ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1816 (03/2023)

SERIES X: Data networks, open system communications and security

IMT-2020 Security

Guidelines and requirements for classifying security capabilities in IMT-2020 network slice

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	**X.1800–X.1819**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1816

Guidelines and requirements for classifying security capabilities in IMT-2020 network slice

Summary

The definition of basic network slicing technology functions and processes has laid a solid foundation for the first wave of IMT-2020 deployment and commercial use of network slicing services. As an end-to-end logical network that is customized on demand, slicing can provide differentiation security capabilities: First, the IMT-2020 network slicing provides the supporting security measures for the differentiated network implementation. Second, the IMT-2020 network supports some optional security measures at the slice level. Some security measures can also provide multiple security options and operators may own different security resources. These may bring different degrees of security guarantee or non-security performance. Slice customers also have specific security requirements and may request customized network slices with different security protection levels from slice operators. There exist some challenges for the slice customers or the slice operators choosing the security capabilities of their slices such as management cost and definition inconsistency, etc. The objective of Recommendation ITU-T X.1816 is to provide a description of differentiated IMT-2020 network slice security capabilities and guidelines for classifying the IMT-2020 network slice security capabilities and IMT-2020 network slice security to help the ecosystem more clearly understand and choose the slicing security capabilities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1816	2023-03-03	17	11.1002/1000/15114

Keywords

Classification, IMT-2020, network slice, security capabilities.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1816

Guidelines and requirements for classifying security capabilities in IMT-2020 network slice

1 Scope

The objective of this Recommendation is to provide guideline and requirements for classifying IMT-2020 network slice security. This Recommendation specifies:

- Definition of the differentiated IMT-2020 network slice security capabilities;
- Principles and methods for identifying the classification of IMT-2020 network slice security capabilities.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T X.1047] Recommendation ITU-T X.1047 (2021), *Security requirements and architecture for network slice management and orchestration*.

[3GPP TS 33.501] Technical Specification 3GPP TS 33.501 V17.1.0 (2021), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 17).*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 network slice [b-ITU-T Y.3100]: A logical network that provides specific network capabilities and network characteristics.

NOTE 1 – Network slices enable the creation of customized networks to provide flexible solutions for different market scenarios which have diverse requirements, with respect to functionalities, performance and resource allocation.

NOTE 2 – A network slice may have the ability to expose its capabilities.

NOTE 3 – The behaviour of a network slice is realized via network slice instance(s).

3.1.2 network slice instance [b-ITU-T Y.3100]: An instance of a network slice, which is created based on a network slice blueprint.

3.1.3 network slice subnet [b-ETSI TS 128 530]: A representation of the management aspects of a set of managed functions and the required resources (e.g., compute, storage and networking resources).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AMF	Access and Mobility Management Function
CN	Core Network
CU	Central Unit
DDoS	Distributed Denial-of-Service
DU	Distributed Unit
EAP	Extensible Authentication Protocol
ENSI	External Network Slice Information
gNB	NR Node B
IMT-2020	International Mobile Telecommunications-2020
NAT	Network Address Translation
NFV	Network Function Virtualization
ng-eNB	Next Generation Evolved Node-B
NSSAI	Network Slice Selection Assistance Information
S-NSSAI	Single Network Slice Selection Assistance Information
PDU	Protocol Data Unit
PNF	Physical Network Function
RAN	Radio Access Network
RB	Radio Bearer
TLS	Transport Layer Security
UE	User Equipment
URL	Uniform Resource Locator
VNF	Virtual Network Function
WAF	Web Application Firewall

5 Conventions

In this Recommendation:

The keywords **"is recommended"** indicate a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords **"can optionally"** indicate an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network

operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Introduction of the classification for IMT-2020 network slice security capabilities

Network slice security is the prerequisite for introducing network slicing. For slice customers who use slice communication services, they require a corresponding security assurance tailored to their slices implementation and might also have specific security requirements based on their services using slices. So, they may request customized network slices with different security protection from the carriers. For the slice operators who design, build and operate networks and provide network slices, slicing involves many domains (e.g., wireless, transmission, core network, and management) and can provide differentiated security capabilities: Firstly, IMT-2020 network slicing provides security measures for differentiated network implementation. Secondly, IMT-2020 network supports some optional security measures at the slice level. Some security measures can also provide multiple security options and operators may own different security resources. These may bring different degrees of security guarantee or non-security performances. Thus, the security capabilities of one slice need to be decided based on the customers' requirements and the security capabilities that the network is capable of providing. Some challenges exist for the slice customers or the slice operators choosing the security capabilities of their slices:

- Customers' security requirements might be vague and few and not enough to be mapped to the security capabilities.
- The customers might have too many security requirements beyond the network's capabilities.

  The knowledge cost of the stakeholders for the security capabilities and the differences can vary and the combination of the capabilities they choose might not be reasonable. For example, the protection provided by the capabilities selected might be inconsistent for multiple domains or stakeholders.
- The number of combinations of the slice security capabilities might be tremendous and the management and orchestration cost of the operators might be relatively high.

Differentiated IMT-2020 network slice security capabilities and a methodology to classify and combine them will be recommended which has the following significance:

- It helps the industry to reach a unified understanding of the security capabilities of the slice and the difference among the slice security capabilities (e.g., performance).
- It provides a general basic classification of the IMT-2020 network slice security capabilities to make the industry clearly understand the slicing security ability and better match most of the industrial applications.
- It helps in realizing roaming between different slices, also facilitating the reuse of slices.
- It provides a reference for industry users to choose appropriate slices which can meet the requirements.
- It provides a reference for industry supervisors to formulate the development plans and strategies of slices.
- It provides a reference for service providers to deploy the services in appropriate slices.
- It provides a reference for operators to formulate the development plans of slices and to assess the value and prices of slices.
- It provides a reference for equipment vendors to plan the technology road map and the product road map of the slices.

The methodology includes the following aspects:

- List the general differentiated slicing security capabilities in a structured form including name, description, security dimension and options. This is provided in clause 7.

- For each security dimension, multiple levels of one security dimension can be formed by listing combinations of corresponding slicing security capabilities with different options based on some principles. This is provided in clause 8.
- Furthermore, basic slice security types composing of security dimensions can be formed by choosing one level for each security dimension based on some principles. This is provided in clause 9.
- The stakeholders can use the classification principle, methods and results to decide the security capabilities of one slice. This is provided in clause 10.

7 IMT-2020 network slice security capabilities

7.1 Template for network slice security capability descriptions

Clause 7 provides the list of the general IMT-2020 network security capabilities which can be different among network slices. The security capability descriptions should be clear, concise and unambiguous. Each description should include:

- Capability description: A detailed description of the differentiation IMT-2020 network slice security capability.
- Capability name: A unique name and an acronym assigned to each security capability.
- Capability security dimension: A particular aspect of the security that the security capability is designed to address. There are eight (8) security dimensions including access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability and privacy [ITU-T X.805].
- Capability options: Multiple choices for each security capability which can be different among slices. Each option is referenced as "capability acronym.serial number" in this Recommendation. Note: The options are generic and are not tied to specific network implementations. They can be further subdivided in order to be consistent with a specific implementation.

7.2 Differentiated IMT-2020 slice security capabilities

7.2.1 Network slice-specific authentication and authorization capability

- Capability description: IMT-2020 system provides optional-to-use network slice-specific authentication and authorization [3GPP TS 33.501] between a user equipment (UE) and an authentication, authorization and accounting server (AAA-S) which may be owned by an external 3rd party enterprise. The network slice-specific authentication and authorization can be triggered based on the single network slice selection assistance information (S-NSSAI) after the primary authentication. AAA server can also trigger slice-specific authorization revocation, re-authentication and re-authorization.
- Capability name: Network slice-specific authentication and authorization (NSSAA)
- Capability security dimension: Authentication, access control
- Capability option:
  - NSSAA.0: off
  - NSSAA.1: on

7.2.2 Network slice isolation capability of the network resource

- Capability description: IMT-2020 network slices run on the operators' unified infrastructure resources. There are a variety of isolation solutions to prevent the slice network elements from accessing or influencing those in different slices through the shared infrastructure resources: From the aspect of slice subnet domains:

– For access network (AN): For the air interface, dynamic radio bear (RB) resource sharing and static RB resource reservation are available for resource allocation. The former has better and a more flexible coverage effect and resource utilization while the latter has higher reliability and cost. For the base station, the central unit (CU) and the (DU) distributed unit of different slices can be the same. For higher isolation levels, they can be physically isolated by allocating dedicated hardware or which are logically isolated by using the network function virtualization (NFV) (i.e., virtual machine/container) to share the hardware.

– For transport network (TN): The isolation on transport networks can be no isolation, physical isolation (e.g., physical network function isolation, physical network link isolation, etc.), logical isolation (e.g., logical network function isolation, logical/virtual network link isolation, etc.) [ITU-T X.1047].

– For core network (CN): Physical isolation of core network resource comprises one or more dedicated physical network function (PNF) isolation, dedicated physical network link isolation, geographical location isolation, compute isolation, memory isolation, storage isolation, PNF, security-based isolation and so on. Logical isolation of core network resource comprises one or more virtual network function (VNF) isolation, virtual link isolation, virtualization technology isolation, virtual compute isolation, virtual memory isolation, virtual storage isolation, geographical location isolation of HW which is virtualized to provide virtual resources, and VNF security-based isolation, and so on [ITU-T X.1047].

  From the aspect of resource types and isolation techniques:

  • For air interface resource: RB sharing or RB reservation

  • For network function resource of AN/TN/CN: physical isolation, logical isolation, or no isolation

• Capability name: Slice isolation of the network resource (SIR)

• Capability security dimension: Access control, availability, privacy

• Capability options and corresponding performance:

  – SIR.0: no isolation

  – SIR.1: Logical isolation+RB sharing

  – SIR.2: Logical+physical isolation+RB sharing

  – SIR.3: Physical isolation+RB sharing

  – SIR.4: Logical isolation+RB reservation

  – SIR.5: Logical+physical isolation+RB reservation

  – SIR.6: Physical isolation+RB reservation

7.2.3 User plane data protection capability

• Capability description: IMT-2020 system can provide differentiated user plane data protection capabilities at the slice level. The next generation evolved Node-B (ng-eNB)/NR Node B (gNB) can decide whether to activate user plane confidentiality and/or user plane integrity protection per PDU session, according to the received user plane security policy. The user plane security policy can be configured to indicate "Required" or "Not needed". There are optional encryption algorithms [3GPP TS 33.501].

• Capability name: User plane data protection (UPDP)

• Capability security dimension: Data confidentiality, data integrity

• Capability option:

  – UPDP.0: not to activate user plane confidentiality and/or user plane integrity protection

– UPDP.1: to activate user plane confidentiality and/or user plane integrity protection with optional encryption algorithms

7.2.4 Boundary protection capability

- Capability description: It is important to protect a network slice from network attacks by deploying security control functions/features at the boundary, especially at the CN boundary (e.g., N6Protection configuration for N6 interface) [b-3GPP TS 28.541]. For different network slice consumers, the security control functions/features might be different and could be changed dynamically according to the requirements. The security control functions can be firewall, network address translation (NAT), antimalware, parental control, distributed denial-of-service (DDoS) protection function, etc. [b-3GPP TS 28.541]. The features refer to forwarding rules, filtering rules, parameter configuration, etc. The requirements could be access control to the data network and tunnelling mechanism.
- Capability name: Boundary protection (BP)
- Capability security dimension: Access control, availability, communication security
- Capability option:
  - BP.0: no security control functions
  - BP.1: security control functions/features deployed

7.2.5 Application service protection capabilities

- Capability description: The operators can deploy security devices or security modules on the network side to provide different security protection for the application services using slices and the users using the application services. For example, the operator network can provide abnormal terminal detection, network traffic cleaning, malicious uniform resource locator (URL) detection, web application firewall (WAF), anti DDoS, and so on.
- Capability name: Application service protection (ASP)
- Capability security dimension: Communication security, access control, availability
- Capability option:
  - ASP.0: no application service protection
  - ASP.1: application service protections deployed

7.2.6 Privacy protection capability of the EAP ID during NSSAA

- Capability description: Multiple extensible authentication protocol (EAP) methods [b-IETF RFC 3748] are possible for slice specific authentication. A privacy-protection capable EAP method e.g., EAP- transport layer security (TLS) [b-IETF RFC 5216], EAP-TTLS [b-IETF RFC 5281]) can be chosen to use to protect privacy of the EAP ID used for the EAP-based NSSAA [3GPP TS 33.501].
- Capability name: Privacy protection of the EAP ID during NSSAA (PPEAP)
- Capability security dimension: Privacy
- Capability option:
  - PPEAP.0: not to use privacy-protection capable EAP methods
  - PPEAP.1: to use privacy-protection capable EAP methods

7.2.7 Privacy protection capability of the (S-)NSSAI

- Capability description: NSSAI is used to identify network slice/service type. Some information about the operator's network and customers might be derived from the NSSAI and its usage. IMT-2020 network provides the capabilities to protect the privacy of (S-)NSSAI by allowing not using the NSSAI or using alternative information outside the

operator's domain. During the registration procedure, the access and mobility management function (AMF) may provide to the UE in the registration accept message, an access stratum connection establishment NSSAI inclusion mode parameter, indicating whether and when the UE shall include NSSAI information in the access stratum connection establishment according to the different modes. The UE shall by default not provide NSSAI in the access stratum of 3GPP access unless it has been provided with an indication to operate in other modes [b-3GPP TS 23.502]. During NSSAA, if the AAA server used belongs to a 3rd party, the S-NSSAI which is an internal IMT-2020 core, the information can be optionally mapped in the operator's network to an external network slice information (ENSI) which is transmitted and used outside the operator domain [3GPP TS 33.501].

- Capability name: Privacy protection of the (S-)NSSAI (PPSI)
- Capability security dimension: privacy
- Capability option:
  - PPSI.0: to use NSSAI outside the operator's domain
  - PPSI.1: not to use NSSAI or to use alternative information outside the operator's domain

7.3 Classification of IMT-2020 slice security capabilities

IMT-2020 slice security capabilities can be classified based on their security dimension as shown in Table 7-1.

Table 7-1 – Classification of IMT-2020 slice security capabilities based on the security dimension

Security dimension / Slice security capability	Network slice-specific authentication and authorization (NSSAA)	Slice isolation for the resource (SIR)	User plane data protection (UPDP)	Boundary protection (BP)	Application service protection (ASP)	Privacy protection of the EAP ID during NSSAA (PPEAP)	Privacy protection of the (S-)NSSAI (PPSI)
Access control	√	√		√	√		
Authentication	√						
Non-repudiation							
Data confidentiality			√				
Communication security				√	√		
Data integrity			√				
Availability		√		√	√		
Privacy		√				√	√

8 Classification for security dimensions achieved by slice security capabilities

8.1 Method and principle for classification of security dimensions based on slice security capabilities

The method for classifying each security dimension is as follows:

1) It is recommended to list the security capabilities and the related options belonging to the security dimension. If there is a small possibility for one security capability affecting some

security dimension, this security capability can optionally not be listed in the security dimension but only be listed in other security dimensions mainly affected.

2) It is recommended to list the combination of different options of the capabilities and form the different levels of the security dimension. If a security dimension is achieved by multiple security capabilities, each protection effect level should be kept consistent for multiple domains or stakeholders when combining the options of security capabilities. The xx.nn (e.g., AC.1, …, DI.0) refers to the level name of the security dimension xx.

Clause 8.2 gives the generic list of the eight security dimensions with levels based on the security capabilities and the options listed in clause 7.

8.2 Security dimensions with levels based on IMT-2020 slice security capabilities

8.2.1 Access control based on IMT-2020 slice security capabilities

Access control can be achieved by capabilities with options including but not limited to: Network slice-specific authentication and authorization, slice isolation of network resource, boundary protection and application service protection. There are a variety of combinations of capabilities with different options for achieving different levels of access control. It is shown as follows based on clause 7.

Table 8-1 – Levels of access control

Security dimension: Access control (AC)														
Capability	**Network slice-specific authentication and authorization (NSSAA)**		**Application service protection (ASP)**		**Slice isolation for the resource (SIR)**							**Boundary protection (BP)**		**Level name**
Options	**NSSAA.0**	**NSSAA.1**	**ASP.0**	**ASP.1**	**SIR.0**	**SIR.1**	**SIR.2**	**SIR.3**	**SIR.4**	**SIR.5**	**SIR.6**	**BP.0**	**BP.1**	
Combination	NSSAA.0		ASP.0		SIR.0							BP.0		AC.0000
					SIR.0							BP.1		AC.0001
					SIR.1 SIR.4							BP.0		AC.0010 AC.0040
					SIR.1 SIR.4							BP.1		AC.0011 AC.0041
					SIR.2 SIR.5							BP.0		AC.0020 AC.0050
					SIR.2 SIR.5							BP.1		AC.0021 AC.0051
					SIR.3 SIR.6							BP.1		AC.0031 AC.0061
			ASP.1		SIR.0							BP.0		AC.0100
					SIR.0							BP.1		AC.0101
					SIR.1 SIR.4							BP.0		AC.0110 AC.0140
					SIR.1 SIR.4							BP.1		AC.0111 AC.0141

Table 8-1 – Levels of access control

<table>
<tr><th colspan="13">Security dimension: Access control (AC)</th></tr>
<tr><th rowspan="2">Capability</th><th colspan="2" rowspan="2">Network slice-specific authentication and authorization (NSSAA)</th><th colspan="2" rowspan="2">Application service protection (ASP)</th><th colspan="7" rowspan="2">Slice isolation for the resource (SIR)</th><th colspan="2" rowspan="2">Boundary protection (BP)</th><th rowspan="2">Level name</th></tr>
<tr></tr>
<tr><th>Options</th><th>NSSAA.0</th><th>NSSAA.1</th><th>ASP.0</th><th>ASP.1</th><th>SIR.0</th><th>SIR.1</th><th>SIR.2</th><th>SIR.3</th><th>SIR.4</th><th>SIR.5</th><th>SIR.6</th><th>BP.0</th><th>BP.1</th><th></th></tr>
<tr><td rowspan="20"></td><td colspan="3" rowspan="3"></td><td colspan="2" rowspan="3"></td><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.0</td><td>AC.0120
AC.0150</td></tr>
<tr><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.1</td><td>AC.0121
AC.0151</td></tr>
<tr><td colspan="7">SIR.3
SIR.6</td><td colspan="2">BP.1</td><td>AC.0131
AC.0161</td></tr>
<tr><td colspan="3" rowspan="18">NSSAA.1</td><td colspan="2" rowspan="9">ASP.0</td><td colspan="7">SIR.0</td><td colspan="2">BP.0</td><td>AC.1000</td></tr>
<tr><td colspan="7">SIR.0</td><td colspan="2">BP.1</td><td>AC.1001</td></tr>
<tr><td colspan="7">SIR.1
SIR.4</td><td colspan="2">BP.0</td><td>AC.1010
AC.1040</td></tr>
<tr><td colspan="7">SIR.1
SIR.4</td><td colspan="2">BP.1</td><td>AC.1011
AC.1041</td></tr>
<tr><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.0</td><td>AC.1020
AC.1050</td></tr>
<tr><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.1</td><td>AC.1021
AC.1051</td></tr>
<tr><td colspan="7">SIR.3
SIR.6</td><td colspan="2">BP.1</td><td>AC.1031
AC.1061</td></tr>
<tr><td colspan="2" rowspan="9">ASP.1</td><td colspan="7">SIR.0</td><td colspan="2">BP.0</td><td>AC.1100</td></tr>
<tr><td colspan="7">SIR.0</td><td colspan="2">BP.1</td><td>AC.1101</td></tr>
<tr><td colspan="7">SIR.1
SIR.4</td><td colspan="2">BP.0</td><td>AC.1110
AC.1140</td></tr>
<tr><td colspan="7">SIR.1
SIR.4</td><td colspan="2">BP.1</td><td>AC.1111
AC.1141</td></tr>
<tr><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.0</td><td>AC.1120
AC.1150</td></tr>
<tr><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.1</td><td>AC.1121
AC.1151</td></tr>
<tr><td colspan="7">SIR.3
SIR.6</td><td colspan="2">BP.1</td><td>AC.1131
AC.1161</td></tr>
</table>

8.2.2 Authentication based on IMT-2020 slice security capabilities

Authentication can be achieved by capabilities including the network slice-specific authentication and authorization. There are two levels of authentication. It is shown as follows:

Table 8-2 – Levels of authentication

Security dimension: Authentication (Au)			
Capability	**Network slice-specific authentication and authorization (NSSAA)**		**Level name**
Options	**NSSAA.0**	**NSSAA.1**	
Combination	NSSAA.0		Au.0
	NSSAA.1		Au.1

8.2.3 Non-repudiation based on IMT-2020 slice security capabilities

No capability in clause 7 achieves non-repudiation.

8.2.4 Data confidentiality based on IMT-2020 slice security capabilities

Data confidentiality can be achieved by capabilities including the user plane data protection. There are two levels of authentication. It is shown as follows:

Table 8-3 – Levels of data confidentiality

Security dimension: Data confidentiality (DC)			
Capability	**User plane data protection (UPDP)**		**Level name**
Options	**UPDP.0**	**UPDP.1**	
Combination	UPDP.0		DC.0
	UPDP.1		DC.1

8.2.5 Communication security based on IMT-2020 slice security capabilities

Communication security can be achieved by capabilities including boundary protection, application service protection. There are a variety of combinations of the capabilities with different options achieving different levels of communication security. It is shown as follows:

Table 8-4 – Levels of communication security

Security dimension: Communication security (CS)					
Capabilities	**Boundary protection (BP)**		**Application service protection (ASP)**		**Level name**
Options	**BP.0**	**BP.1**	**ASP.0**	**ASP.1**	
Combinations	BP.0		ASP.0		CS.00
	BP.0		ASP.1		CS.01
	BP.1		ASP.0		CS.10
	BP.1		ASP.1		CS.11

8.2.6 Data integrity based on IMT-2020 slice security capabilities

Data integrity can be achieved by the capabilities including user plane data protection capability. There are two levels of data integrity. It is shown as follows:

Table 8-5 – Levels of data integrity

Security dimension: Data integrity (DI)			
Capability	**User plane data protection (UPDP)**		**Level name**
Options	**UPDP.0**	**UPDP.1**	
Combination	UPDP.0		DI.0
	UPDP.1		DI.1

8.2.7 Availability based on IMT-2020 slice security capabilities

Availability can be achieved by the capabilities including slice isolation for the network resource, boundary protection and application service protection. There are a variety of combinations of the capabilities with different options achieving different levels of availability. It is shown as follows:

Table 8-6 – Levels of availability

Security dimension: Availability (Av)							
Capability	**Application service protection (ASP)**		**Slice isolation for the resource (SIR)**		**Boundary protection (BP)**		**Level name**
Options combination	**ASP.0**	**ASP.1**	**SIR.1/SIR.2/SIR.3**	**SIR.4/SIR.5/SIR.6**	**BP.0**	**BP.1**	
	ASP.0		SIR.1/SIR.2/SIR.3		BP.0		Av.000
					BP.1		Av.001
			SIR.4/SIR.5/SIR.6		BP.0		Av.010
					BP.1		Av.011
	ASP.1		SIR.1/SIR.2/SIR.3		BP.0		Av.100
					BP.1		Av.101
			SIR.4/SIR.5/SIR.6		BP.0		Av.110
					BP.1		Av.111

8.2.8 Privacy based on IMT-2020 slice security capabilities

Privacy can be achieved by the capabilities including privacy protection of the EAP ID during NSSAA, privacy protection of the (S-)NSSAI. There are a variety of combinations of the capabilities with different options achieving different levels of privacy. It is shown as follows:

Table 8-7 – Levels of privacy

Security dimension: Privacy (Pr)					
Capabilities	**Privacy protection of the EAP ID during NSSAA (PPEAP)**		**Privacy protection of the (S-)NSSAI (PPSI)**		**Level name**
Options	**PPEAP.0**	**PPEAP.1**	**PPSI.0**	**PPSI.1**	
Combinations	PPEAP.0		PPSI.0		Pr.00
	PPEAP.0		PPSI.1		Pr.01
	PPEAP.1		PPSI.0		Pr.10
	PPEAP.1		PPSI.1		Pr.11

9 Guideline and requirements for slice security types

A set of security dimensions can characterize a security type of network slice and can be differentiated by a service category. There will be many kinds of slice security types by combining security dimensions with different levels. But not all combinations are reasonable.

The method and principle to form slice security types are:

1) It is recommended to determine the levels of the security dimensions with higher priority first according to service requirements and performance of the levels.
2) It is recommended to determine the levels of remaining security dimensions according to service requirements and performance of the levels.
3) It is recommended to check whether there is a conflict between each security dimension for coordination. In a slice, for different security dimensions containing the same security capability, the options of the security capability should be consistent.
4) When the option of some capabilities or the level of some security dimensions are updated for a slice security type, it is recommended to change the related capabilities and security dimension to keep consistent.

10 Guideline and requirements for stakeholders with the classification for network slice security capabilities

It is recommended for the slice operators to prepare their own slice security capability list based on the generic slice security capability list in clause 7 and their private security capabilities.

It is recommended for the slice operators to prepare their own list of security dimensions with levels based on the generic list of security dimensions with levels and their private security capabilities or other dimensions according to the method in clause 8.

It is recommended for the slice operators to prepare their own list of slice security types according to the method in clause 9.

It is recommended for the slice operators to decide the security capabilities and options for a slice instance (e.g., during provisioning [b-ETSI TS 128 531]) based on their slice security capability list or their list of security dimensions with levels or their lists of slice security types by mapping from the levels of security dimensions or slice security types.

It is recommended for the slice customers to choose combinations of security capabilities and options from the generic slice security capability list or the operator's slice security capability list if the customers know clearly about their security requirements and the mapped security capabilities.

It is recommended for the slice customers to choose levels of related security dimensions according to the performance of the levels from the generic list of security dimensions with levels or the operator's list of security dimensions with levels, if the customers know the effect of some security dimension they want to achieve.

It is recommended for the slice customers to choose one type from the operator's list of slice security types, if the customers barely know the detailed security content.

Appendix I

Performance for IMT-2020 network slice security capabilities' options

(This appendix does not form an integral part of this Recommendation.)

NOTE – The performance depends on specific implementation details and may change with the development of technology.

- Performance for NSSAA's options:
  - NSSAA.0: base level
  - NSSAA.1: more autonomy (for the vertical industry)
- Performance for SIR's options:
  - SIR.0: no isolation: base level
  - SIR.1: Logical isolation+RB sharing: SIR.1 is more flexible and may have lower costs than SIR.2 and SIR.3.
  - SIR.2: Logical+physical isolation+RB sharing: SIR.2 is more flexible and may have lower cost than SIR.3. SIR.2 has higher reliability than SIR.1.
  - SIR.3: Physical isolation+RB sharing: SIR.3 has higher reliability and resource cost than SIR.1 and SIR.2.
  - SIR.4: Logical isolation+RB reservation: SIR.4 is more flexible and may have lower costs than SIR.5 and SIR.6.
  - SIR.5: Logical+physical isolation+RB reservation: SIR.5 is more flexible and may have a lower cost than SIR.6. SIR.2 has higher reliability than SIR.4
  - SIR.6: Physical isolation+RB reservation: SIR.6 has lower latency, higher reliability and cost than others.

Options with logical isolation may have lower costs on server resources than the options with physical isolation while the former may need more cost on security countermeasures than the latter to achieve a similar protection effect.

Options with physical isolation may achieve a higher level of access control than options with logical isolation.

Options with RB sharing have better and more flexible coverage effect and resource utilization than options with RB reservation.

- Performance for UPDP's options:
  - UPDP.0: There is no data protection in the air interface and lower latency than UPDP.1
  - UPDP.1: There is data protection in the air interface with different protection effects depending on the optional encryption algorithms
- Performance for BP's options:
  - BP.0: base level
  - BP.1: There is boundary protection with different protection effects depending on the optional security control functions/features deployed
- Performance for ASP's options:
  - ASP.0: base level
  - ASP.1: There is an application service protection with different protection effects depending on the optional application service protections
- Performance for PPEAP's options:

  - PPEAP.0: UE's identity is exposed
  - PPEAP.1: UE's identity is anonymous
- Performance for PPSI's options:
  - PPSI.0: (S-)NSSAI is exposed
  - PPSI.1: (S-)NSSAI is unrevealed

Appendix II

Example of basic IMT-2020 slice security types

(This appendix does not form an integral part of this Recommendation.)

The following table of the basic slice security types is formed based on the method of clause 9 which can be directly used by the stakeholders or adjusted on this to form their own basic slice security types.

Table II.1 – Examples of basic slice security types

Slice security type	Access control	Authentication	Availability	Communication security	Data confidentiality	Data integrity	Non-repudiation	Privacy	Judgement	Suitable services
0	AC.0	Au.0	Av.0	CS.0	DC.0	DI.0	–	Pr.0	Base security	Public network
1	AC.1161	Au.1	Av.111	CS.11	DC.1	DI.1	–	Pr.11	High security, highest cost	High security types, like Private lines for government, finance, securities and power grid customers
2	AC.0000	Autor.0	Av.0	CS.0	–	–	–	–	Low cost	Low-cost type, Internet access and OTT video
3	AC.xx61	–	Av.x11	–	–	–	–	Pr.xx4 Pr.xx6	High isolation, high cost	High isolation type
4	–	–	Av.x1x	–	DC.0	DI.0	–	–	Low latency	Low latency type, like cloud game

NOTE – x in the serial number of the level name refers to any value.

Bibliography

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-3GPP TS 23.502] 3GPP TS 23.502, *Procedures for the 5G System (5GS)*. <https://www.3gpp.org/ftp/Specs/archive/23_series/23.502>

[b-3GPP TS 28.541] 3GPP TS 28.541, *Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3*. <https://www.3gpp.org/ftp/Specs/archive/28_series/28.541>

[b-IETF RFC 3748] IETF RFC 3748, *Extensible Authentication Protocol (EAP).* <https://tools.ietf.org/html/rfc3748>

[b-IETF RFC 5216] IETF RFC 5216, *The EAP-TLS Authentication Protocol*. <https://www.rfc-editor.org/rfc/rfc5216.html>

[b-IETF RFC 5281] IETF RFC 5281, *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0).* <https://datatracker.ietf.org/doc/html/rfc5281>

[b-ETSI TS 128 530] Technical Specification ETSI TS 128 530 V17.1.0 (2022), *5G; Management and orchestration; Concepts, use cases and requirements* (3GPP TS 28.530 version 17.2.0 Release 17). < https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/17.02.00_60/ts_128530v170200p.pdf>

[b-ETSI TS 128 531] Technical Specification ETSI TS 128 531 V16.9.0 (2021), *5G; Management and orchestration; Provisioning;* (3GPP TS 28.531 version 16.6.0 Release 16). <https://www.etsi.org/deliver/etsi_ts/128500_128599/128531/16.06.00_60/ts_128531v160600p.pdf >

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023