (UP)*
TSG SA3	TR 33.854	*Study on security aspects of unmanned aerial systems (UAS)*
TSG SA3	TR 33.855	*Security aspects; Study on security aspects of the 5G service based architecture (SBA)*
TSG SA3	TR 33.856	*Study on security aspects of single radio voice continuity from 5G to UTRAN*
TSG SA3	TR 33.857	*Study on enhanced security support for non-public networks (NPN)*
TSG SA3	TR 33.859	*Study on the introduction of key hierarchy in universal terrestrial radio access network (UTRAN)*
TSG SA3	TR 33.860	*Study on enhanced general packet radio service (EGPRS) access security enhancements with relation to cellular Internet of things (IoT)*

Table 6-3 – Security related documents in the 3rd Generation Partnership Project

Group	3GPP number	Title
TSG SA3	TR 33.861	*Study on evolution of cellular internet of things (CIoT) security for the 5G system*
TSG SA3	TR 33.862	*Study on security aspects of the message service for MIoT over the 5G system (MSGin5G)*
TSG SA3	TR 33.863	*Study on battery efficient security for very low throughput machine type communication (MTC) devices*
TSG SA3	TR 33.865	*Security aspects of WLAN network selection for 3GPP terminals*
TSG SA3	TR 33.866	*Study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2*
TSG SA3	TR 33.868	*Study on security aspects of machine-type communications (MTC) and other mobile data applications communications enhancements*
TSG SA3	TR 33.875	*Study on enhanced security aspects of the 5G service based architecture (SBA)*
TSG SA3	TR 33.876	*Study on automated certificate management in SBA*
TSG SA3	TR 33.881	*Study on non-seamless WLAN offload (NSWO) in 5G system (5GS) using 3GPP credentials*
TSG SA3	TR 33.889	*Study on security aspects of machine-type communications (MTC) architecture and feature enhancements*

6.4 European Telecommunications Standards Institute

Table 6-4 lists standardization items related to 5G security from the European Telecommunications Standards Institute (ETSI).

Table 6-4 – Security related documents from the European Telecommunications Standards Institute

Group	Number	Title
ISG MEC	GS MEC 030	*Multi-access edge computing (MEC); V2X information service API*
ISG MEC	GR MEC 031	*Multi-access edge computing (MEC) MEC 5G integration*
ISG NFV	GS NFV-SEC 001	*Network functions virtualisation (NFV); NFV security; Problem statement*
ISG NFV	GS NFV-SEC 002	*Network functions virtualisation (NFV); NFV security; Cataloguing security features in management software*
ISG NFV	GS NFV-SEC 003	*Network functions virtualisation (NFV); NFV security; Security and trust guidance*
ISG NFV	GS NFV-SEC 004	*Network functions virtualisation (NFV); NFV security; Privacy and regulation; Report on lawful interception implications*
ISG NFV	GR NFV-SEC 005	*Network functions virtualisation (NFV); Trust; Report on certificate management*
ISG NFV	GS NFV-SEC 006	*Network functions virtualisation (NFV); Security guide; Report on security aspects and regulatory concerns*
ISG NFV	GR NFV-EVE 007	*Network functions virtualisation (NFV); Trust; Report on attestation technologies and practices for secure deployments*
ISG NFV	GS NFV-SEC 009	*Network functions virtualisation (NFV); NFV security; Report on use cases and technical approaches for multi-layer host administration*

Table 6-4 – Security related documents from the European Telecommunications Standards Institute

Group	Number	Title
ISG NFV	GS NFV-SEC 010	*Network functions virtualisation (NFV); NFV security; Report on retained data problem statement and requirements*
ISG NFV	GR NFV-SEC 011	*Network functions virtualisation (NFV); Security; Report on NFV LI architecture*
ISG NFV	GS NFV-SEC 012	*Network functions virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components*
ISG NFV	GS NFV-SEC 013	*Network functions virtualisation (NFV) Release 3; Security; Security management and monitoring specification*
ISG NFV	GS NFV-SEC 014	*Network functions virtualisation (NFV) Release 3; NFV security; Security specification for MANO components and reference points*
ISG NFV	GR NFV-EVE 018	*Network functions virtualisation (NFV); Security; Report on NFV remote attestation architecture*
ISG NFV	GS NFV-SEC 021	*Network functions virtualisation (NFV) release 2; Security; VNF package security specification*
ISG NFV	GS NFV-SEC 022 (Early draft)	*Network functions virtualisation (NFV) Release 3; Security; Access token specification for API access*
ISG NFV	GS NFV-SEC 023 (Early draft)	*Network functions virtualisation (NFV) Release 4; Security; container security specification*
ISG ZSM	GR ZSM 010	*Zero-touch network and service management (ZSM); General security aspects*

6.5 Institute of Electrical and Electronics Engineers

Table 6-5 lists standardization items related to 5G security from the Institute of Electrical and Electronics Engineers (IEEE).

Table 6-5 – Security related documents from the Institute of Electrical and Electronics Engineers

Group	Number	Title
	IEEE P1912	*Standard for privacy and security architecture for consumer wireless devices*

7 Documents and reports related to 5G security

This clause contains the list of 5G security related documents including guideline, threat analysis, etc.

7.1 Next Generation for Mobile Network

Table 7-1 lists documents related to 5G security published by the Next Generation for Mobile Network (NGMN).

Table 7-1 – 5G Security related documents from the Next Generation for Mobile Network

Title	Abbrev.	Outline	Publication date
5G security recommendations – Package #1	NGMN Pac1	This package focuses on improving the access network and identifies denial of service attack scenarios in a 5G context.	May 2016
5G security recommendations – Package #2: Network Slicing	NGMN Pac2	This document focuses on security threats or flaws that could emerge through network slicing use in 5G.	April 2016
5G security – Package 3: Mobile edge computing/low latency/consistent user experience, V2.0	NGMN Pac3	This document focuses on mobile edge computing, low latency and consistent user experience. Mobile edge computing (which is part of the slightly broader concept of MEC) and low latency allow new types of services. The NGMN 5G SEC group studied the security threats, frauds and vulnerabilities that such concepts could introduce in 5G and provide security recommendations to mitigate them.	February 2018
Security aspects of network capabilities exposure in 5G	NGMN NCE	The scope of this document is: to identify different network capabilities exposure scenarios; to investigate and propose security requirements for these scenarios; to investigate the exposure of security capabilities and present and evaluate the corresponding use cases.	September 2018
5G end-to-end architecture framework, V4.31	NGMN E2E	This document delineates the requirements in terms of entities and functions that characterize the capabilities of an end-to-end (E2E) framework.	November 2020
Security considerations for 5G network operation	NGMN NO	The scope of this document is to analyse new challenges as well as common security issues for 5G network operation, and to investigate security requirements and guidelines in a technical or non-technical way for 5G network operation	August 2021
Sustainable trust	NGMN Trust	The sustainable trust model provides a runtime evaluation of trustworthiness to all network functions and stakeholders via standard interactions. It is also complementary to all SDO trust models.	July 2021

7.2 GSM Association

Table 7-2 lists the documents related to 5G security published by the GSM Association (GSMA).

Table 7-2 – 5G security-related documents published by the GSM Association

No.	Title	Outline	Publication date
FS.13	*Network equipment security assurance scheme – Overview*, V2.1	The network equipment security assurance scheme (NESAS), jointly established by 3GPP and GSMA, provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry. NESAS specifies security requirements and an assessment framework for secure product development and product lifecycle processes, as well as using 3GPP-	January 2022
FS.14	*Network equipment security assurance scheme – Security test laboratory accreditation*, V2.1		January 2022
FS.15	*Network equipment security assurance scheme –*		January 2022

Table 7-2 – 5G security-related documents published by the GSM Association

No.	Title	Outline	Publication date
	Development and lifecycle assessment methodology, V2.1	established security test cases for the security evaluation of network equipment.	
FS.16	*Network equipment security assurance scheme – Development and lifecycle security requirements*, V2.1		January 2022
FS.21	*Interconnect signalling security recommendations*	Describes interconnect security vulnerabilities and suggests mobile network operator (MNO) responses, including implementation recommendations fora security edge protection proxy (SEPP)	May 2022
FS.33	*Network function virtualisation threats analysis*	Describes a range of security threats to NFV, a key 5G enabling technology and provides guidance on mitigation measures.	March 2020
FS.34	*Key management for 4G and 5G inter-PMN security*, V4.0	Describes the exchange of certificates and key materials that are used between interconnect parties to secure 4G and 5G roaming.	May 2022
FS.35	*Security algorithm implementation roadmap*, V1.0	Provides guidance and recommendations on the best algorithm deployment options, including for 5G privacy and integrity and subscription permanent identifier encryption.	March 2020
FS.36	*5G interconnect security*	Outlines potential 5G interconnect attacks against mobile networks and their customers and related countermeasures.	May 2022
FS.37	*GTP-U security*	Provides recommendations for MNOs to detect and prevent attacks using general packet radio service tunnelling protocol for user (GTP-U) plane data and how to deploy security capabilities, including those for the N3 and N9 interfaces in 5G.	June 2021
FS.38	*SIP network security*	Outlines potential security and fraud attacks based on the session initiation protocol (SIP) against mobile and fixed mobile converged (FMC) networks and their customers as well as describing countermeasures for those attacks.	April 2021
FS.39	5G fraud risks guide	Describes potential attacks against 5G networks and the services they support and recommends countermeasures to mitigate the risks posed to network operators and their customers.	June 2021
FS.40	5G security guide	Contains an overview of the security aspects and capabilities of 5G networks and serves as an educational resource that describes the security enhancements and capabilities inherent in 5G technology.	October 202i
IR.77	*Inter-operator IP backbone security req. for service and inter-operator IP backbone providers*, V5.0	Describes common guidelines to achieve an adequate security level on the IPX Network.	October 2019

Table 7-2 – 5G security-related documents published by the GSM Association

No.	Title	Outline	Publication date
NG.113	*5GS roaming guidelines*, V5.0	Provides guidelines for engineers and operational roaming teams on 5G roaming aspects.	December 2021
NG.116	*Generic network slice template*, V6.0	Provides a standardized list of attributes, including security aspects, that can characterize a type of network slice	November 2021

7.3 European Network and Information Security Agency

Table 7-3 lists the documents related to 5G security published by the European Network and Information Security Agency (ENISA).

Table 7-3 – 5G Security related documents from the European Network and Information Security Agency

Title	Abbrev.	Outline	Publication date
Threat landscape and good practice guide for software defined networks/5G	ENISA SDN	This report contributes to the definition of a threat landscape, which is an overview of current and emerging threats applicable to the software-defined networking/fifth generation (SDN/5G) technologies and their associated trends. Since 5G is a general term that integrates various networking technologies with different technological maturity, this study focuses on backbone network operation technologies, i.e., SDN. Around these core technologies, other integral components of 5G, including radio access and NFV are also discussed. This discussion, however, takes place within the scope of the relation of these other 5G components to SDN.	December 2015
Security aspects of virtualization	ENISA Virtual	This report provides an overview of the status of security of virtualized environments. It gives the basis to understand issues and challenges related to virtualization security, as well as a discussion on common best practices for security protection in virtualized environments and gaps that need to be filled to implement a secure virtualized environment.	February 2017
Signalling security in telecom SS7/diameter/5G – EU level assessment of the current situation	ENISA Signal	This document provides a good understanding of the status in the EU of security interconnect signalling and the overall risk level, current measures in place and future actions to be taken. Providing technical solutions that can solve problems is not the objective of this document. Nevertheless, taking into account the technical aspects of the topic, in some cases technical details are provided to validate the findings.	March 2018
ENISA threat landscape for 5G networks – Threat assessment for the	ENISA Threat1	This report provides a basis for future threat and risk assessments, focusing on particular use cases or specific components of the 5G infrastructure,	November 2019

Table 7-3 – 5G Security related documents from the European Network and Information Security Agency

Title	Abbrev.	Outline	Publication date
fifth generation of mobile telecommunications networks (5G)		which may be conducted on demand by all kinds of 5G stakeholders.	
ENISA threat landscape for 5G networks – Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)	ENISA Threat2	This report is a major update of the first edition of 2019. It encompasses all novelties introduced, it captures developments in the 5G architecture and it summarizes information found in standardisation documents.	December 2020
5G supplement to the guideline on security measures under the EECC, 2nd edition	ENISA EECC	This document contains a 5G technology profile that supplements the guideline on security measures under the European electronic communications code (EECC). The 5G technology profile gives additional guidance to competent national authorities about how to ensure the security of 5G networks. This document was developed in close collaboration with experts from national telecommunication security authorities across the EU, i.e., the European Competent Authorities for Secure Electronic Communications expert group (formerly known as the article 13a expert group), and with the members of the NIS CG work stream for 5G cybersecurity.	July 2021
Security in 5G specifications – Controls in 3GPP security specifications (5G SA)	ENISA 3GPP	This report aims to help EU member states implementing the technical measure TM02 from the EU toolbox on 5G security. The report also intends to help national competent and regulatory authorities get a better picture of the standardization environment pertaining to 5G security and to improve understanding of 3GPP security specifications, as well as its main elements and security controls. With this, competent authorities will be in a better position to understand what the key security controls that operators have to implement are and what the role of such controls is for achieving the overall security of 5G networks.	February 2021
ENISA threat landscape for supply chain attacks	ENISA Supply	This report aims to map and study the supply chain attacks that were discovered from January 2020 to early July 2021.	July 2021
NFV security in 5G – Challenges and best practices	ENISA NFV	This report explores relevant challenges, vulnerabilities and attacks to NFV within the 5G network. NFV changes the network security environment due to resource pools based on cloud computing and open network architecture. 60 Security challenges grouped in seven categories	February 2022

Table 7-3 – 5G Security related documents from the European Network and Information Security Agency

Title	Abbrev.	Outline	Publication date
		are identified and explored. Among others, this report exposes vulnerabilities, attack scenarios and their impact on 5G NFV assets. To address these upcoming challenges, security controls and best practices are put forward, taking into account the particularities of this highly complex, heterogeneous and volatile environment. In particular, 55 best practices categorized in technical, policy and organizational categories are identified.	
5G cybersecurity standards – Analysis of standardisation requirements in support of cybersecurity policy	ENISA Standards	This report outlines the contribution of standardization to the mitigation of technical risks, and therefore to trust and resilience, in the 5G ecosystem. This report focuses on standardization from a technical and organizational perspective.	March 2022

7.4 National Institute of Standards and Technology

Table 7-4 lists the documents related to 5G security published from the National Institute of Standards and Technology (NIST).

Table 7-4 – 5G Security related documents from the National Institute of Standards and Technology

Title	Abbrev.	Outline	Publication Date
5G cybersecurity – Preparing a secure evolution to 5G	NIST SE5G	The scope of this project is to leverage the 5G standardized security features that are defined in 3GPP standards to provide enhanced cybersecurity capabilities built into the network equipment and end-user devices. In addition, the project aims to identify security characteristics of the underlying technologies and components of the supporting infrastructure required to effectively operate a 5G network.	April 2020
NIST SP 1800-33A, *5G cybersecurity – Volume A: Executive summary* (preliminary draft)	NIST SP1800-33A	This project will demonstrate how operators and users of 5G networks can mitigate 5G cybersecurity risks. This is accomplished by strengthening the system's architectural components, providing a secure cloud-based supporting infrastructure, and enabling the security features introduced in the 5G standards. These measures support common use cases and meet industry sectors' recommended cybersecurity practices and compliance requirements.	February 2021
NIST SP 1800-33B, *5G cybersecurity – Volume B: Approach, architecture, and security characteristics*	NIST SP1800-33B		April 2022

8 Categorization of 5G security topics

This clause itemizes topics on 5G security by using information about standardization work and 5G security-related documents, and categorizes those topics into several groups to identify security issues for each topic.

8.1 5G core network

SBA, signalling, monitoring, network capability exposure, exposure security capabilities, JavaScript object notation/RESTful interface, etc.

8.2 Radio access network

Fake base stations, eavesdropping, termination point of user equipment security, central unit/distributed unit split, F1 interface security, tampering, etc.

8.3 Radio access

Jamming, physical layer security, etc.

8.4 Network infrastructure

Virtualization technologies, management and network orchestration (MANO) security, operating system, hardware security, open source, open architecture, supply chain security for network equipment, complicated network structure, etc.

8.5 Network slicing

Isolation of slices, slice authentication and access control, privacy preservation for slice users, attack to slice management, management among slices, access to multiple slices with various security levels, etc.

8.6 Software-defined networking

Security using SDN, security of SDN, etc.

8.7 Network function virtualization

Attack to orchestrator or controller, etc.

8.8 Multi-access edge computing

Cloud computing security, third party applications, decentralized authentication, etc.

8.9 Interoperability with 3G and 4G

Gateway and interconnection for signalling system No. 7 (SS7) and diameter), etc.

8.10 Roaming

Trust relationship, SEPP and gateway security, etc.

8.11 User equipment

Security of user equipment, etc.

8.12 Services based on 5G network functions

Authentication framework using device identifier or subscriber identification module (SIM) or embedded SIM, security for vertical services using 5G network functions, etc.

8.13 Security controls

Vulnerability management, security management, policy framework, inventory and configuration management, identity and account management, credential management, management protocol, security monitoring, disaster planning, etc.

8.14 Fraud

Stolen devices, counterfeit devices, abuse of network services, etc.

8.15 Non-public networks

Non-public networks (NPNs), local 5G, etc.

8.16 Others

Cryptographic algorithms, network operation and management, security assurance, etc.

9 Gap analysis in 5G security standardization

This clause provides a matrix for gap analysis and the related standardization activities with 5G security in order to identify standardization gaps.

The matrix is composed of two axes. The horizontal axis describes document categories that cover the subject of applications as follows:

- **general, definition**: the standard that provides general descriptions or terms and definitions of the technology;
- **common requirements, use cases**: the standard that provides use cases and derived general/functional requirements;
- **architecture**: the standard that provides reference architecture;
- **technical specification**: the standard that provides security procedures and mechanisms to protect a 5G system;
- **guideline**: the guideline document that provides countermeasures and guidance for 5G system management;
- **certification**: the standard that provides criteria for security assurance level or process of security certification;
- **others** (e.g., technical reports).

The vertical axis describes the related technologies for supporting 5G security, which is categorized in clause 8.

NOTE 1 – The items on the horizontal axis are not subordinated to the different technologies.

NOTE 2 – The items on the vertical axis can be modified with technology change.

NOTE 3 – A standard has more than one location on the matrix. If one standard is included in multiple document categories (horizontal axis) or related technologies (vertical axis), it can be mapped several times.

Table 9-1 – Standardization matrix of 5G security

Application	Category						
	General/ Definition	Common requirement, use cases	Architecture	Technical specification	Guideline	Certification	Others
General	3GPP TS 33.805, GSMA FS.40, 3GPP TR 33.866,	NIST SE5G			ITU-T X.5Gsec-guide,		

Table 9-1 – Standardization matrix of 5G security

Application	Category						
	General/ Definition	**Common requirement, use cases**	**Architecture**	**Technical specification**	**Guideline**	**Certification**	**Others**
	3GPP TR 33.852, ENISA Threat, ENISA Threat2				ENISA Supply NIST SP1800-33A, NIST SP1800-33B		
5G core network	3GPP TR 33.845	3GPP TS 33.814	3GPP TS 33.501, 3GPP TS 33.535 3GPP TS 33.807	3GPP TS 33.501, 3GPP TS 33.535, 3GPP TS 33.807, 3GPP TR 33.846, 3GPP TR 33.847, 3GPP TR 33.855, 3GPP TR 33.856, 3GPP TR 33.875	3GPP TS 33.808, 3GPP TR 33.876	3GPP TS 33.512, 3GPP TS 33.513, 3GPP TS 33.514, 3GPP TS 33.515, 3GPP TS 33.516, 3GPP TS 33.517, 3GPP TS 33.518, 3GPP TS 33.519, 3GPP TS 33.520, 3GPP TS 33.521, 3GPP TS 33.522	NGMN NCE
Radio access network		3GPP TS 33.840		3GPP TS 33.824	NGMN Pac1	3GPP TS 33.511	
Radio access	3GPP TR 33.865			3GPP TS 33.809, 3GPP TR 33.859, 3GPP TR 33.861, 3GPP TR 33.863			
Network infrastructure	3GPP TR 33.848	3GPP TS 33.818			3GPP TR 33.738	GSMA FS.13, GSMA FS.14, GSMA FS.15, GSMA FS.16	ENISA Virtual
Network slicing	ETSI GR ZSM 010	ITU-T X.1047, ITU-T X.5Gsec-ssl	ITU-T X.1047	3GPP TS 33.811, 3GPP TS 33.813			NGMN Pac2, GSMA NG.116
SDN	IEEE P1915.1	ITU-T X.1038, ITU-T X.1042	ITU-T X.1038, ITU-T X.1046				ENISA SDN
NFV	ETSI GS-VFV-SEC 001, ETSI GS-VFV-SEC 002 GSMA FS.33,	ITU-T X.1044, ITU-T X.1045,	ITU-T X.1046 ETSI GS-VFV-SEC 011		ETSI GS-VFV-SEC 003,		ETSI GS-VFV-SEC 004

Table 9-1 – Standardization matrix of 5G security

Application	Category						
	General/ Definition	**Common requirement, use cases**	**Architecture**	**Technical specification**	**Guideline**	**Certification**	**Others**
	IEEE P1915.1	ETSI GS-VFV-SEC 009, ETSI GS-VFV-SEC 014, ETSI GS-VFV-SEC 016, ETSI GS-VFV-SEC 020, ETSI GS-VFV-SEC 021, ETSI GS-VFV-SEC 022, ETSI GS-VFV-SEC 023, ETSI GS-VFV-SEC 024, ETSI GS-VFV-SEC 025	ETSI GS-VFV-SEC 012, ETSI GS-VFV-SEC 026		ETSI GS-VFV-SEC 006, ENISA NFV		ETSI GS-VFV-SEC 010 ETSI GS-VFV-SEC 013
MEC		ITU-T X.5Gsec-ecs, ITU-T X.5Gsec-netec, ITU-T X.itssec-5	ITU-T X.5Gsec-ecs	3GPP TS 33.839	3GPP TR 33.739		NGMN Pac3, ETSI GS MEC 030, ETSI GR MEC 031
Interoperability					GSMA FS.34	3GPP TS 33.520	
Roaming	ENISA Signal				GSMA FS.21, GSMA FS.36, GSMA FS.37, GSMA IR.77, GSMA NG.113	3GPP TS 33.517	
User equipment			IEEE P1912				
Services using 5G		3GPP TS 33.536, 3GPP TS 33.819, 3GPP TS 33.835, 3GPP TS 33.836,	NGMN E2E	3GPP TS 33.122, 3GPP TS 33.503, 3GPP TR 33.825, 3GPP TR 33.862	3GPP TR 33.740, 3GPP TR 33.881, 3GPP TR 33.889		

Table 9-1 – Standardization matrix of 5G security

Application	Category						
	General/ Definition	**Common requirement, use cases**	**Architecture**	**Technical specification**	**Guideline**	**Certification**	**Others**
		3GPP TR 33.850, 3GPP TR 33.851, 3GPP TR 33.854, X.5Gsec-message					
Security control	ETSI GR ZSM 010	ENISA 3GPP	ITU-T X.5Gsec-t, NGMN Trust		ETSI GS-VFV-SEC 013, NGMN NO, ENISA EECC		
Fraud	GSMA FS.39				GSMA FS.38		NGMN Pac3
Non public network		ITU-T X.5Gsec-vs		3GPP TR 33.857			
Others	3GPP TR 33.841, GSMA FS.35, ENISA Standards	3GPP TS 33.126	3GPP TS 33.127	3GPP TR 33.842	ITU-T X.1811		

According to the gap analysis in Table 9-1, note the following.

- ITU-T has been focusing on "common requirement or use cases", "architecture", "guideline" with specific technical area described in vertical axis.
- A 5G network system has many elements and becomes complicated. It is expected that standardization efforts of ITU-T will focus to provide security criteria by determining requirements to manage 5G network system component.
- Use cases using new functionality of 5G network will increase. It is expected that standardization efforts of ITU-T will provide risk or threat analysis and its countermeasures for new use cases.
- The entries in the row "Security control" are insufficient and their items are limited. There are several topics, such as controls of organization, people, operational or the physical situation. ITU-T has to consider initiating work items related to this topic.
- The need for 5G NPNs will increase in various vertical services. It is expected that standardization efforts of ITU-T will provide risk or threat analysis and its countermeasures for 5G NPN services in various vertical services.
- A 5G system employs certificate-based security mechanisms, such as TLS and OAuth2.0. However, traditional public key infrastructure (PKI) and certificate management are not suitable for 5G-based application environments since virtualized network function (VNF), SBA and microservice architecture are introduced to implement applications in 5G systems. Therefore, PKI and certificate management are the critical considerations for the standardization efforts of ITU-T.

– 5G system standards and specifications are complex and fundamental. Proper implementation of security features of standards and proper operation and management of 5G systems are critical to making 5G systems and applications secure. It is expected that standardization efforts of ITU-T will provide security best practices for network configuration, deployment, operation, and management.