International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1047

(10/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

Security requirements and architecture for network slice management and orchestration

Recommendation ITU-T X.1047

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.1047

Security requirements and architecture for network slice management and orchestration

Summary

Recommendation ITU-T X.1047 establishes the security requirements and architecture for network slice management and orchestration, as well as the automatic creation of an end-to-end (E2E) network slices with customized security capabilities, to deploy full-scale E2E network slicing for consumers, businesses and government segments.

Mobile communication is fast developing and reaching industries such as the automotive, manufacturing, logistics and energy, as well as sectors such as the finance and healthcare that do not currently fully exploit the potentiality of mobile services. However, various applications have different requirements. Some applications may require ultra-reliable communication, whereas others may require ultra-high-bandwidth communication or extremely low latency. Hence, network slicing has been introduced to offer a differentiated mix of capabilities to meet all these diverse requirements at the same time.

With network slicing, various types of users or customers can enjoy connectivity and data processing tailored to their specific requirements (e.g., data speed, quality, latency, reliability, security and pricing model) that adhere to a service level agreement (SLA) that agrees with consumers, enterprises and vertical industries. However, there are also challenges for implementing full-scale E2E network slicing deployments for consumers, businesses and government segments, e.g., E2E precision slicing, network slice reliability, network slice scalability and network slice lifecycle management. Among these challenges, the most important one is network slice security, which is receiving far more attention from academia and various industries.

3GPP TR 33.811 is a study on the security for the interface exposed to network slice management and integrity protection of the network slice subnet template, and 3GPP TS 33.501 specified security management of network slices (e.g., authentication, authorization, integrity protection and confidentiality protection for the interface between the producer and the consumer of management service). 3GPP TR 33.813 further focusses on the network slice specific authentication and authorization, data confidentiality and integrity, user identification privacy and inter-slice security isolation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1047	2021-10-29	17	11.1002/1000/14794

Keywords

Network slice management and orchestration, security, tamper-proof network slice management data.

---

* 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

Page

Introduction

This Recommendation leverages on the network function virtualization (NFV), software-defining network and service function chain where logical network slices are created to offer end-to-end communication services to consumers, enterprises and industry verticals. However, various users have different needs in terms of latency, bandwidth, security, etc. Some require high-level security protection, while others are satisfied with the so-called 'good enough'. This is called network slicing where the network can be logically separated into different network slices, each supporting a different service level agreement and security (SEC) protection level.

Recommendation ITU-T X.1047

Security requirements and architecture for network slice management and orchestration

1 Scope

This Recommendation specifies:

- security requirements for *network slice management and orchestration*;
- security requirements for *network slice subnet (NSS) management and orchestration*;
- security requirements for service-based interfaces for the logical management functions
- security requirements for the interface between the *network slice subnet (NSS) management and orchestration and the network function virtualization-management and orchestration (NFV-MANO) / network function management (NFM) / transport network controller (TNC)* logical functions;
- a security reference architecture for network slice management and orchestration (MANO);
- how to apply the security reference architecture to the automatic creation of end-to-end (E2E) network slice with customized security capabilities, such as being isolated with fine-grained isolation policy and preventing network attacks at the edge of NSS domains;
- how to evaluate tamper-proof and access control mechanisms for network slice management data in order to make network slice management data traceable, verifiable and immutable, as well as guaranteeing that only authorized data consumers can access network slice management data based on fine-grained access control policy.

This is done in order to deploy a full-scale E2E network slicing securely for consumers, businesses and government segments.

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.1045] Recommendation ITU-T X.1045 (2019), *Security service chain architecture for networks and applications*.

[ITU-T Y.3111] Recommendation ITU-T Y.3111 (2017), *IMT-2020 network management and orchestration framework*.

[ETSI GS NFV-SEC 013] ETSI GS NFV-SEC 013 V3.1.1 (2017), *Network functions virtualisation (NFV) Release 3; Security; Security management and monitoring specification*.

[IETF RFC 4279] IETF RFC 4279 (2005), *Pre-shared key ciphersuites for transport layer security (TLS)*.

[IETF RFC 4301] IETF RFC 4301 (2005), *Security architecture for the Internet protocol*.

[IETF RFC 4303] IETF RFC 4303 (2005), *IP encapsulating security payload (ESP)*.

[IETF RFC 4306] IETF RFC 4306 (2005), *Internet key exchange (IKEv2) protocol*.

[IETF RFC 4314] IETF RFC 4314 (2005), *IMAP4 access control list (ACL) extension*.

[IETF RFC 4594] IETF RFC 4594 (2006), *Configuration guidelines for DiffServ service classes*.

[IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol: Version 1.2*.

[IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 authorization framework*.

[IETF RFC 7321] IETF RFC 7321 (2014), *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.

[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.

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

3.1.3 network slice subnet (NSS) [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).

3.1.4 network slice subnet instance (NSSI) [b-ETSI TS 128 530]: An instance of network slice subnet representing the management aspects of a set of managed function instances and the used resources (e.g., compute, storage and networking resources).

3.1.5 orchestration [b-ITU-T Y.3100]: In the context of IMT-2020, the processes aiming at the automated arrangement, coordination, instantiation and use of network functions and resources for both physical and virtual infrastructure by optimization criteria.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL Access Control List

AN Access Network

CN Core Network

DDoS Distributed Denial of Service

DLT Distributed Ledger Technology

eMBB enhanced Mobile Broadband

FW	Firewall
HW	Hardware
ID	Identifier
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MANO	Management and Orchestration
NAT	Network Address Translation
NFM	Network Function Management
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NFVO	Network Function Virtualization and Orchestration
NS	Network Slice
NSI	Network Slice Instance
NSS	Network Slice Subnet
NSSI	Network Slice Subnet Instance
NST	Network Slice Template
NSST	Network Slice Subnet Template
PNF	Physical Network Function
PSF	Physical Security Function
RAN	Radio Access Network
SEC	Security
SFC	Service Function Chain
SLA	Service Level Agreement
SDN	Software-Defined Network
TNC	Transport Network Controller
TN	Transport Network
VIM	Virtual Infrastructure Management
VLAN	Virtual Local Area Network
VNF	Virtual Network Function
VNFM	Virtual Network Function Management
VSF	Virtual Security Function

5 Conventions

In this Recommendation:

The keywords **"is required to"** indicate a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

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 **"is prohibited from"** indicate a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

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.

Italics are used in this Recommendation to indicate logical functions.

The R-nn (e.g., R-01, …, R-60) in clause 7 refers to the serial number of the security requirements for the network slice (NS) management and orchestration.

6 Introduction of network slice management and orchestration

Referring to [b-ETSI TS 128 530], [b-ETSI TS 128 531], [b-ETSI TS 128 533], [b-ETSI TS 128 541], [b-ETSI GS NFV-MAN 001], [b-IETF-TNS-framework] and [b-ETSI GS ZSM 002], reference architecture of network slice (NS) management and orchestration is shown in Figure 6-1.

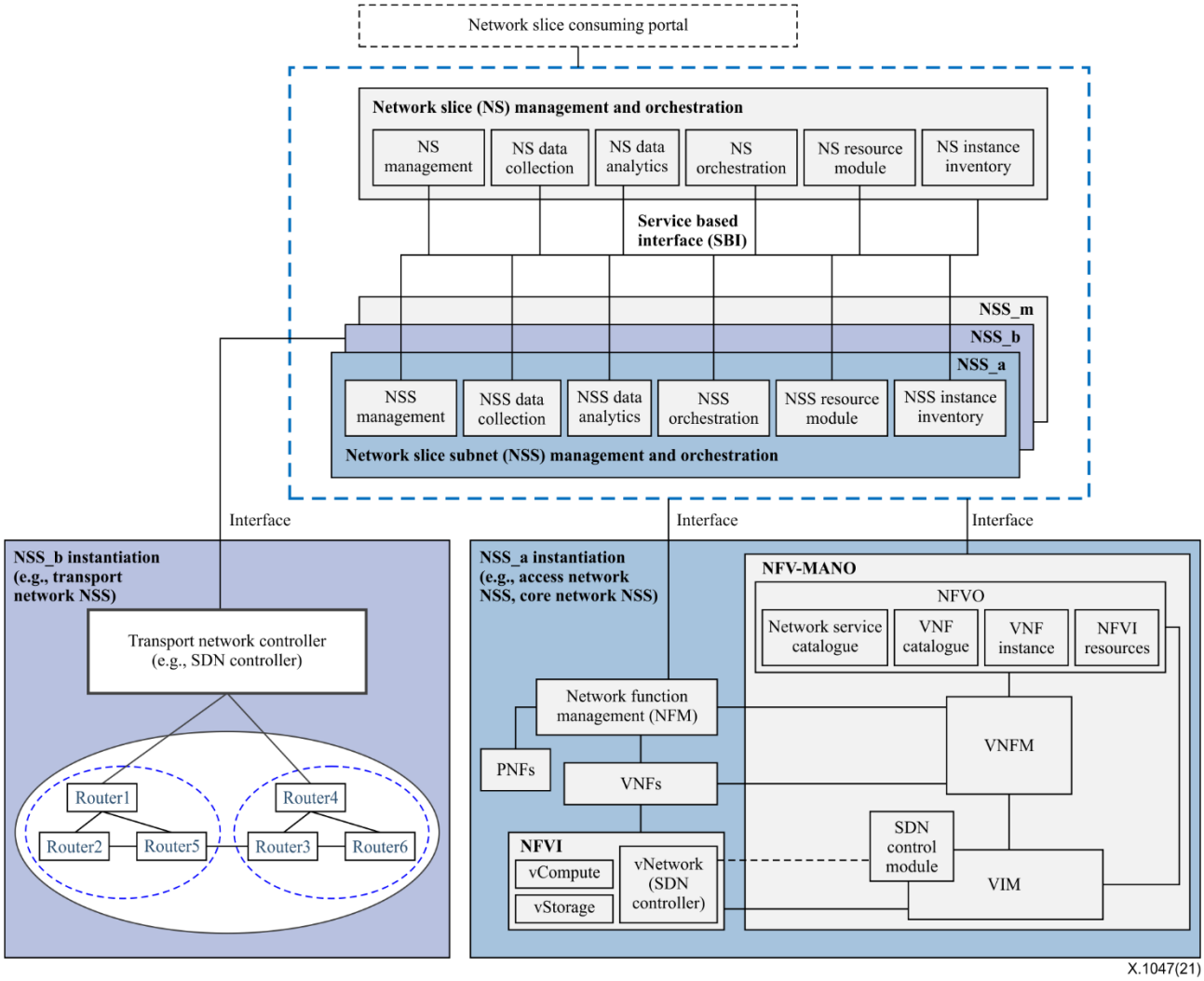

Figure 6-1 – Reference architecture of network slice management and orchestration

In Figure 6-1, an NSS instance may be a transport network (TN) NSS (e.g., NSS_b) instantiated through TNC, or an access network/core network (AN/CN) NSS (e.g., NSS_a) instantiated through NFV-MANO.

The capabilities or services provided by the logical functions of the reference architecture of NS MANO in Figure 6-1 are outlined as follows.

The reference architecture in Figure 6-1 supports service-based interfaces (SBI) for the logical functions of the *network slice (NS) management and orchestration* and the *network slice subnet (NSS) management and orchestration*.

The *network slice (NS) management and orchestration* consists of the following logical functions and is responsible for the preparation, commissioning, operation and decommissioning of network slice instance.

- The *NS orchestration* has the following capabilities:
  - **1)** resource capacity planning and modification [b-ETSI TS 128 530] [b-ETSI GS ZSM 002];
  - **2)** to receive the request for allocating resources for a network slice with certain characteristics (e.g., network slice type such as enhanced mobile broadband (eMBB), bandwidth, latency) from the *network slice consuming portal*;
  - **3)** to map the received request to an appropriate resource module (e.g., the chained NSSs) and the NSS requirements (e.g., slice profile, NSS type such as a radio access network (RAN) eMBB and CN eMBB, bandwidth, latency) [b-ETSI TS 128 531];
  - **4)** to decide whether this request for the allocation of resources for network slice is to be assigned to an existing network slice instance or a new network slice instance is to be created by checking the active network slice instances from the *NS instance inventory* [b-ETSI TS 128 531]. If there is no active network slice instance for the requested network slice service, then the *NS orchestration* gets to know the NSSs (e.g., NSS_a and NSS_b), and then sends the requests for allocation resource of NSS to the corresponding *NSS orchestrations* (e.g., of NSS_a and NSS_b) separately;
  - **5)** to receive the confirmed response of the allocation resources of the NSS from the *NSS orchestration*;
  - **6)** to check the feasibility and availability of allocated resources;
  - **7)** to configure the allocated resources;
  - **8)** to confirm the allocated resources of the network slice to the *network slice consuming portal*.
- The *NS resource module* has the capabilities to store network slice resource model, which describes the static parameters and functional components of network slice, including service profile, network slice type (e.g., eMBB), additional system feature (e.g., multicast) and priority [b-ETSI TS 128 531].
- The *NS instance inventory* has the capability to store information about the available network slice instances [b-ETSI GS ZSM 002].
- The *NS management* has the capability to support the following operation for a network slice instance: activation, supervision, performance reporting (e.g., for KPI monitoring) and deactivation [b-ETSI TS 128 530] [b-ETSI GS ZSM 002].
- The *NS data collection* has the capability of collecting network data (e.g., service, network slice, NSS, or network functions related data) to support the improving network performance, and the efficiency to accommodate and support the diversity of services and requirements [b-ETSI TS 128 530].
- The *NS data analytics* has the capability to utilize the collected network data to perform analytics in order to assist and complement the management services for optimum network performance and service assurance [b-ETSI TS 128 530].

The *network slice subnet (NSS) management and orchestration* consist of the following logical functions and is responsible for the preparation, commissioning, operation and decommissioning of an NSSI.

- The *NSS orchestration* has the following capabilities:
  - **1)** resource capacity planning and modification;
  - **2)** to receive the request for allocating resources for an NSS;
  - **3)** to map the received request to an appropriate resource model of the *NSS resource module* (e.g., the chained lower level NSS, list of managed network functions and their configuration parameters, network service in virtualization case, etc.) [b-ETSI TS 128 531];
  - **4)** to decide whether this request for allocating resources for an NSS is to be assigned to an existing NSSI or whether a new NSSI is to be created by checking the active NSSIs from the *NSS instance inventory*. If there is no active NSSI, the *NSS orchestration* sends the request for allocation resource for network service to the *NFV-MANO* in case a virtualized resource is provided [b-ETSI TS 128 531];
  - **5)** to receive the confirmed response of the allocation of resources of a network service from the *NFV-MANO*;
  - **6)** to confirm the allocation resources of the NSS to the *NS orchestration*.
- The *NSS resource module* has the capability to store the NSS resource model, which describes the static parameters and functional component of NSS, it includes network slice profile, NSS type (e.g., RAN eMBB, CN eMBB), additional system feature (e.g., multicast), priority and QoS attributes (e.g., bandwidth, latency) [b-ETSI TS 128 531].
- The *NSS instance inventory* has the capability to store information about the available NSSIs [b-ETSI GS ZSM 002].
- The *NSS management* has the capability to support the following operation for an NSSI: activation, supervision, performance reporting (e.g., for KPI monitoring) and deactivation [b-ETSI TS 128 530].
- The *NSS data collection* has the capability of collecting network data (e.g., network slice, NSS, network service, or network functions related data) to support the improving network performance and the efficiency to accommodate and support the diversity of services and requirements [b-ETSI TS 128 530].
- The *NSS data analytics* has the capability of utilizing the collected network data to perform analytics in order to assist and complement management services for optimum network performance and service assurance [b-ETSI TS 128 530].
- The *network function management* (NFM) is capable of application level management of virtual network functions (VNFs) and physical network functions (PNFs), and is a producer of the network function management as provisioning also including NF supervising services [b-ETSI TS 128 533].

  The *NFV-MANO* has the following capabilities:

  - **1)** to manage the network function virtualization infrastructure (NFVI) and orchestrate the allocation resources needed by the network services and VNFs;
  - **2)** to receive the request of allocating resources for network service from the *NSS orchestration*;
  - **3)** to map the received request to an appropriate network service catalogue with some network service instance requirements (e.g., bandwidth, latency);
  - **4)** to confirm the allocated resources for network service instance to the *NSS orchestration*. The logical functions of *NFV-MANO* in Figure 6-1 are summarized in Annex B.1.

The *transport network controller* [b-IETF-TNS-framework] [b-IETF-TS-definition] is a traditional network infrastructure controller (e.g., software-defined network (SDN) controller) that offers network resources to TN NSS MANO to be used for the realization of a particular transport slice. The TNC are existing network controllers used for a specific technology to realize transport slices in its network.

7 Security requirements for network slice management and orchestration

Based on the relevant security threats given in Annex A and providing network slice with customized security services for vertical industries, high-level security requirements for the components and interfaces in Figure 6-1 are established in this clause. This is done in order to secure network slice MANO, to create network slice instance with customized security capabilities, to monitor the network slice instance status, to ensure that service level agreements (SLAs) are consistently conformed to, and so on.

7.1 Security requirements for NS management and orchestration

The Recommendation mainly establishes security requirements for both the creation of network slice instance and the operation of network slice instance as follows.

7.1.1 Security requirements for the creation of a network slice instance

The process of the request for the allocation of resources of network slice includes assigning the request to an active network slice instance or creating a new network instance for the request.

R-01 It is required to have the capability to authenticate the *consumer* when the *consumer* requests the allocated resources for a network slice [3GPP TS 33.501] [b-3GPP TR 33.811] [ITU-T Y.3111].

R-02 It is required to have the capability to authorize the *consumer* when the *consumer* requests the allocated resources for a network slice [3GPP TS 33.501] [b-3GPP TR 33.811].

R-03 It is required to have the capability to support the logical functions of the *NS management and orchestration* mutually authenticating each other.

R-04 It is required to have the capability to support the logical function of the *NS management and orchestration* validating whether a requesting logical function is authorized to request a given service(s).

R-05 It is recommended to have the capability to support integrity protection for data transport over the service-based interfaces for the logical functions of the *NS management and orchestration*.

R-06 It is recommended to have the capability to support confidentiality protection for data transport over the service-based interfaces for the logical functions of the *NS management and orchestration*.

R-07 It is recommended to have the capability to support replay protection for data transport over the service-based interfaces for the logical functions of the *NS management and orchestration*.

R-08 It is required to have the capability to support the isolation between network slice instances [b-3GPP TR33.813].

R-09 It is recommended to have the capability to support integrity protection for the network slice resource model (i.e., network slice template (NST)) during transmission and in storage.

R-10 It is recommended to have the capability to support confidentiality protection for the network slice resource model (i.e., NST) during transmission and in storage.

R-11 It is recommended to have the capability to provide customized security services (e.g., integrity protection, confidentiality protection, hardware (HW) isolation, software isolation, anti-distributed denial of service (anti-DDoS) attack, anti-virus and anti-malware software) in order to satisfy the security requirements from the *consumer* via the *network slice consuming portal*.

R-12 It is recommended to have the capability to evaluate if the network slice resource model (i.e., NST) can satisfy the security requirements of the requested network slice resource from the *consumer* via the *network slice consuming portal*.

R-13 It is recommended to have the capability to evaluate if an active network slice instance can satisfy the security requirements of the requested network slice resource from the *consumer* via the *network slice consuming portal*.

R-14 It is required to support the integrity of managed services and management functions of the *NS management and orchestration* [b-ETSI GS ZSM 002].

7.1.2 Security requirements for the operation of a network slice instance

R-15 It is required to perform end user authentication and authorization before the end user accesses a network slice instance [b-3GPP TR 33.813] [ITU-T Y.3111].

R-16 It is recommended to have the capability to provide automated attack/incident detection, identification, prevention and mitigation for the network slice instance [b-ETSI GS ZSM 002] [ITU-T Y.3111].

R-17 It is recommended to have the capabilities for monitoring the activities, status, anomalous events of the network slice instance [ITU-T Y.3111].

R-18 It is recommended to have the capabilities for analysing the monitored data and providing reports on the behaviour of the network slice instance [ITU-T Y.3111].

R-19 It is recommended to have the capabilities for storing and retrieving monitored data and analysis reports of the network slice instance [ITU-T Y.3111].

R-20 It is recommended to support integrity protection for the result of network slice instance supervision/reporting in the *NS management and orchestration* [b-3GPP TR 33.811].

R-21 It is recommended to support the confidentiality protection for the network slice instance supervision and reporting data in the *NS management and orchestration* [b-3GPP TR 33.811].

R-22 It is required to support the integrity of management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) of network slice instance in the *NS management and orchestration* [b-ETSI GS ZSM 002].

R-23 It is required to support non-repudiation/tamper-proof of management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) of network slice instance in the *NS management and orchestration*.

R-24 It is recommended to support the confidentiality of the management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) of network slice instance in the *NS management and orchestration* [b-ETSI GS ZSM 002].

7.2 Security requirements for NSS management and orchestration

The Recommendation mainly establishes security requirements for both the creation and operation of an NSSI as follows:

7.2.1 Security requirements for the creation of a network slice subnet instance

R-25 It is required to have the capability to support the logical functions of the *NSS management and orchestration* mutually authenticating each other.

R-26 It is required to have the capability to support the logical function of the *NSS management and orchestration* validating whether a requesting logical function is authorized to request a given service(s).

R-27 It is recommended to have the capability to support integrity protection for data transport over the service-based interfaces for the logical functions of the *NSS management and orchestration*.

R-28 It is recommended to have the capability to support confidentiality protection for data transport over the service-based interfaces for the logical functions of the *NSS management and orchestration*.

R-29 It is recommended to have the capability to support replay protection for data transport over the service-based interfaces for the logical functions of the *NSS management and orchestration*.

R-30 It is required to have the capability to authenticate the *NFV-MANO/NFM/TNC*.

R-31 It is required to have the capability to support data integrity protection for data transport over the interface between the *NSS management and orchestration* and the *NFV-MANO/NFM/TNC*.

R-32 It is required to have the capability to support data confidentiality protection for data transport over the interface between the *NSS management and orchestration* and the *NFV-MANO/NFM/TNC*.

R-33 It is required to have the capability to support replay protection for data transport over the interface between the *NSS management and orchestration* and the *NFV-MANO/NFM/TNC*.

R-34 It is recommended to have the capability to support integrity protection for the NSS resource model (i.e., network slice subnet template (NSST)) during transmission and in storage [b-3GPP TR 33.811].

R-35 It is recommended to have the capability to support the confidentiality protection for the NSS resource model (i.e., NSST) during transmission and in storage [b-3GPP TR 33.811].

R-36 It is recommended to have the capability to provide customized security services (e.g., integrity protection, confidentiality protection, HW isolation, software isolation, anti-DDoS attack, anti-virus and anti-malware software) to satisfy the security requirements from the *NS management and orchestration*.

R-37 It is recommended to have the capability to create a separate NSSI in order to provide customized security services.

R-38 It is recommended to have the capability to evaluate if the NSS resource model (i.e., NSST) can satisfy the security requirements from the *NS management and orchestration*.

R-39 It is recommended to have the capability to evaluate if the available and active NSSI can satisfy the security requirements of the requested NSS resource from *NS management and orchestration*.

R-40 It is required to have the capability to support the isolation between NSSIs.

R-41 It is required to support the integrity of managed services and management functions of *NSS management and orchestration*.

7.2.2 Security requirements for the operation of a network slice subnet instance

R-42 It is recommended to have the capability to provide automated attack/incident detection, identification, prevention and mitigation for NSSI.

R-43 It is recommended to have the capabilities for monitoring the activities, status, anomalous events of the NSSI.

R-44 It is recommended to have the capabilities for analysing the monitored data and providing reports on the behaviour of the NSSI.

R-45 It is recommended to have the capabilities for storing and retrieving monitored data and analysis reports as logging records stored in the *NSS management and orchestration*.

R-46 It is recommended to perform integrity protection for the result of the NSSI supervision/reporting in the *NSS management and orchestration*.

R-47 It is recommended to perform confidentiality protection for the NSSI supervision and reporting data in the *NSS management and orchestration*.

R-48 It is required to support the integrity of the management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) of the NSSI in the *NSS management and orchestration*.

R-49 It is required to support the non-repudiation/tamper-proof of the management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) of the NSSI in the *NSS management and orchestration*.

R-50 It is recommended to support the confidentiality of the management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) of the NSSI in the *NSS management and orchestration*.

7.3 Security requirements for service-based interfaces for the logical functions

The logical functions of the *NS management and orchestration* and the *NSS management and orchestration* communicate with each other over service-based interfaces. This Recommendation establishes security requirements for service-based interfaces for the logical functions as follows.

R-51 It is required to have the capability to support the logical functions mutually authenticating each other.

R-52 It is required to have the capability to support the logical function validating whether a requesting logical function is authorized to request a given service(s).

R-53 It is recommended to have the capability to support integrity protection for data transport over the service-based interfaces for the logical functions.

R-54 It is recommended to have the capability to support the confidentiality protection for data transport over the service-based interfaces for the logical functions.

R-55 It is recommended to have the capability to support replay protection for data transport over the service-based interfaces for the logical functions.

7.4 Security requirements for an interface between *NSS management and orchestration* and *NFV-MANO/NFM/TNC*

This Recommendation establishes security requirements for the interfaces between *NSS management and orchestration* and *NFV-MANO/NFM/TNC* as follows.

R-56 It is required to perform mutual authentication between the *NSS management* and the *NFV-MANO/NFM/TNC*.

R-57 It is required for the NFV-MANO/NFM/TNC to authorize the requests from the *NSS management*.

R-58 It is required to provide integrity protection for data transport over the interface between the *NSS management* and the *NFV-MANO/NFM/TNC*.

R-59 It is required to provide confidentiality protection for data transport over the interface between the *NSS management* and the *NFV-MANO/NFM/TNC*.

R-60 It is required to provide replay protection for data transport over the interface between the *NSS management* and the *NFV-MANO/NFM/TNC*.

In order to support the securing of a network slice MANO, creating a network slice instance with customized security services and monitoring the network slice instance status to ensure that SLAs are consistently conformed to, security requirements for the *NFV-MANO* are defined in Annex B.2.

8 Security reference architecture for a network slice management and orchestration

A security reference architecture for a network slice MANO is shown in Figure 8-1, which is also integrated into the reference architecture of network slice MANO in Figure 6-1.

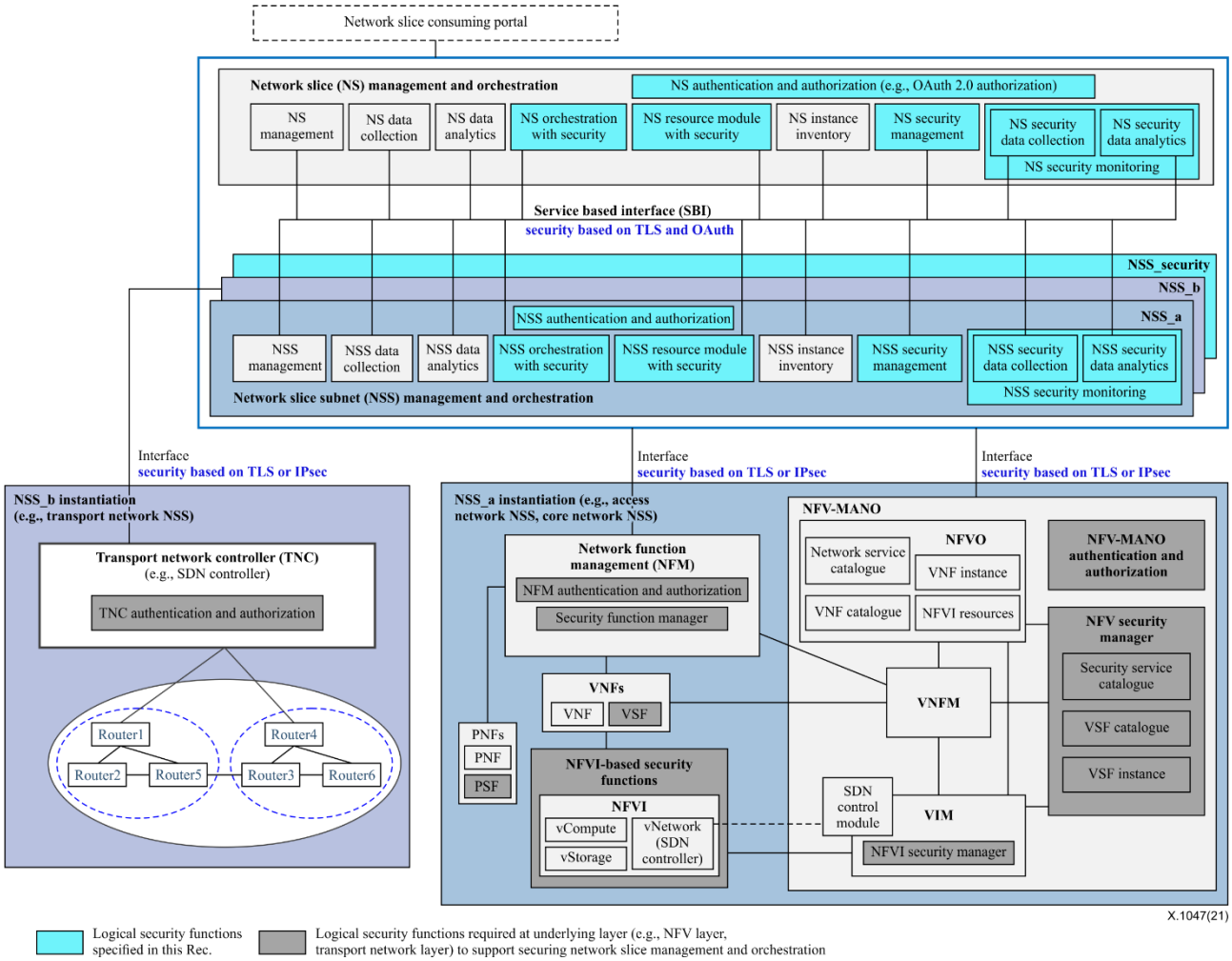

Figure 8-1 – Security reference architecture for a network slice management and orchestration

In Figure 8-1, some logical functions in Figure 6-1 are improved with security capabilities and some new logical security functions are introduced in this Recommendation in order to support the securing

of a network slice MANO, creating network slice instance with customized security capabilities for vertical industries, monitoring the network slice instance status to ensure that SLAs are consistently conformed to, and so on.

The logical security functions (i.e., blocks in light blue of Figure 8-1) relevant to NS or NSS MANO are specified in clauses 8.1 to 8.4. The logical security functions (i.e., blocks in grey of Figure 8-1) relevant to the *NFV-MANO* and the *transport network controller* are summarized in Annex B.3 and Annex C.1, respectively.

8.1 Security capabilities of a network slice (NS) management and orchestration

The new logical function *NS authentication & authorization* is introduced in this Recommendation to authenticate the *consumer* based on the certificate [IETF RFC 4306] [IETF RFC 5246] or a pre-shared key [IETF RFC 4279] [IETF RFC 4306] and authorizes the *consumer* based on a whitelist/blacklist [b-IETF RFC 5782] [b-IETF RFC 5851] or with an access control list (ACL) [IETF RFC 4314] [b-IETF RFC 4949], when the *consumer* requests the allocated resources for a network slice.

The new logical function *NS authentication & authorization* as the OAuth 2.0 authorization server supports all the logical functions of the *NS management and orchestration* mutually authenticating each other based on the certificate [IETF RFC 4306] [IETF RFC 5246] and validating whether a requesting logical function is authorized to request a given service(s) based on OAuth [IETF RFC 6749]. Integrity protection and confidentiality protection for data transport over the service-based interfaces for the logical functions of the *NS management and orchestration* are based on TLSv1.2 [IETF RFC 5246].

In order to provide a network slice with customized security capabilities through a creation of a security service function chain (SFC) comprising a set of security functions (e.g., authentication, firewall (FW) and the intrusion detection system/intrusion prevention system (IDS/IPS)) [ITU-T X.1045] [b-Hu], the logical function *NS orchestration* given in Figure 6-1 is to be improved as the logical function *NS orchestration with security* in Figure 8-1, that includes one or more logical functions, such as security orchestration, isolation management and FW management. Also, to simplify the security reference architecture, only one logical function *NS orchestration with security* is shown in Figure 8-1. The *NS orchestration with security* has the following security capabilities:

- to extend the network slice service characteristics in order to include security capabilities represented by a security service type list (e.g., security protection at the edge of network slice, slice isolation, malware/virus detection and data cleaning, tamper-proof for management data, confidentiality protection for data in transit and at rest, integrity protection for data in transit and at rest);
- to receive the request for the allocation of resources for a network slice with security requirements;
- to map the received request with security requirements to an appropriate resource module of the *NS resource module with security* (e.g., service profile, …, security profile(s) (e.g., data confidentiality protection, data integrity protection, data filtering, malware/virus detection and data cleaning, security protection at the edge of network slice, slice isolation));
- to decide whether this request for the allocation of resources for a network slice with security requirements is to be assigned to an existing network slice instance or whether a new network slice instance is to be created, after checking the existing active network slice instances from the *NS instance inventory* (i.e., to check if there is an existing network slice instance in the *NS instance inventory* which can be reused). Also, checking if it can satisfy the security requirements of the requested network slice service. That is to say, a new network slice instance is to be created if the existing active network slice instance does not satisfy the security requirements;

- to obtain the security status of the NSSI from the supporting security functionality of the NSS instance from the *NSS security data analysis*;
- to support the checking of the security requirements whether the requested allocated resources for the network slice are satisfied by the allocated network slice instance.

The *NS resource module with security* is an improved logical function with the capabilities of extending the network slice resource model to reflect security requirements of the requested network slice service, for example, adding one static parameter on security, i.e., security profile(s) (e.g., data confidentiality protection, data integrity protection, data filtering, malware/virus detection and data cleaning, security protection at the edge of network slice and slice isolation).

The *NS security management* is a new logical function introduced in this Recommendation with the capabilities of reflecting security requirements of the requested network slice service into a network slice security policy, which will be provisioned in the *NSS security management* and also providing security status of network slice instance together with the *NS security data analysis*.

The *NS security monitoring*, which consists of the *NS security data collection* and the *NS security data analytics*, is to ensure that the security SLAs of network slices are consistently conformed to.

- The *NS security data collection* is a new logical function introduced in this Recommendation with the capabilities of collecting security policy enforcement status on network data (e.g., service, network slice, NSS, network functions related data, security data, isolation data) to support the checking if security requirements for the requested network slice services are satisfied or not and detecting security events/incidents.
- The *NS security data analytics* is a new logical function introduced in this Recommendation with the capabilities of utilizing the collected network data on security policy enforcement status to perform analytics for an optimum network slice security assurance.

8.2 Security capabilities of NSS management and orchestration

The new logical function *NSS authentication & authorization* as the OAuth 2.0 authorization server supports all the logical functions of the *NSS management and orchestration* mutually authenticating each other based on the certificate [IETF RFC 4306] [IETF RFC 5246] and validating whether a requested logical function is authorized to request a given service(s) based on OAuth [IETF RFC 6749]. Integrity protection and confidentiality protection for data transport over the service-based interfaces for the logical functions of the *NSS management and orchestration* are based on TLSv1.2 [IETF RFC 5246] and [b-ITU-T X.1811] to make the system quantum safe.

The new logical function *NSS authentication and authorization* has the following capabilities to authenticate the *NFV-MANO/NFM/TNC* based on the certificate [IETF RFC 4306] [IETF RFC 5246] and authorize the *NFV-MANO/NFM/TNC* based on the ACL [IETF RFC 4314] [b-IETF RFC 4949] when requesting the allocated resources for NSS.

The *NSS orchestration with security* is an improved logical function, which includes one or more logical functions such as security orchestration, isolation management, FW management, and so on. In order to simplify the security reference architecture, only one logical function *NSS orchestration with security* is shown in Figure 8-1. The *NSS orchestration with security* has the following security capabilities:

- to receive the request for allocating resources for a NSS with security profile(s) from the *NS orchestration with security*;
- to map the requested NSS with security profile(s) to an appropriate resource module of the *NSS resource module with security* (e.g., network slice profile(s), …, subnet security profile(s));
- to decide whether this request for the allocation of resources for the NSS is to be assigned to an existing NSSI or whether a new NSSI is to be created, after checking the existing active

NSSIs from the *NSS instance inventory* (i.e., to check if there is an existing NSSI in the *NSS instance inventory* which can be reused). Also, checking if it can satisfy the security requirements of the requested NSS. That is to say, a new NSSI is to be created if the existing active NSSI does not satisfy the security requirements;

- to obtain the security status of a network service instance from the logical function *NFV security manager* in the virtualization case;
- to support the checking of the security requirements whether the requested allocated resources for the NSS are satisfied by the NSSI.

The *NSS resource module with security* is an improved logical function with the capabilities of extending the NSS resource model to satisfy security requirements of the requested NSS, for example, adding one static parameter on security, i.e., security profile(s).

The *NSS security management* is a new logical function introduced in this Recommendation with the capabilities of setting a network slice security policy to the NSS security controlling which security requirements will be provisioned in the logical function *NFV security manager* in the virtualization case, and also providing the security status of the NSSI together with the *NSS security data analysis*.

The *NSS security monitoring*, which consists of the *NSS security data collection* and the *NSS security data analytics*, is to check that the security SLAs of NSS are consistently conformed to.

- The *NSS security data collection* is a new logical function introduced in this Recommendation with the capabilities of collecting security policy enforcement status on network data (e.g., network slice, NSS, network functions related data, security data, isolation data) to support the checking if the security requirements for the requested NSS are satisfied or not.
- The *NSS security data analytics* is a new logical function introduced in this Recommendation with the capability of utilizing the collected network data on the security policy enforcement status to perform analytics for an optimum NSS security assurance.

The security function manager, specified in [ETSI GS NFV-SEC 013], is a specific type of security element manager to manage security functions.

The NSS on security (NSS_security, like RAN NSS and CN NSS) is a new type of NSSs. NSS_security consists of security SFCs to provide customized security services such as network attacks detection and automatic response, virus detection and data cleaning and isolation of data transport.

An instance of NSS_security can be created with the assistance of the logical function *security service catalogue* in the *NFV-MANO* given in Figure 8-1 in the virtualization case. For the creation of security SFCs, see [ITU-T X.1045] [b-Hu].

8.3 Security capabilities of service-based interfaces for logical functions

The logical functions of the *NS management and orchestration* and the *NSS management and orchestration* communicate with each other over the service-based interfaces.

The logical functions mutually authenticate each other based on the certificate defined in [IETF RFC 4306] [IETF RFC 5246]. The logical functions validate whether a requesting logical function is authorized to request a given service(s) based on OAuth [IETF RFC 6749]. Integrity protection and confidentiality protection for data transport over the service-based interfaces for the logical functions of the *NSS management and orchestration* are based on TLSv1.2 [IETF RFC 5246].

8.4 Security capabilities of an interface between *NSS management and orchestration* and *NFV-MANO/NFM/TNC*

It is recommended that TLSv1.2 [IETF RFC 5246] or the IPSec protocols ([IETF RFC 4301], [IETF RFC 4303], [b-IETF RFC 4835]) are implemented and deployed in the *NSS management and orchestration* and the *NFV-MANO/NFM/TNC* to provide mutual authentication between them, as well as to provide confidentiality protection and integrity protection for data transport between them.

It is recommended that whitelist/blacklist or ACL [IETF RFC 4314] [b-IETF RFC 4949] or [b-IETF RFC 5782] [b-IETF RFC 5851] be used to provide authorization for the *NSS management and orchestration* to access the *NFV-MANO/NFM/TNC*.

9 Automation and assurance of end-to-end network slice with customized security capabilities

Based on the security reference architecture for a network slice MANO in Figure 8-1, the automatic creation of an E2E network slice instance with customized security capabilities (e.g., fine-grained slice isolation, security protection at the edge of NSS domains) is described in clauses 9.1 and 9.2. Moreover, it also describes monitoring the network slice instance running status to check whether the requested security requirements are consistently met.

9.1 End-to-end network slice isolated with fine-grained slice isolation policy

E2E network slicing is a general concept that spans network domains, such as access network (AN) domain, CN domain and TN domain. With network slicing, network resources can be shared among different tenants/industries and consequently, network resource utilization can be improved. However, how to provide E2E slice isolation for a network slice is a big problem.

Figure 9-1 shows an IMT-2020 network slice isolated with a fine-grained E2E slice isolation policy, which is enforced in IMT-2020 RAN NSS, TN NSS and IMT-2020 CN NSS.

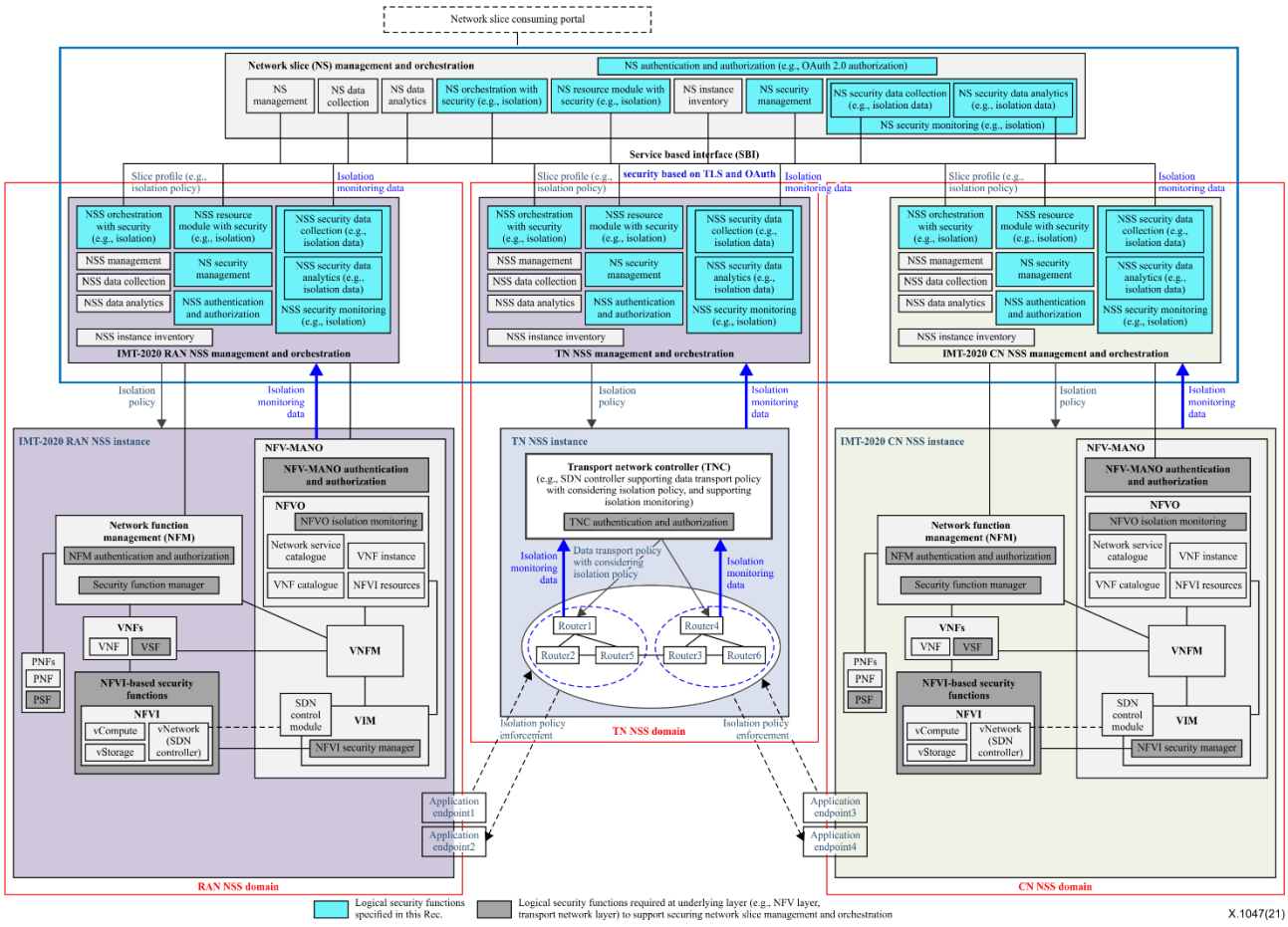

Figure 9-1 – IMT-2020 network slice isolated with a fine-grained end-to-end slice isolation policy

In this Recommendation, isolation is considered as one of the security capabilities/features for a network slice. Figure 9-1 shows applying the security reference architecture in Figure 8-1 to providing an E2E slice isolation for an IMT-2020 network slice.

In order to provide an IMT-2020 network slice isolated with a fine-grained E2E slice isolation policy, the capability of the *NFV-MANO* in the IMT-2020 RAN/CN NSS domain and the *TNC (transport network controller)* in the TN NSS domain is improved, and the corresponding improvements are described in Annexes B.4 and C.2, respectively.

9.1.1 Fine-grained end-to-end network slice isolation planned or orchestrated during network slice instance creation

According to Figure 9-1, the procedures of a fine-grained E2E network slice isolation planned or orchestrated during a network slice instance (NSI) creation is outlined as follows.

1) The logical function *NS orchestration with security (e.g., isolation)* receives a request from the *network slice consuming portal* to create an E2E network slice instance for a service provider (e.g., financial service provider, IoT service provider, gaming service provider, healthcare service provider), and then gets to know the slice profile together with the slice isolation policy (e.g., "no isolation", "physical isolation", "logical isolation", etc.) from the service profile.

2) Based on the derived slice profile together with the slice isolation policy, the logical function *NS orchestration with security (e.g., isolation)* selects an E2E network slice module from the *NS resource module with security (e.g., isolation)*, and checks if there is an existing network slice instance in the *NS instance inventory* satisfying the requirements, especially the slice

isolation policy. If yes, the existing network slice instance is reused. Otherwise, the logical function *NS orchestration with security (e.g., isolation)* calls RAN&TN&CN NSS separately to create NSSs. The logical function of *NS orchestration with security (e.g., isolation)* also breaks down the E2E network slice isolation policy to separate slice isolation policy for each NSS domain.

3) After receiving the request to create NSSs with the slice isolation policy, RAN/TN/CN NSS domains take the following actions separately:

   a) TN NSS domain: after receiving a request to create a TN NSS with a slice isolation policy and after successful mutual authentication between *NS orchestration with security (e.g., isolation)* and *TN NSS orchestration with security (e.g., isolation)*, the following actions will be taken.

      i) The *TN NSS orchestration with security (e.g., isolation)* maps the slice isolation policy to the network resource isolation policy (e.g., no isolation, physical network function isolation, logical network function isolation, physical network link isolation, logical/virtual network link isolation, etc.) and the traffic isolation policy (e.g., no isolation, service type isolation, security protection level isolation, data type isolation, video type isolation, etc.). It further maps the network resource isolation policy and the traffic isolation policy to the TN resource allocation policy (e.g., standard/undifferentiated isolation, dedicated HW for switch/router, dedicated software for switch/router, logical isolated vSwitch/vRouter, etc.) and data traffic forward policy (e.g., standard/undifferentiated isolation, IPSec related rules, access control/filter rules, DSCP (differentiated services code point) rules, forward rules in the flow table, etc.) respectively. The detailed mapping is shown in Annex C.3.

      ii) Based on the derived TN resource allocation policy and the data traffic forward policy, the logical function of the *TN NSS orchestration with security (e.g., isolation)* selects a NSS module from the *TN NSS resource module with security (e.g., isolation)* and checks if there is an existing TN NSS instance (e.g., virtual local area network (VLAN)) in the *TN NSS instance inventory* satisfying the requirements, especially the slice isolation policy. If yes, the existing TN NSS instance for example VLAN identifier (ID) is reused and the S-NSSAI is mapped to the corresponding VLAN ID. The mapping between S-NSSAI and VLAN ID is sent to the *TNC (transport network controller)* and further configured to the corresponding router/switch. Otherwise, the logical function *TN NSS orchestration with security (e.g., isolation)* requests the *TNC (transport network controller)* to create a new TN NSS instance (e.g., VLAN) according to the TN resource allocation policy and the data traffic forward policy, and then maps S-NSSAI to the newly created VLAN ID. After that, the mapping between S-NSSAI and VLAI ID is sent to the *TNC* and is further configured to the corresponding router/switch. This newly created TN NSS instance is added into the *TN NSS instance inventory*.

      iii) *TN NSS orchestration with security (e.g., isolation)* checks if the TN slice isolation policy for the TN NSS, including the network resource isolation policy and the traffic isolation policy, has any contradiction/confliction with other network slices or NSSs that share the same isolation policy. If yes, the *TN NSS orchestration with security (e.g., isolation)* updates the newly created TN NSS with a new/updated resource allocation policy or a data traffic forward policy to remove the contradiction/confliction.

      iv) The TN NSS orchestration with security (e.g., isolation) responds to the logical function NS orchestration with security (e.g., isolation) and then the requested TN NSS is created.

b) RAN/CN NSS domain: after receiving a request to create a RAN/CN NSS with slice isolation policy and after successful mutual authentication between *NS orchestration with security (e.g., isolation)* and *RAN/CN NSS orchestration with security (e.g., isolation)*, the following actions will be taken.

NOTE – As for isolation consideration, RAN/CN NSS domains take similar actions which are described together as follows.

i) The *RAN/CN NSS orchestration with security (e.g., isolation)* maps the slice isolation policy to the network resource isolation policy, application level isolation policy and the traffic isolation policy, and furthermore maps the network resource isolation policy, application level isolation policy and the traffic isolation policy to RAN/CN resource allocation policy, application level policy and the data traffic forward policy, in the same way as the *TN NSS orchestration with security (e.g., isolation)* does in the above step 3) a). The mapping between the traffic isolation policy and the data traffic forward policy in RAN/CN NSS domain can refer to the corresponding mapping of the TN NSS domain in the above step 3) a). The mapping between application level isolation policy and application level policy is sent to the *NFM* of the RAN/CN NSS domain. And then the *NFM* of the RAN/CN NSS domain configures the network functions according to the received application level policy. However, the mapping between network resource isolation policy and access/core network resource allocation policy in RAN/CN NSS domain is much more complicated than that of the TN NSS domain. According to the isolation relevant information elements of the network service/VNF/PNF in Annex B.5, network resource isolation policy mapped to the access/core network resource allocation policy in the RAN/CN NSS domain is summarized as follows:

- physical isolation of the network resource isolation policy is mapped to the access/core network resource allocation policy which comprises one or more dedicated 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 network resource isolation policy is mapped to access/core network resource allocation policy which comprises one or more 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.

ii) Based on the derived access/core network resource allocation policy and the data traffic forward policy, the logical function *RAN/CN NSS orchestration with security (e.g., isolation)* selects a NSS module from the *RAN/CN NSS resource module with security (e.g., isolation)* and checks if there is an existing RAN/CN NSS instance in the *RAN/CN NSS instance inventory* satisfying the requirements especially, the slice isolation policy. If yes, the existing RAN/CN NSS instance (e.g., the chain of one or more network services) is reused and the S-NSSAI is mapped to the corresponding network services. Otherwise, the logical function *RAN/CN NSS orchestration with security (e.g., isolation)* requests the *NFV-MANO* to create one or more network services according to the access/core network resource allocation policy and the data traffic forward policy, and then maps the S-NSSAI to the newly created network services. The *NFV-MANO* creates one or more network services by chaining a set of isolation functions or network functions with isolation capabilities according to Annex B and Annex C. In this way, the requested RAN/CN NSS instance satisfying the isolation policy is created and added into the *RAN/CN NSS instance inventory*.

Moreover, the *NFM* of RAN/CN NSS domain configures the network functions according to the received application level policy.

iii) *RAN/CN NSS orchestration with security (e.g., isolation)* checks if the RAN/CN slice isolation policy for the access/core network NSS, including the network resource isolation policy and the traffic isolation policy, has contradiction/confliction with other network slices or NSSs that share the same isolation policy. If yes, the *RAN/CN NSS orchestration with security (e.g., isolation)* updates the newly created access/core network NSS instance with the new/updated resource allocation policy or the data traffic forward policy to remove the contradiction/confliction.

iv) The *RAN/CN NSS orchestration with security (e.g., isolation)* together with the *NFM* responds to the logical function *NS orchestration with security (e.g., isolation)* and then the requested access/core network NSS is created.

4) After receiving the confirmation that the NSSs have been created from the RAN&TN&CN NSS domains, the logical function *NS orchestration with security (e.g., isolation)* creates a network slice instance comprising of RAN&TN&CN NSS instances. It responds to the *network slice consuming portal* that the requested E2E network slice instance is created with the isolation requirements. The newly created network slice instance is then added into the *NS instance inventory*.

9.1.2 Fine-grained end-to-end network slice isolation monitored during network slice instance running

According to Figure 9-1, the procedures of a fine-grained E2E network slice isolation monitored during NSI running are outlined as follows.

1) The logical function of the *NS security monitoring (e.g., isolation monitoring)* receives a request to monitor the isolation status of the IMT-2020 network slice instance and to check if the E2E network slice isolation policy is enforced correctly or not.

2) The logical function of the *NS security monitoring (e.g., isolation monitoring)* calls the *NSS security monitoring (e.g., isolation monitoring)* of the RAN&TN&CN NSS domains separately to collect the isolation monitoring data from the relevant NSS instances which constitute the IMT-2020 network slice instance.

3) After receiving the request of collecting the isolation data, RAN/TN/CN NSS domains takes the following actions separately:

   a) TN NSS domain: after successful mutual authentication between the NS security monitoring (e.g., isolation monitoring) and the TN NSS security monitoring (e.g., isolation monitoring), the TN NSS security monitoring (e.g., isolation monitoring) collects the isolation monitoring data from the transport network controller (TNC) which is further then collected from the routers or switches according to the TN network resource allocation policy and the data traffic forward policy. It then analyses the collected isolation monitoring data to check/verify if the isolation policies enforced among the TN NSS domains are correct or not, and finally sends the corresponding analysis result (maybe together with the origin isolation monitoring data) back to the NS security monitoring (e.g., isolation monitoring). The TN NSS security monitoring (e.g., isolation monitoring) triggers the TN NSS security management to reconfigure or the TN NSS orchestration with security to re-orchestrate the TN NSS instance to comply with the isolation policies if the isolation policies enforced in the TN NSS domain are incorrect, inconsistent or conflicted.

   b) RAN/CN NSS domain: after successful mutual authentication between the NS security monitoring (e.g., isolation monitoring) and the RAN/CN NSS security monitoring (e.g., isolation monitoring), the RAN/CN NSS security monitoring (e.g., isolation monitoring) collects the isolation monitoring data from the NFM and the network function

virtualization and orchestration (NFVO) isolation monitoring of the NFV-MANO which is then further collected from the virtual network function management (VNFM) and virtual infrastructure management (VIM), according to the RAN/CN network resource allocation policy and the data traffic forward policy. It then analyses the collected isolation monitoring data to check/verify if the isolation policies enforced among the RAN/CN NSS domains are correct or not, and finally sends the corresponding analysis result (maybe together with the origin isolation monitoring data) back to the NS security monitoring (e.g., isolation monitoring). The RAN/CN NSS security monitoring (e.g., isolation monitoring) triggers the RAN/CN NSS security management to reconfigure or the RAN/CN NSS orchestration with security to re-orchestrate RAN/CN NSS instance to comply with the isolation policies if the isolation policies are enforced in the RAN/CN NSS domain are incorrect, inconsistent or conflicted.

4) After receiving the isolation monitoring data from the RAN&TN&CN NSS domains, the logical function *NS security monitoring (e.g., isolation monitoring)* checks/verifies if the E2E network slice isolation policy is enforced correctly or not. If yes, the *NS security monitoring (e.g., isolation monitoring)* confirms with the *network slice consuming portal* that the E2E isolation policies of the network slice instance are enforced correctly. Otherwise, the *NS security monitoring (e.g., isolation monitoring)* sends alarms to the *Network slice consuming portal* and triggers the *NS security management* to reconfigure or the *NS orchestration with security* to re-orchestrate network slice instance to comply with the E2E isolation policies.

9.2 End-to-end network slice with prevention from network attacks at the edge of NSS domains

Heterogeneous network slice customers from vertical industries sharing the same mobile network infrastructure via network slicing will require different levels of security protection. To provide secure inter- and intra- network slice communication as well as the prevention of attacks at the edge of network slices (e.g., to provide secure internet access), will be a major requirement from mobile network operators (MNOs) or vertical industries. Therefore, it is important to protect a network slice from network attacks by deploying FWs at the edge e.g., protect the N6 interface by deploying an FW at the edge of the core network.

For different network slice consumers, the policies/rules for data filtering in the FWs (e.g., at the edge of the core network) might be different and can be changed dynamically. Thus, it is important to dynamically configure security policies/rules for FWs, in order to support a quick response to network attacks automatically. However, the FW solutions deployed in the NSSIs (NSSIs) e.g., in CN NSSI or even at the user plane function should not be managed separately. Instead, FW solutions in each NSSI must have knowledge of the security status of other NSSIs (e.g., AN NSSI, TN NSSI) because the data filtering policy/rule in the FW might be inconsistent with or even conflicted with the policies/rules of other NSSIs. Furthermore, the FW solution should be aware of security considerations in the service profile of the network slice.

This Recommendation is drawn up to describe how to prevent network attacks at the edge of NSS domains of a network slice by deploying and running security functions (e.g., FWs) from a holistic point of view, e.g., holistic view regarding link/edge protection. In this way, the network attacks to CN NSSI via the interface N6 as well as network attacks to other NSSIs (e.g., AN NSSI, TN NSSI) can be prevented with high efficiency.

Figure 9-2 shows the applying of the security reference architecture in Figure 8-1 to create an IMT-2020 network slice instance, that has the capability to prevent network attacks by deploying FWs at the edge of NSS domains.

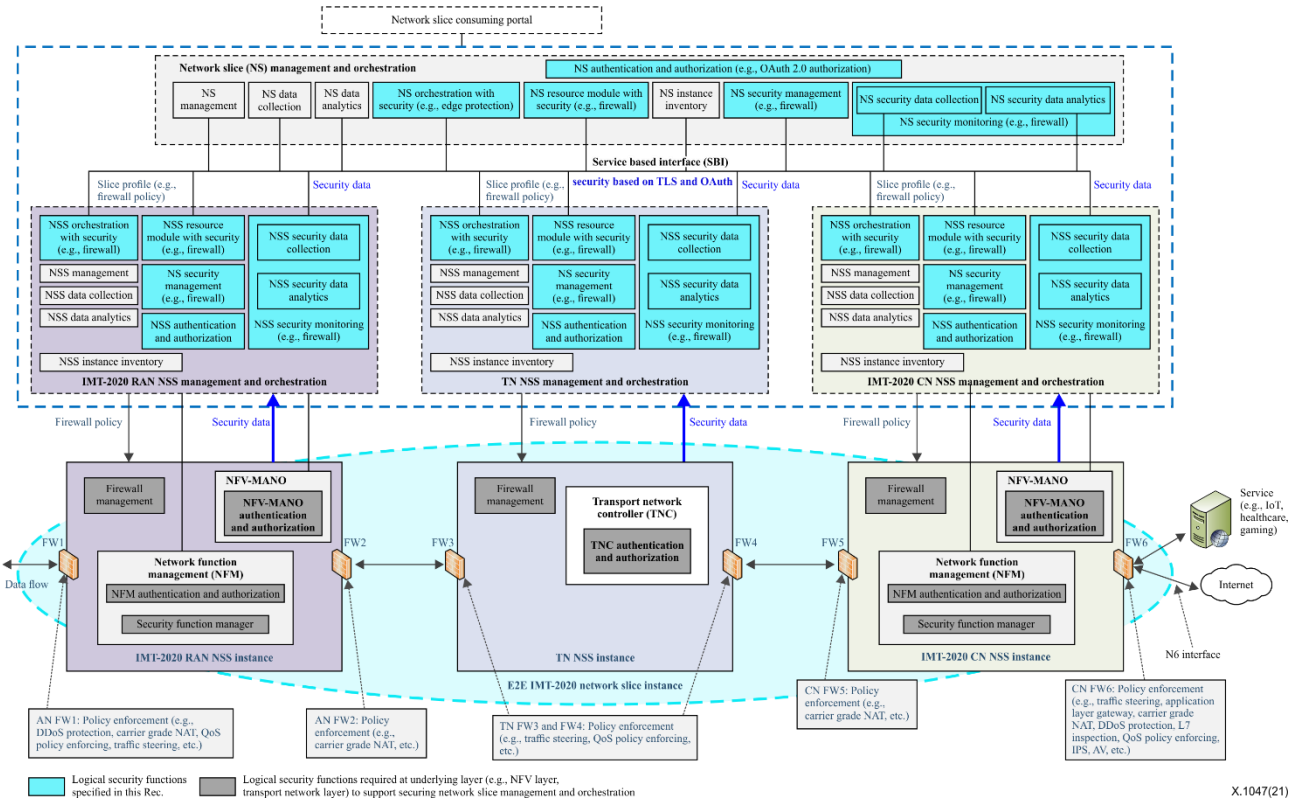

Figure 9-2 – End-to-end IMT-2020 network slice with prevention from network attacks at the edge of the NSS domains

In order to create an IMT-2020 network slice with prevention from network attacks at the edge of the NSS domains, the capability of the RAN&CN&TN NSS domains is improved to support the FW management as shown in Figure 9-2.

9.2.1 Network attacks prevention at the edge of NSS domains planned/orchestrated during the network slice instance creation

According to Figure 9-2, the procedures of network attacks prevention at the edge of the NSS domains planned/orchestrated during the NSI creation are outlined as follows.

1) The logical function *NS orchestration with security (e.g., edge protection)* receives a request from the *Network slice consuming portal* to create an E2E IMT-2020 network slice instance for a service provider (e.g., financial service provider, IoT service provider, gaming service provider, healthcare service provider), and gets to know the slice profile with security attributes (e.g., security protection at the edge of network slice) from the service profile (e.g., data speed, quality, latency and security).

2) Based on the derived slice profile with security attributes (e.g., security protection at the edge of network slice), the *NS orchestration with security (e.g., firewall)* selects a network slice module from the *NS resource module with security (e.g., firewall)* by deploying FWs at the edge of RAN & TN & CN NSS domains to prevent network attacks. The *NS orchestration with security (e.g., firewall)* checks if there is an existing network slice instance in the *NS instance inventory* satisfying the requirements for preventing network attacks at the edge of NSS domains. If yes, the existing network slice instance is reused. Otherwise, the *NS orchestration with security (e.g., firewall)* determines data filtering policies for the FWs at the edge of each NSS domain as follows.

   - RAN NSS domain: DDoS protection, carrier grade network address translation (NAT), QoS policy enforcing, L7 inspection, traffic steering, etc.

- TN NSS domain: Traffic steering, QoS policy enforcing, etc.
- CN NSS domain: Traffic steering, application layer gateway, carrier grade NAT, DDoS protection, L7 inspection, QoS policy enforcing, etc.

3) The *NS orchestration with security (e.g., FW)* sends the requests to the RAN&TN&CN NSS domain separately to create NSSs according to the corresponding FW policies as above.

4) After receiving the request to create a RAN/TN/CN NSSIs with the FW policy and after successful mutual authentication between *NS orchestration with security (e.g., firewall)* and the *RAN/TN/CN NSS orchestration with security (e.g., firewall),* the following actions will be taken.

- CN NSS domain: based on the received FW policy for the CN NSS domain, the *CN NSS orchestration with security (e.g., firewall)* selects a NSS module from the *CN NSS resource module with security (e.g., firewall)* and checks if there is an existing CN NSS instance satisfying the FW policy in the *CN NSS instance inventory*. If yes, the existing CN NSS instance is reused. Otherwise, the *CN NSS orchestration with security (e.g., firewall)* requests the *NFV-MANO* to create a new one according to the FW policy. The *NFV-MANO* creates one or more network services by chaining a set of FWs or network functions with the FW filtering capabilities according to Annex B and Annex C. For example, security functions (i.e., FW5 and FW6) in Figure 9-2 are deployed at the edge of the CN NSS instance for the requested IMT-2020 network slice instance. The *Firewall management* in the CN NSS instance is triggered to configure the policies for FW5 (e.g., carrier grade NAT) and FW6 (e.g., traffic steering, application layer gateway, carrier grade NAT, DDoS protection, L7 inspection, QoS policy enforcing, IPS and antivirus). In this way, the requested CN NSS instance satisfying the FW policy is created and added into the *CN NSS instance inventory*. During the creation of the CN NSS instance by deploying security functions (e.g., FWs) at the edge, the *CN NSS orchestration with security (e.g., Firewall)* should confirm that there are no side effects on the other network slices/NSSIs if the security functions (e.g., FWs) of the CN NSS instance are shared by multiple network slices/NSSIs. Therefore, security policies (e.g., FW policies) per slice are maintained to enable checking if the data filter policy/rule in the FW is consistent with or conflicted with the data filter policy/rule applied for other NSSIs. If the data filter policy/rule of one NSSI is inconsistent with or conflicted with the policy/rule of other NSSIs, one or more dedicated physical or virtualized security functions (e.g., FW or virtual FW) are deployed for this newly created NSSI.
- TN&RAN NSS domain: in the same way of creating CN NSS instance, TN NSS instance is created by deploying FW3 (e.g., traffic steering, QoS policy enforcing, etc.) and FW4 (e.g., traffic steering, QoS policy enforcing, etc.) at the edge of TN NSSI, and the RAN NSS instance is created by deploying FW1(e.g., DDoS protection, carrier grade NAT, QoS policy enforcing and traffic steering) and FW2 (e.g., carrier grade NAT) at the edge of the RAN NSSI. The newly created TN&RAN NSS instances are added into the *TN&RAN NSS instance inventory* respectively.

5) The RAN&TN&CN NSS orchestration with security (e.g., firewall) responds to the NS orchestration with security (e.g., firewall) and then the requested RAN/TN/CN NSS instance is created.

6) After receiving the response that the NSSs have been created from the RAN&TN&CN NSS domains, the *NS orchestration with security (e.g., firewall)* creates a network slice instance comprising RAN&TN&CN NSS instances. It then responds to the *network slice consuming portal* that the requested E2E network slice instance is created for preventing the network attacks at the edge. The newly created network slice instance is then added into the *NS instance inventory.*

In this way, this requested IMT-2020 network slice instance has the capability to prevent network attacks for inter-NS and intra-NS communications as well as to prevent network attacks at the edge of the network slice (e.g., the interface N6 between CN NSS domain and the internet).

9.2.2 Network attacks prevention at edge, enforced and monitored during network slice instance running

As in Figure 9-2, security policies are enforced by six FWs running at the edge of RAN&TN&CN NSSIs to prevent network attacks during an E2E IMT-2020 network slice instance running. In order to monitor the security status of this IMT-2020 network slice instance, security data is collected and analysed. The procedures of monitoring network attacks prevention at the edge of NSS domains during NSI running can refer to clause 9.1.2. Based on the security data monitoring and analytics, some new network attacks can also be detected.

When new network attacks are detected at the edge of NSS instances, the *firewall management* of the NSS instances will be notified to take some actions to prevent these new network attacks. For example, when new attacks are detected through the data flow between the CN NSS domain and the internet in Figure 9-2, the *firewall management* of the CN NSS instance will be notified to take some actions as follows:

- The *firewall management* of the CN NSS instance checks its FW policy and if it finds that the FW policy cannot prevent the detected new network attacks, it then reconfigures the FW6 with a new/additional FW policy. After that, FW6 enforces the latest configured policy to prevent those new network attacks.
- The *firewall management* of the CN NSS instance checks its FW policy and if it finds that the existing FW policy cannot prevent the detected new network attacks it triggers the deployment of a new FW to mitigate the risk. In some situations, the *firewall management* of the CN NSS instance does not know how to prevent these new network attacks. During this time, the *firewall management* of the CN NSS instance sends alarms to the *CN NSS security management (e.g., firewall)*. The *CN NSS security management (e.g., firewall)* might know how to prevent these new network attacks, so it then triggers the *CN NSS orchestration with security (e.g., firewall)* to re-allocate the security functions (e.g., dedicated FWs) to cooperate with the FW FW6. Even more, it is also possible to trigger the *NS orchestration with security (e.g., firewall)* to re-allocate network resources and update the security requirements on the associated NSSIs (e.g., TN NSSI) to cooperate with the FW FW6 in CN NSS. That means, this IMT-2020 network slice instance is updated.

Sometimes, the *firewall management* of the CN NSS instance finds that the existing FW policy in FW6 is enough to prevent the network attacks at the edge of the CN NSS instance. However, the data rate increases suddenly at the edge of the CN NSS instance and the capacity of FW6 is not enough to perform data filtering. During this time, the *firewall management* of the CN NSS instance triggers the *CN NSS security management (e.g., firewall)* and the *CN NSS orchestration with security (e.g., firewall)* to deploy additional firewalls at the edge of the CN NSS instance and cooperate with the FW FW6.

9.2.3 Creating a separate security NSS instance at the edge of NSS domains

There may be a special scenario. An enterprise requests a separate network slice instance for its corporate services. It is assumed that base stations are deployed within the office park and the radio access is secure. It is also assumed that the communications between the RAN NSS instance, TN NSS instance and the CN NSS instance are secure. However, the communication between CN NSS instance and the internet/services is not secure when the users access the internet or the services. Therefore, it is very important to prevent network attacks at the edge of this network slice instance.

Figure 9-3 shows the creation of a separate security NSS instance at the edge of network slice instance (e.g., at the edge of CN NSS instance) to prevent network attacks from different services and different network layers.

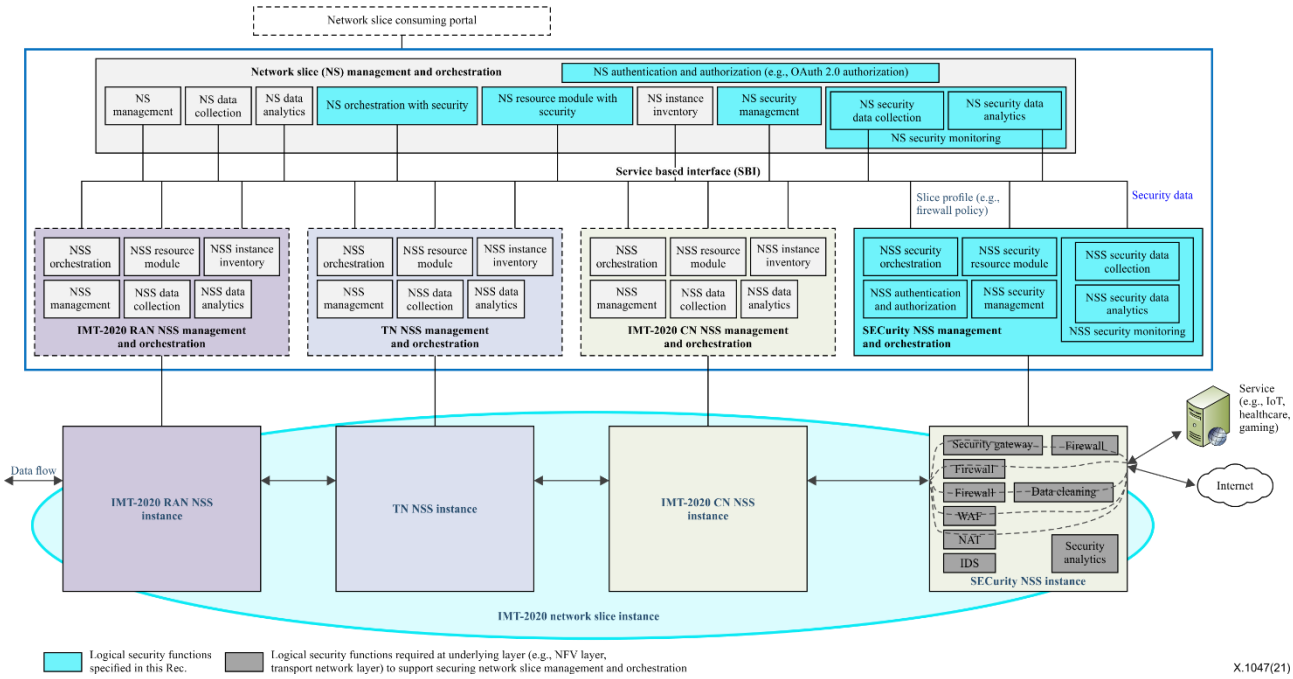

Figure 9-3 – A separate security NSS instance at the edge of a network slice instance to prevent network attacks

The security (SEC) NSS instance in Figure 9-3 is an NSSI that is responsible for detecting network attacks and preventing them automatically at the edge of a network slice instance. The SEC NSS instance can be created and kept at the edge of each NSS domain to prevent network attacks.

When requesting to create RAN&TN&CN NSS instances, *NS orchestration with security (e.g., firewall)* also requests the *SEC NSS security orchestration* to create an SEC NSS instance to protect network attacks at the edge of the network slice instance with security requirements included in the service/slice profile. The *SEC NSS security orchestration* creates or reuses a security NSS instance to satisfy the security requirement. For example, the *SEC NSS security management* breaks down the requirement to security functions (e.g., FWs) and policies of FWs, then deploys FWs and configures the corresponding policies on them.

During runtime, the FW proceeds the ingress/egress traffics based on the policies and reports the FW status and events. The *SEC NSS security orchestration* triggers to update the scale FW based on security requirement change, network capacity change or security posture changes, etc.

A SEC NSS instance has the capability to prevent network attacks from different services and different network layers, which is shown in Figure 9-3. For example, the *SEC NSS security orchestration* deploys and configures security functions "security gateway" and "firewall" for service A, security function "firewall" for service B and security function "web application firewall" for service C (e.g., internet services).

10 Tamper-proof and access-controlled network slice management data

According to Figure 6-1, a network slice instance is composed of one or more active NSSIs, and a NSSI is composed of a set of managed run-time network functions or TNs. That means, there are some participants/partners (e.g., network slice provider, NSS provider, TN provider, software

provider, HW provider) who collaborate and cooperate to provide customized network slices for a variety of vertical industries.

During network slice instance running, vertical industries periodically check's the network slice management data (e.g., performance data, fault data, configuration data, security data) to ensure that the performance or availability of network slices complies with the SLA. If the service performance is limited or the network slice is not available, all the participants/partners can turn to the network slice management data to find out what and how it happened and who is responsible for this issue.

The participants/partners at fault may be motivated to tamper network slice management data (by adding, removing, or manipulating a part of the network slice management data or the entire network slice management data) in order to hide their fault. The participant/partners at fault may also try to tamper the network slice management data and fabricate a scenario in which another participant/partner becomes the main reason behind the failure and, therefore, responsible for the caused damage. Given that the network slice management data is generated and stored in each participant's/partner's own data centre, there are many tampering possibilities.

Therefore, it is very important to make network slice management data (especially for SLA monitoring) tamper-proof, traceable, verifiable, and immutable [b-TM Forum-Blockchain] [b-TM Forum-TR 279] [b-Bihannic] [b-TM Forum-Accenture] [b-NGMN-5G] [b-EU-INSPIRE-5Gplus-D2.1] [b-ITU-T X.1402]. In this way, trust is established among the participants/partners who collaborate and cooperate to provide customized network slices for a variety of vertical industries. Furthermore, it is possible to track the participants/partners who are responsible for the issue when the network slice is not available, or its performance is limited.

Configuration data is sensitive since a skilled attacker may use a system configuration data to penetrate the network slice system. For example, the attacker may tamper the configuration data via illegal tactics, such as tampering with configuration data during its storage through unauthorized access or tampering with the configuration data during its transportation in plaintext. After that, the attacker may remove the access record from the system log. It is then very difficult to know the identity of the person behind the tampering of the configuration data and the attacks on the network. Hence, it is very important to guarantee that the configuration data is defined/created only by authentic parties and is not modified during transportation. Moreover, it is also important to guarantee that only authorized data consumers can access the network slice management data.

This Recommendation is drawn up to protect the network slice management data, whether at rest, in transit or in use, from being tampered and from having unauthorized access.

10.1 Tamper-proof network slice management data in transit

Network slice management data in transit means relevant data moves from one place to another in the form of packets over the network within one domain or cross domains (e.g., RAN NSS domain, TN NSS domain and CN NSS domain). An attacker may tamper, modify or eavesdrop on the network slice management data in transit. Hence, it is required to protect the network slice management data from being tampered with in transit.

Some available and feasible security methods, such as HTTPS [b-IETF RFC 2818] and TLS [IETF RFC 5246], can be used to provide data confidentiality and data integrity, in order to protect network slice management data from being tampered, modified or eavesdropped in transit.

10.2 Tamper-proof network slice management data at rest

Network slice management data at rest means relevant data can be stored in the files or tables of a database within one domain or cross domains.

Traditionally, there is no need to provide security methods to protect network management data from being tampered since all the network management relevant data is managed within one administrative domain. However, there are some participants/partners (e.g., network slice provider, NSS provider,

TN provider, software provider, HW provider) who collaborate and cooperate to provide customized network slices for a variety of vertical industries. Generally, network slice management data is collected, managed and stored in each administrative domain (e.g., RAN NSS domain, TN NSS domain and CN NSS domain). As mentioned above, participants in a multi-partner context may be motivated to tamper network slice management data to hide their fault and to further avoid the responsibility for paying a fine.

Blockchain technologies are now envisioned as the key enablers to avoid manipulations on the data exchanged and data provenance in such multi-partner context, thanks to a shared, distributed and fault-tolerant database [b-EU-INSPIRE-5Gplus-DLT based solutions in 5G Security] [b-EU-INSPIRE-5Gplus-D5.1]. SLA monitoring based on blockchain can reduce the number of disputes between vendors and service providers [b-TM Forum-Blockchain] [b-TM Forum-TR 279]. Thus, the design of network slices should now integrate the architecture of distributed ledgers that are in charge of the ordering and storing of the network slice management data in a tamper-proof way [b-Bihannic]. One of the feasible security mechanisms, i.e., making network slice management data tamper-proof and traceable based on a distributed ledger technology (DLT) in Annex D, can be used to support the making of the network slice management data tamper-proof at rest.

10.3 Access control for network slice management data in use

Network slice management data in use means that the relevant data can be found in the files or tables of a database within one domain or cross domains (e.g., RAN NSS domain, TN NSS domain and CN NSS domain). An attacker may masquerade as a legitimate user to get, modify or delete a network slice management data or may masquerade as an administrator to get, modify or delete audit logs. Thus, it is required to protect network slice management data from unauthorized access. It is also required to record the identity of who accessed the system, when was the system accessed and what actions have been taken [b-TM Forum-Accenture] [b-NGMN-5G].

Some available and feasible security methods, such as a whitelist/blacklist [b-IETF RFC 5782], ACL [IETF RFC 4314] or an access token [IETF RFC 6749] [b-IETF RFC 7519] can be used to provide data access control in order to protect network slice management data from unauthorized access. To provide non-repudiation of data access in a multi-partner context, a feasible security method in Annex D, i.e., a DLT-based network slice management data storage and access can be used.

Annex A

Security threats to network slice management and orchestration

(This annex forms an integral part of this Recommendation.)

Main security threats to network slice MANO given in Figure 6-1 are described in this annex.

A.1 Security threats to the logical functions of *NS&NSS management and orchestration*

Main security threats to the logical functions of *NS&NSS management and orchestration* are described as follows:

- Spoofing attacks;
- Theft of service;
- Leakage of sensitive information about network slice consumers, such as service requirements, network slice profile, identity information of the consumers, etc.;
- Leakage of sensitive information about NSTs or NSSTs;
- Tampering NSTs or NSSTs;
- Tampering the configuration of the slices or the subnet slices before/at activation or during running time;
- Creating fake network slice instances or NSSIs;
- Compromising/denying access to the slices or the subnet slices;
- Conducting performance and DoS attacks;
- Breaking privacy of customers;
- Deleting/deactivating the slices or the subnet slices;
- Extensive use of network resources and network functions;
- Denial of service attacks and flooding attacks against *NS&NSS management and orchestration* platform;
- Masquerade as a valid *NS&NSS management and orchestration* platform;
- Misconfiguration of *NS&NSS management and orchestration* platform;
- Attacks on OAM and its traffic;
- Tampering network slice management data (e.g., fault/performance/configuration/security data);
- Fraudulent software update/configuration changes;
- Environmental/side-channel attacks against the logical functions of *NS&NSS management and orchestration*.

A.2 Security threats to service-based interfaces for the logical functions of *NS&NSS management and orchestration*

Main security threats to service-based interfaces for the logical functions of the *NS&NSS management and orchestration* are described as follows:

- Leakage of sensitive information about network slice consumers, such as service requirements, network slice profile, identity information of the consumers, etc.;
- Theft of service if authentication/authorization credentials are transferred uncyphered;
- Eavesdropping of sensitive information during transferring;

- Man-in-the-middle (MITM) attacks that actively modify the messages between the logical functions of the *NS&NSS management and orchestration*;
- Lack of availability caused by malformed messages due to unnoticed modifications during transferring;
- Unauthorized modification of information during transferring;
- Loss of control if authentication/authorization credentials are replayed;
- Causing a denial of service situation by successfully forcing the logical function of *NS&NSS management and orchestration* to perform service requests.

A.3 Security threats to the interface between the *NSS management and orchestration* and the *NFV-MANO/NFM/TNC*

The security threats in Annex A.2 are also applied to the interface between the *NSS management and orchestration* and the *NFV-MANO/NFM/TNC*.

Annex B

Capabilities of logical functions at network function virtualization layer to support the network slice management and orchestration

(This annex forms an integral part of this Recommendation.)

This annex describes the capabilities of logical functions at the network function virtualization (NFV) layer, e.g., to support the securing of network slice MANO, creation of a network slice instance with customized security services through security SFCs comprising a set of security functions (e.g., authentication, FW, IDS/IPS) [ITU-T X.1045] [b-Hu] and the monitoring of the network slice instance running status to ensure that security SLAs are consistently conformed to.

B.1 General capabilities of logical functions at the network function virtualization layer

According to Figure 6-1, general capabilities of the logical functions [b-ETSI GS NFV-MAN 001] at the NFV layer are summarized as follows.

- The *NFVO (NFV orchestrator)* is responsible for the orchestration of the NFVI resources across multiple virtual infrastructure managements (VIMs) and the lifecycle management of network services. Network function virtualization and orchestration (NFVO) includes *network service catalogue*, *VNF catalogue*, *NFV instance inventory* and *NFVI resources*.
- The *VNFM (VNF manager)* is responsible for the lifecycle management of VNF instances.
- The *VIM (virtualised infrastructure manager)* is responsible for controlling and managing the NFVI compute, storage and network resources. *SDN control module* including data forward policies may be included into the *VIM*.
- The *NFVI (NFV infrastructure)* is to store the information about the available/reserved/allocated NFVI resources (e.g., vCompute, vStorage, vNetwork) as abstracted by the *VIM*.
- The *VNFs* are virtualized network functions. The *PNFs* are physical network functions.
- The *network service (NS) catalogue* represents the repository of all of the on-boarded network services, supporting the creation and management of the NS deployment templates (network service descriptor (NSD), virtual link descriptor (VLD), and VNF forwarding graph descriptor (VNFFGD) via the interface operations exposed by the NFVO.
- The *VNF catalogue* represents the repository of all of the on-boarded VNF packages, supporting the creation and management of the VNF package (VNF descriptor (VNFD), software images, manifest files, etc.) via the interface operations exposed by the NFVO. Both the NFVO and the virtual network function management (VNFM) can query the VNF catalogue for finding and retrieving a VNFD, to support the different operations (e.g., validation, checking instantiation feasibility.
- The *NFV instances* repository holds information of all VNF instances and network service instances. Each VNF instance is represented by a VNF record, and each NS instance is represented by an NS record. Those records are updated during the lifecycle of the respective instances and reflecting changes resulting from the execution of the NS lifecycle management operations or the VNF lifecycle management operations. This supports the NFVO and the VNFM responsibilities in maintaining the integrity and visibility of the NS or VNF instances, and the relationship between them.
- The *NFVI resources* repository holds information about the available/reserved/allocated NFVI resources as abstracted by the VIM across the operator's infrastructure domains, thus supporting information useful for resources reservation and allocation and monitoring purposes. As such, the NFVI resources repository plays an important role in supporting the

resource orchestration and governance role of the NFVO, by allowing the NFVI reserved/allocated resources to be tracked against the NS and VNF instances associated with the NFVO resources (e.g., number of VMs used by a certain VNF instance at any time during its lifecycle).

B.2 Security requirements for the logical functions at the network function virtualization layer

It is required that the *NFV-MANO* and the *NFM* have the capability to authenticate the *NSS management and orchestration* before the *NSS management and orchestration* requests to create network service instances or collect network data (e.g., network link status, security, QoS, bandwidth, throughput, latency, etc.).

It is required that the *NFV-MANO* and the *NFM* have the capability to authorize the *NSS management and orchestration* before the *NSS management and orchestration* requests to create a network service instance or collect network data (e.g., network link status, security, security, QoS, bandwidth, throughput, latency, etc.).

It is required to have the capability to support integrity protection for data transport via the interface between the *NFV-MANO/NFM* and the *NSS management and orchestration*.

It is required to have the capability to support confidentiality protection for data transport via the interface between the *NFV-MANO/NFM* and the *NSS management and orchestration*.

It is required to have the capability to support replay protection for data transport via the interface between the *NFV-MANO/NFM* and the *NSS management and orchestration*.

It is recommended to have the capability to support integrity protection for the network service catalogue (i.e., network service chain template) during transmission and in storage.

It is recommended to have the capability to support confidentiality protection for the network service catalogue (i.e., network service chain template) during transmission and in storage.

It is required to have the capability to create security SFCs [ITU-T X.1045] [b-Hu] to provide customized security service (e.g., authentication, integrity protection, confidentiality protection, HW isolation, software isolation, anti-DDoS attack, anti-virus and anti-malware software), in order to satisfy the security requirements from the *NSS management and orchestration*.

It is recommended to have the capability to create a separate network service instances to provide customized security services by creating security SFCs comprising of a set of security functions (e.g., authentication, FW, IDS/IPS) [ITU-T X.1045] [b-Hu].

It is recommended to have the capability to evaluate if the network service catalogue (i.e., network service template) can satisfy the security requirements of the requested network service resource from the *NSS management and orchestration*.

It is recommended to have the capability to evaluate if the available, feasible and active network service instances can satisfy the security requirements of the requested network service resource from the *NSS management and orchestration*.

It is required to have the capability to support the isolation between network service instances.

It is required to support integrity of managed services and management functions at the NFV layer.

It is recommended to have the capability for automated attack/incident detection, identification, prevention, and mitigation of network service instances.

It is recommended to have the capability for monitoring and collecting the activities, status, anomalous events of the instances of the VNFs and PNFs.

It is recommended to have the capabilities for analysing the collected data and providing reports on the behaviour of the instances of VNFs and PNFs.

It is recommended to have the capability for storing and retrieving collected data, analysis reports and logging records in the *NFV-MANO* and in the *NFM*.

It is recommended to provide integrity protection for the collected data, analysis reports and logging records stored in the *NFV-MANO* and in the *NFM*.

It is recommended to provide confidentiality protection for the collected data, analysis reports and logging records stored in the *NFV-MANO* and in the *NFM*.

It is required to support integrity protection for management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) stored in the *NFV-MANO* and in the *NFM*.

It is required to support non-repudiation/tamper-proof of management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) stored in the *NFV-MANO* and in the *NFM*.

It is recommended to support confidentiality protection for management data (e.g., fault, configuration, performance, security, and data related to management functions such as logs) stored in the *NFV-MANO* and in the *NFM*.

B.3 Security capabilities of the logical functions at the network function virtualization layer

To provide customized security services by creating security SFCs comprising of a set of security functions (e.g., authentication, FW, IDS/IPS) [ITU-T X.1045] [b-Hu] for the industry verticals, some logical functions of *NFV-MANO/NFM* in Figure 8-1 are improved with security capabilities; and some new logical security functions are introduced in this Recommendation.

The *NFV-MANO authentication and authorization* and the *NFM authentication and authorization* are logical functions introduced in this Recommendation and have the following capabilities: 1) to authenticate the *NSS management and orchestration* based on the certificate [IETF RFC 4306] [IETF RFC 5246]; 2) to authorize the *NSS management and orchestration* to request the allocated resource of the network service based on the certificate [IETF RFC 4306] [IETF RFC 5246].

The *security service catalogue* is a logical function introduced in this Recommendation with the following capabilities: 1) to store all of the on-boarded security services which are security SFCs comprising of a set of security functions (e.g., authentication, FW, IDS/IPS) [ITU-T X.1045] [b-Hu]; 2) to support the creation and management of the security service resource model; 3) to support the creation of the NSSI (i.e., NSS_security).

The *NFV security manager*, specified in [ETSI GS NFV-SEC 013], is a logical function used to manage the security on a network service over its entire lifecycle. The *NFV security manager* and the *NFV-MANO* are improved for creating security SFCs comprising of a set of security functions (e.g., authentication, security gateway, FW, IDS/IPS) [ITU-T X.1045] [b-Hu] to provide customized security services.

The *NFVI security manager*, specified in [ETSI GS NFV-SEC 013], is a logical function used to build and manage the security in NFVI and to support the *NFV security manager* requests for managing the security of the network services in the higher layer.

The *VSF (virtual security function)*, specified in [ETSI GS NFV-SEC 013], is a special type of VNF with tailored security functionality (e.g., authentication, FW, IDS/IPS, virtualized security monitoring functions).

The *VSF catalogue* is a specific type of VNF catalogue specified in [ETSI GS NFV-SEC 013].

The *VSF instance* is a specific type of VNF instance specified in [ETSI GS NFV-SEC 013].

The *NFVI-based security function*, specified in [ETSI GS NFV-SEC 013], is provided by the NFV infrastructure. It includes virtualized security appliances or software security features (e.g., hypervisor-based FWs) and HW-based security appliances/modules/features (e.g., HW security modules, crypto accelerators, or trusted platform modules).

The *PSF (physical security function)*, specified and defined in [ETSI GS NFV-SEC 013], is a conventionally realized security function in the physical part of the hybrid network.

B.4 Isolation capabilities of the logical functions at the network function virtualization layer

To provide an IMT-2020 network slice isolated with a fine-grained E2E slice isolation policy, some logical functions of the *NFV-MANO/NFM* in Figure 9-1 are improved with some isolation capabilities as follows:

- the logical function *NFVO isolation monitoring* of the *NFVO* supports the collection of relevant data isolation in the access/core network and reporting it to the logical function *RAN/CN NSS security monitoring (e.g., isolation monitoring)*.
- NFVO NBI (north-bound interface) is extended to support isolation policies (e.g., NS isolation, virtualized network function isolation, vCompute isolation, vStorage isolation, HW location isolation, security capability isolation, virtual link isolation) for network service to support RAN/CN NSS isolation.
- VNFM NBI is extended to support isolation policies (e.g., VNF component infrastructure isolation, vCompute isolation, vStorage isolation, HW location isolation, security capability isolation, virtual link isolation) for VNF to support the constituent managed function of RAN/CN NSS.
- NFM NBI is extended to support isolation policies such as security capabilities (e.g., authentication, confidentiality, integrity and non-repudiation), location isolation of physical network function, network link isolation, etc.

B.5 Information element of a network service/PNF/VNF related to the network resource isolation policy

According to the descriptor of the network service/PNF/VNF in [b-ETSI GS NFV-IFA 011] [b-ETSI GS NFV-IFA 014] [b-ETSI GR NFV-SEC 009], the information elements related to network resource isolation policy are selected and shown in Figure B.1.

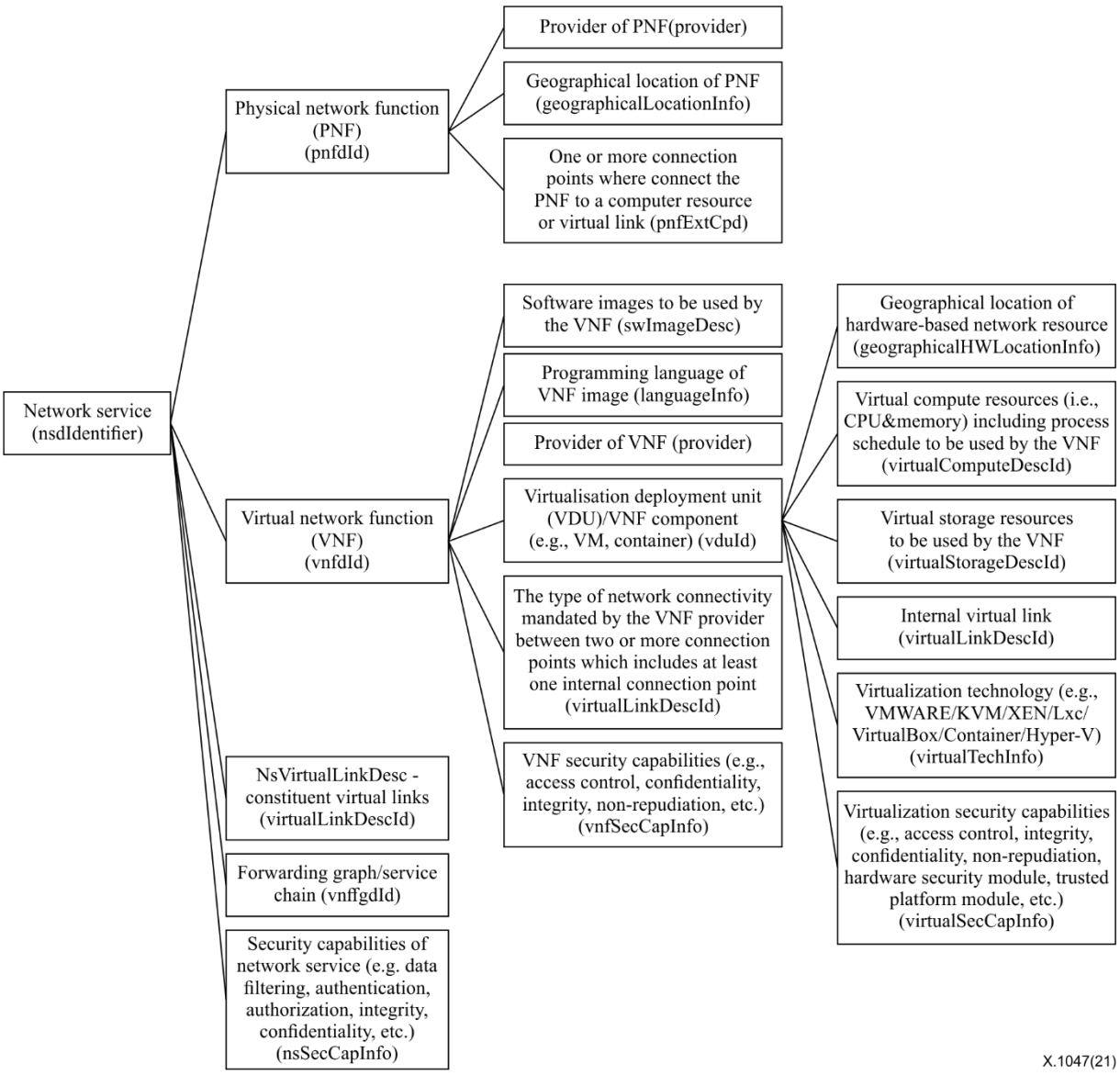

Figure B.1 – Information element of a network service/PNF/VNF related to the network resource isolation policy

Annex C

Capabilities of logical functions at the transport network layer to support network slice management and orchestration

(This annex forms an integral part of this Recommendation.)

This annex describes the capabilities of logical functions at the TN layer to support securing network slice MANO, creating network slice instance with customized security services, monitoring the network slice instance running status to ensure that security SLAs are consistently conformed to, and so on.

C.1 Security capabilities of the logical functions at the transport network layer

In order to provide customized security services for the industry verticals, the logical *transport network controller (TNC)* in Figure 8-1 is improved with security capabilities.

The *TNC authentication and authorization* logical function introduced in this Recommendation has the following capabilities: 1) to authenticate the *NSS management and orchestration* based on the certificate [IETF RFC 4306] [IETF RFC 5246]; 2) to authorize the *NSS management and orchestration* to request the allocated resource for the TN based on the certificate [IETF RFC 4306] [IETF RFC 5246].

C.2 Isolation capabilities of the logical functions at the transport network layer

In order to provide an IMT-2020 network slice isolated with a fine-grained E2E slice isolation policy, the logical *transport network controller (TNC)* in Figure 9-1 is improved with some isolation capabilities as follows:

- to support the creation of a dedicated physical or logical data transport channel for a specific slice or slice group. For example, a tenant requests to create an E2E network slice with physical isolation, the logical function *transport network controller (TNC)* should have the capability to create a dedicated data transport channel along with allocating a dedicated physical router, dedicated physical switches and dedicated physical circuits, as well as to configure the edge router to prevent the data of other S-NSSAIs from being transported through this dedicated physical data transport channel.
- to collect relevant data isolation in the TN and report it to the logical function *TN NSS security monitoring (e.g., isolation monitoring)*.

C.3 Mapping between slice isolation policy in the TN NSS layer and data forward policy in the transport network layer

Table C.1 shows the mapping between network resource isolation policy and network resource allocation policy, and the mapping between traffic isolation policy and data traffic forward policy, respectively.

Table C.1 – Mapping between slice isolation policy in the TN NSS layer and data forward policy in the transport network layer

Data forward policy in the transport network				Slice isolation policy in the TN NSS layer		
Transport network resource allocation policy	Router	standard/undifferentiated		no isolation		Network resource isolation policy
		dedicated hardware		physical network function isolation		
		dedicated software/virtual		logical network function isolation		
	Switch	standard/undifferentiated		no isolation		
		dedicated hardware		physical network function isolation		
		dedicated software/virtual		logical network function isolation		
	Channel	standard/undifferentiated		no isolation		
		dedicated hardware		physical network link isolation		
		dedicated software/virtual		logical network link isolation		
Data traffic forward policy	IPsec	no IPsec	no integrity/ confidentiality	no isolation		Traffic isolation policy
		IPsec AH	data origin authentication	medium-level isolation with data origin authentication (security protection level isolation)		
		IPsec ESP	data origin authentication, data integrity, data confidentiality, detection and rejection of replays	high-level isolation with integrity and confidentiality protection (security protection level isolation)		
	Filter rules	ACL – white list	data from a specific list of VLAN_IDs to be forwarded	data type 1, data type 3, …	data type 1: bank service, data type 3: finance service, data type 15: gaming service, …	
		ACL – black list	data from a specific list of VLAN_IDs to be dropped	data type 15, …	data type 1 and data type 3 can be grouped and transported over one VLAN_ID, over which data type 15 cannot be forwarded (data type isolation)	
		other rules	……	…		
	DSCP classes	DF (CS0)	standard	no isolation		

Table C.1 – Mapping between slice isolation policy in the TN NSS layer and data forward policy in the transport network layer

Data forward policy in the transport network				Slice isolation policy in the TN NSS layer
	[IETF RFC 4594]	AF21, AF22, AF23	low-latency data	uRLLC data (service type isolation)
		AF11, AF12, AF13	high-throughput data	eMBB data (service type isolation)
		CS1	low-priority data	mMTC data (service type isolation)
		CS4	real-time interactive	real-time interactive video conference data (video type isolation)
		CS3	broadcast video	broadcast video data (video type isolation)
		AF31, AF32, AF33	multimedia streaming	multimedia streaming data on demand (video type isolation)
		…	…	…

Annex D

DLT-based mechanisms on making network slice management data tamper-proof and traceable

(This annex forms an integral part of this Recommendation.)

Feasible mechanisms based on the distributed ledger technology (DLT) to make network slice management data tamper-proof and traceable are described in this annex.

D.1 DLT-based data model for network slice management data

Generally, the volume of fault/performance/security data of network slice management is too big to be stored at the distributed ledgers or blocks. The volume of configuration data/parameter is small. However, configuration data/parameter is sensitive and cannot be stored at the distributed ledgers or blocks as a plaintext. While, only some attributes of the network slice management data (e.g., fault data, performance data, security data, configuration data) in Table D.1 are stored at the distributed ledgers or blocks, raw network slice management data is collected and stored at the traditional datacentre. If raw network slice management data is modified intentionally or unintentionally, the modification will be detected with the associated attributes stored at the distributed ledgers or blocks.

Table D.1 – Attributes of network slice management data to be stored at the distributed ledgers or blocks

data_index	data_type	data_generator	data_user	timestamp	data_storage_location	data_hash	signature

The attributes in Table D.1 are defined as follows:

- data_index: an ID to indicate the index of network slice management data attributes.
- data_type: a flag to indicate the data types of network slice management data, such as fault data, performance data, configuration data, security data, and so on.
- data_generator: an ID to indicate the network function which generates the relevant network slice management data. The data_generator comprises the ID of the network function and the ID (e.g., a public key) of the associated service provider who manages/administrates the network function. According to Figure 8-1, the network functions are *PNF, VNF, VIM, VNFM, NFVO, NFM, transport network controller, NSS data collection, NSS security data collection, NS data collection, NS security data collection*, and so on. The corresponding service providers are network slice provider, NSS provider, TN provider, core network provider, AN provider, software provider, HW provider, and so on.
- data_user: an ID to indicate the network function which consumes the relevant slice management data. The data_user comprises the ID of the network function and the ID (e.g., a public key) of the associated service provider who manages/administrates the network function.

For example, the *NSS security monitoring* of each NSS domain in Figure 8-1 stores the network slice instance relevant security data attribute to the distributed ledger or block. In order to know the security status of the E2E network slice instance, the *NS security monitoring* accesses security data attribute stored at the distributed ledger or block, gets the corresponding security data from the database of the relevant NSS domains (e.g., AN/TN/CN NSS domain), and then analyses the security data correlatively. The *NSS security monitoring* of the AN/TN/CN NSS domain is the security data generator, and the corresponding service provider is the AN/TN/CN NSS provider. Thus, the data_generator comprises the ID of the *NSS security monitoring* of the AN/TN/CN NSS domain and the ID of the AN/TN/CN NSS provider (e.g., a public key). The *NS security monitoring* is the security data consumer, and the corresponding service provider is the network slice provider. Thus, the

data_user comprises the ID of the *NS security monitoring* and the ID of the network slice provider (e.g., a public key).

- timestamp: the time of the network slice management data collected or generated.
- data_storage_location: the location of the network slice management data storage, which may be a file, a table of the database, or an entry of a table.
- data_hash: a hash value of the network slice management data.
- signature: the signature is generated with the private key of the attribute generator (i.e., relevant service provider).

Figure D.1 shows the structure of one distributed ledger/block to store the attributes of the network slice management data in Table D.1. The relevant network slice management data is stored at the database with the location indicated by the attribute data_storage_location in Table D.1.

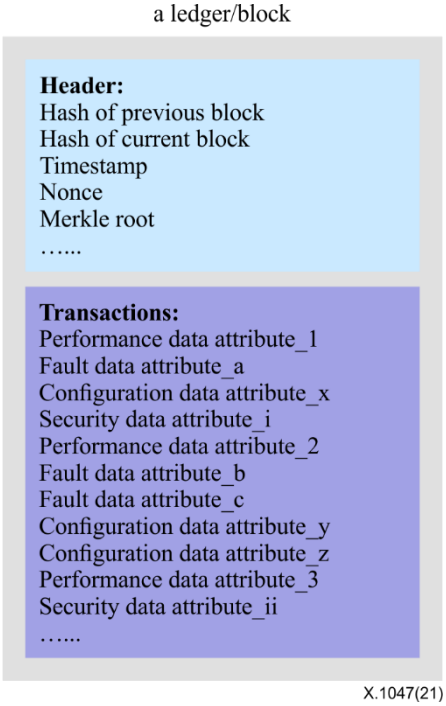

Figure D.1 – Structure of one ledger/block to store the attributes in Table D.1

D.2 DLT-based data storage for the attributes of the network slice management data

According to Figure 6-1, there are some participants/partners who collaborate and cooperate to provide customized network slices for a variety of vertical industries. These participants/partners comprise network slice provider, NSS provider, TN provider, core network provider, AN provider, software provider, HW provider, and so on. In order to make network slice management data tamper-proof and traceable and to further then ensure that the network slices conform to the SLAs [b-TM Forum-Blockchain], these participants or partners can build trust between them based on the consortium blockchain and store the attributes of the network slice management data to the distributed ledgers/blocks, which is shown in Figure D.2.

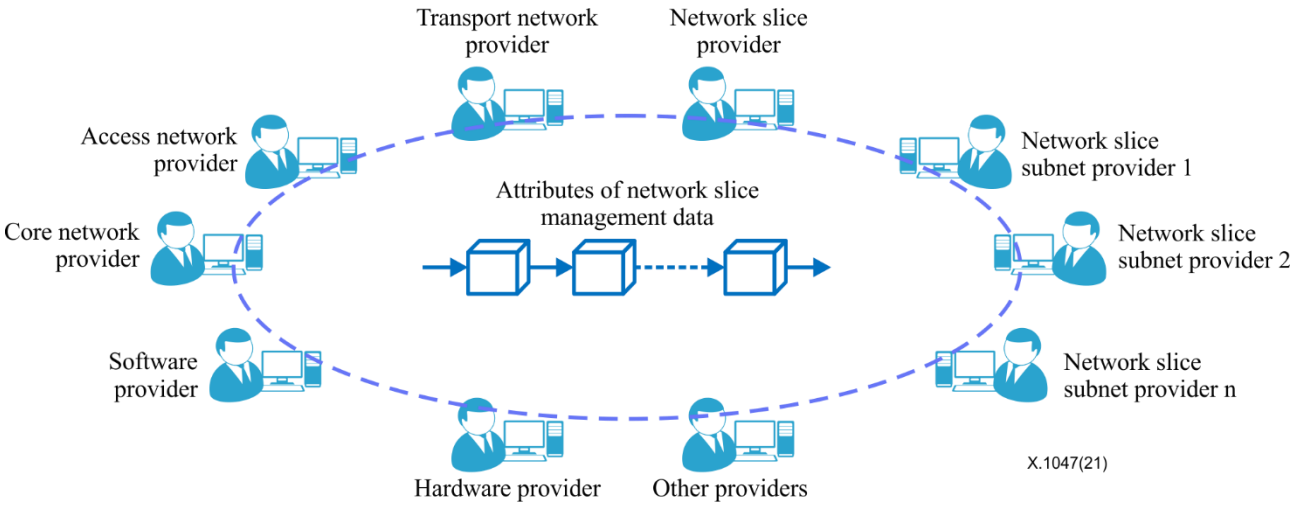

Figure D.2 – Building trust between participants or partners based on a consortium blockchain

In order to build trust between participants/partners and support storing attributes of the network slice management data to the distributed ledgers/blocks, all the network functions relevant to manage/store network slice management data should install a logical function *DLT agent*, which is shown in Figure D.3. The logical function *DLT agent* is described in clause D.3.

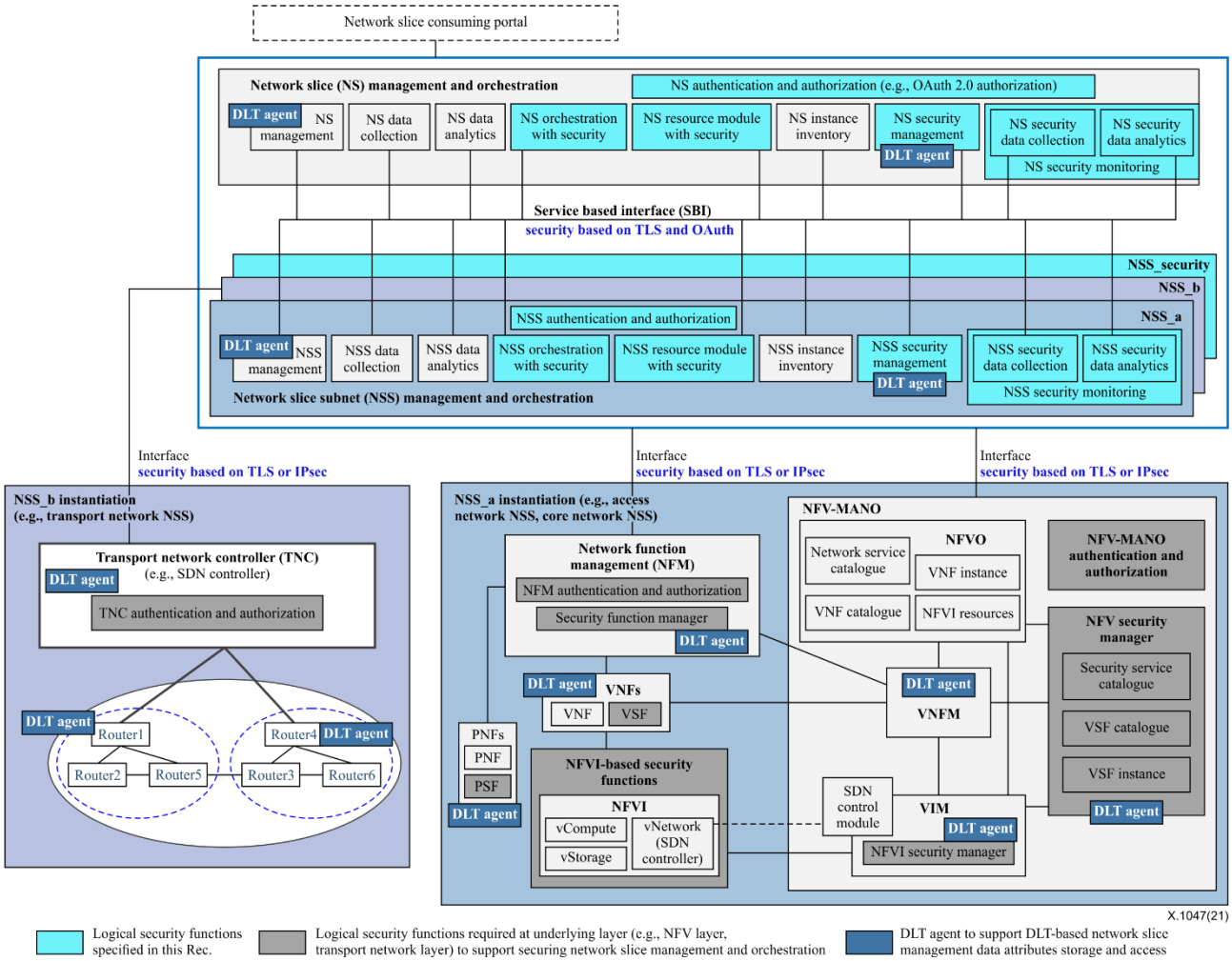

Figure D.3 – DLT agent to support storing attributes of the network slice management data to the distributed ledgers or blocks

D.3 DLT-based network slice management data storage and access

The implementation of a DLT-based network slice management data storage and access is shown in Figure D.4.

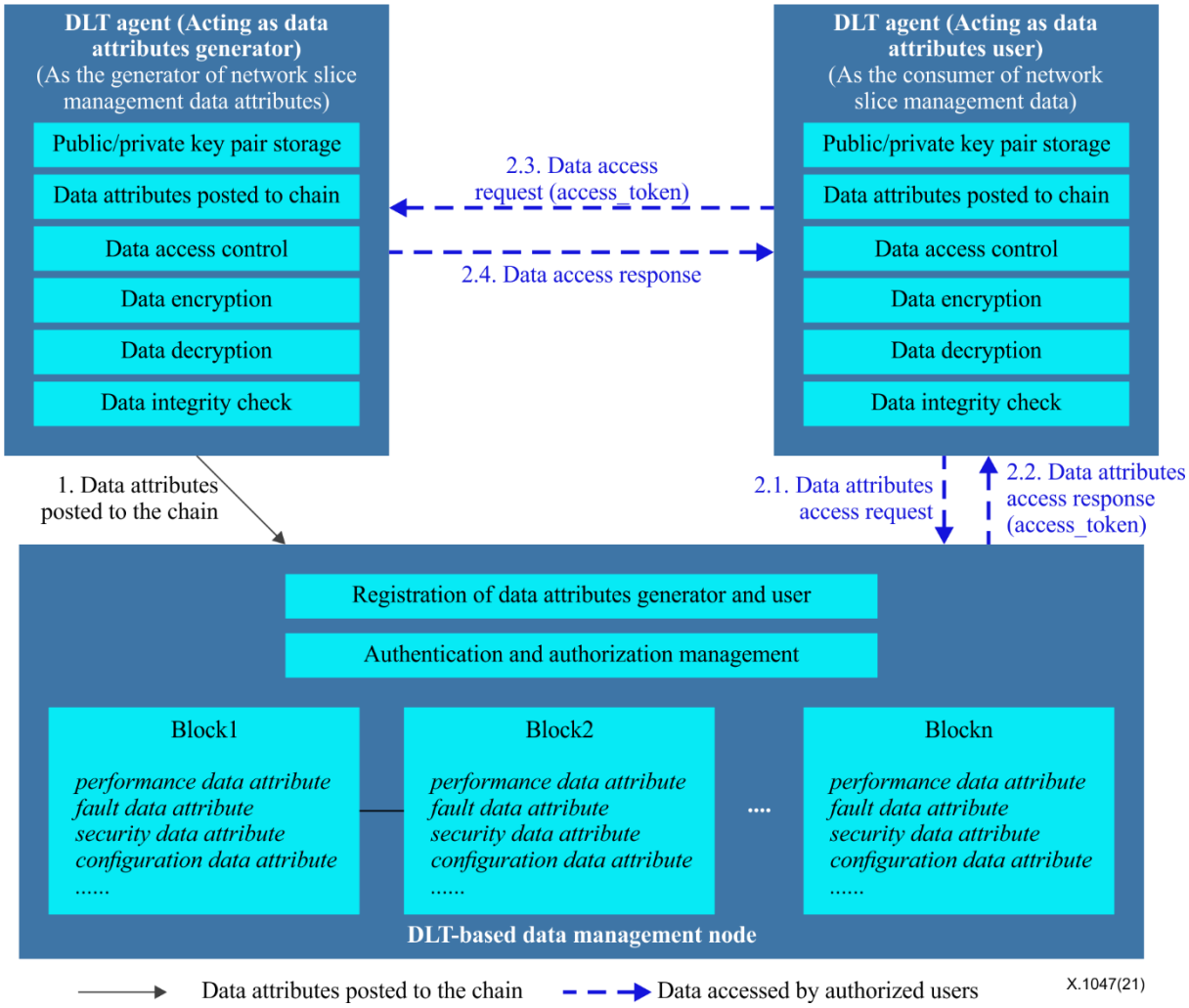

Figure D.4 – DLT-based network slice management data storage and access

In Figure D.4, the logical function *DLT agent* act as both the data attributes generator and the user network slice management data. The *DLT agent* has the following components:

- *Public/private key pair storage*: to store public/private key pairs for the service provider who manages/administrates the relevant network functions/services together with the network slice management data.
- *Data attributes posted to chain*: to generate the attributes of the network slice management data according to Table D.1, and then send/post the data attributes to the *DLT-based data management node* which is capable of generating a new block/ledger. The *DLT-based data management node* aggregates the attributes, creates a new block/ledger then publishes the new block/ledger to the chain.
- *Data access control*: to validate the "access_token" which is generated by the *DLT-based data management node*. If validated successfully, the location of the requested data will be sent to the data user.
- *Data integrity check*: to check if the network slice management data is tampered or not with the value of data_hash, one of the attributes defined in Table D.1.

- *Data encryption:* to encrypt data especially configuration data before the data is sent to the data attributes user.
- *Data decryption:* to decrypt data especially configuration data in ciphertext after it is received from the data attributes generators.

In Figure D.4, the logical function *DLT-based data management node* acts as a blockchain node and has the capability of creating new blocks/ledgers and keeping a full copy or its own local copy of the blockchain. The *DLT-based data management node* is deployed in the server side, as a stand-alone network function or integrated with any of the network management functions. Each service provider may have its own *DLT-based data management node*.

The *DLT-based data management node* has the following components:

- *Registration of data attributes generator and user/consumer*: to manage the registration of a service provider that generates or uses/consumes network slice management data. The unique ID of the data attributes generator or data attributes user/consumer includes the ID of the network function and the corresponding service provider's public key together with the other parameters. Data attributes generator and data attributes user/consumer must keep the corresponding private key by themselves via a *DLT agent*.
- *Authentication and authorization management*: to authenticate data attributes user/consumer that requests an AN slice management data and to then authorize the data attributes user/consumer to access the requested data. After successful authentication and authorization, "access_token" is generated and responded to the data attributes user/consumer.
- *Ledger/block*: to store the ledgers/blocks which include the attributes of the network slice management data.

For example, in order to know the security status of the E2E network slice instance in Figure 8-1, firstly, the *NS security monitoring* should get the corresponding security data from all its constituent parts, such as the *NSS security monitoring* of the AN, *NSS security monitoring* of the TN, *NSS security monitoring* of core network, *transport network controller*, *NFV security manager*, *security function manager*, and so on. In order to simplify the description of the procedures, it is assumed that one *NSS security monitoring* is the security data attributes generator and the *NS security monitoring* is the security data attributes user/consumer.

In the Figure D.4, according to the step "1. Data attributes posted to the chain," the procedure of the *NSS security monitoring* storing the attributes of the network slice management data is described as follows:

a) The component *data attributes posted to chain* of the *DLT agent* in the *NSS security monitoring* sends the attributes of the security data to the *DLT-based data management node* periodically or when it responds to a request from the *NS security monitoring*. The attributes of the security data are generated according to the DLT-based data model in Table D.1, where the data_type is the security data, and the data_generator comprises the ID of the *NSS security monitoring* and the public key of the associated NSS provider.

b) The *DLT-based data management node* aggregates the data attributes, creates a new block/ledger then publishes the new block/ledger to the chain.

c) The *DLT-based data management node* keeps a full copy or its individual copy of the blockchain.

In the Figure D.4, according to step "2. Accessing network slice management data," the procedure of *NS security monitoring* accessing data is described as follows:

2.1) The *DLT agent* of *NS security monitoring* (as data attributes user) sends the message "data attributes access request" to the *DLT-based data management node* in order to access the attributes of the security data. This request includes the network slice provider's public key,

NSS provider's public key, network slice instance information, data type (i.e., security data), the time of raw security data collected or generated.

2.2) The *authentication and authorization management* of the *DLT-based data management node* authenticates the data attributes user i.e., network slice provider with its public key, then checks if the data_user list includes the requested network slice provider. If the requested network slice provider is authenticated successfully and is found in the data_user list, the *DLT-based data management node* generates an "access_token" and sends the message "data attributes access response" to the *DLT agent* of the *NS security monitoring* (as data attributes user). This response message includes data storage location "data_storage_location", hash value of the raw data "data_hash", and the access token "access_token".

2.3) After receiving the message "data attributes access response" from the *DLT-based data management node*, the *DLT agent* of the *NS security monitoring* (as data attributes user) sends the message "data access request" to the *DLT agent* of the *NSS security monitoring* (as data attributes generator) in order to access the raw security data. This request message includes the network slice provider's public key, data storage location "data_storage_location", and the access token "access_token".

2.4) After receiving the message "data access request" from the *DLT agent* of the *NS security monitoring* (as data attributes user), the component *data access control* of the *DLT agent* in the *NSS security monitoring* (as data attributes generator) validates the "access_token". If the "access_token" is valid, the component *data access control* of the *DLT agent* in the *NSS security monitoring* (acting as data attributes generator) indicates that the *DLT agent* in the *NSS security monitoring* sends the message "data access response" back to the *DLT agent* of the *NS security monitoring* (as data attributes user). This response message includes the requested raw security data. After receiving the requested raw security data, the component *data integrity check* of the *DLT agent* of the *NS security monitoring* (as data attributes user) calculates the hash value of the received raw security data, by comparing the calculated hash value with the hash value "data_hash" received from the *DLT-based data management node*. If these two hash values are equal, the raw network slice management data is not tampered.

In this way, data tampering can be detected. Moreover, access to raw network slice management data is guaranteed only to authorized data users.

According to Figure D.4, the components *data encryption* and *data decryption* of the *DLT agent* is used for configuration data storage and access since the configuration data is sensitive. However, the corresponding procedures are not mentioned in this Recommendation in order to simplify the description.

Bibliography

[b-ITU-T X.1811] Recommendation ITU-T X.1811 (2021), *Security guidelines for applying quantum-safe algorithms in IMT-2020 systems*.

[b-ITU-T X.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology*.

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

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP over TLS*. https://datatracker.ietf.org/doc/html/rfc2818

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic algorithm implementation requirements for encapsulating security payload (ESP) and authentication header (AH)*. https://datatracker.ietf.org/doc/html/rfc4835

[b-IETF RFC 4949] IETF RFC 4949 (2007), *Internet security glossary, version 2*. https://datatracker.ietf.org/doc/html/rfc4949

[b-IETF RFC 5782] IETF RFC 5782 (2010), *DNS blacklists and whitelists*. https://datatracker.ietf.org/doc/html/rfc5782

[b-IETF RFC 5851] IETF RFC 5851 (2010), *Framework and requirements for an access node control mechanism in broadband multi-service networks*. https://datatracker.ietf.org/doc/html/rfc5851

[b-IETF RFC 7519] IETF RFC 7519 (2015), *JSON web token (JWT)*. https://datatracker.ietf.org/doc/html/rfc7519

[b-IETF-TNS-framework] IETF (2021), *Framework for IETF network slices: draft-nsdt-teas-ns-framework-05*. Available [viewed 2021-06-06] at: https://tools.ietf.org/html/draft-nsdt-teas-ns-framework-05

[b-IETF-TS-definition] IETF (2020), *IETF definition of transport slice: draft-nsdt-teas-transport-slice-definition-04*. Available [viewed 2021-06-06] at: https://tools.ietf.org/html/draft-nsdt-teas-transport-slice-definition-04

[b-3GPP TR 33.811] Technical Report 3GPP TR 33.811 V15.0.0 (2018), *3rd Generation Partnership Project; Technical specification group services and system aspects; Study on security aspects of 5G network slicing management (Release 15)*.

[b-3GPP TR 33.813] Technical Report 3GPP TR 33.813 V16.0.0 (2020), *3rd Generation Partnership Project; Technical specification group services and system aspects; Security aspects*; *Study on security aspects of network slicing enhancement (Release 16)*.

[b-ETSI GR NFV-SEC 009] Group Report ETSI GR NFV-SEC 009 V1.2.1 (2017), *Network functions virtualisation (NFV); NFV security; Report on use cases and technical approaches for multi-layer host administration.*

[b-ETSI GS NFV-MAN 001] Group Specification ETSI GS NFV-MAN 001 V1.1.1 (2014), *Network functions virtualisation (NFV); Management and orchestration.* https://pdf4pro.com/fullscreen/etsi-gs-nfv-man-001-v1-1-28f31d.html

[b-ETSI GS NFV-IFA 011] Group Specification ETSI GS NFV-IFA 011 V4.1.1 (2020), *Network functions virtualisation (NFV) release 4; Management and orchestration; VNF descriptor and packaging specification.*

[b-ETSI GS NFV-IFA 014] Group Specification ETSI GS NFV-IFA 014 V3.4.1 (2020), *Network functions virtualisation (NFV) release 3; Management and orchestration; Network service templates specification.* https://docbox.etsi.org/isg/nfv/open/Publications_pdf/Specs-Reports/NFV-IFA%20014v3.4.1%20-%20GS%20-%20Network%20Service%20Templates%20Spec.pdf

[b-ETSI GS ZSM 002] Group Specification ETSI GS ZSM 002 V1.1.1 (2019), *Zero-touch network and service management (ZSM); Reference architecture.* https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf

[b-ETSI TS 128 530] Technical Specification ETSI TS 128 530 V17.1.0 (2021), *5G; Management and orchestration; Concepts, use cases and requirements* (3GPP TS 28.530 version 17.1.0 Release 17).

[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 16.9.0 Release 16).

[b-ETSI TS 128 533] Technical Specification ETSI TS 128 533 V16.7.0 (2021), *5G; Management and orchestration; Architecture framework* (3GPP TS 28.533 version 16.7.0 Release 16). https://www.etsi.org/deliver/etsi_ts/128500_128599/128533/16.07.00_60/ts_128533v160700p.pdf

[b-ETSI TS 128 541] Technical Specification ETSI TS 128 541 V17.2.1 (2021), *5G; Management and orchestration; 5G network resource model (NRM); Stage 2 and stage 3* (3GPP TS 28.541 version 17.2.1 Release 17).

[b-EU-INSPIRE-5Gplus-DLT] INSPIRE-5Gplus INtelligent Security and PervasIve tRust for 5G and Beyond. https://cordis.europa.eu/project/id/871808

[b-EU-Inspire-5Gplus-D2.1] Inspire-5Gplus Deliverable (2020), *D2.1: 5G security – Current status and future trends.* Version v1.0. Heidelberg: Inspire-5Gplus Consortium. 101 pp. Available [viewed 2021-06-06] at: https://www.inspire-5gplus.eu/wp-content/uploads/2020/05/i5-d2.1_5g-security-current-status-and-future-trends_v1.0.pdf

[b-EU-Inspire-5Gplus-D5.1] Inspire-5Gplus Deliverable (2020), *D5.1: 5G security test cases.* Version v1.0. 102 pp. Available [viewed 2021-06-06] at: https://www.inspire-5gplus.eu/wp-content/uploads/2020/11/i5-d5.1_5g-security-test-cases_v1.0.pdf?x87609

[b-NGMN-5G] NGMN-5G, Thalanany, S. (2019), *5G end-to-end architecture framework* V3.0.8. Frankfurt-am-Main: NGMN Alliance. 70 pp. Available [viewed 2021-06-06] from: https://www.ngmn.org/publications/5g-end-to-end-architecture-framework-v3-0-8.html

[b-TM Forum-Accenture] TM Forum-Accenture (2019), Ridgewell, P., Bushaus, D. *Blockchain: Where's the value for telecoms?* Nice, France. 39 pp. Available [viewed 2021-06-06] at: https://www.accenture.com/_acnmedia/PDF-101/Accenture-Blockchain-Wheres-the-Value-for-Telecoms.pdf

[b-TM Forum-Blockchain] TM Forum-Blockchain (2018), *Blockchain unleashed*. Available [viewed 2021-06-06] at: https://www.tmforum.org/wp-content/uploads/2018/03/T.-Blockchain-Unleashed.pdf

[b-TM Forum-TR 279] TM Forum-TR 279 (2019), *TR279 CSP use cases utilizing blockchain v3.1.1*. Available [viewed 2021-06-06] at: https://www.tmforum.org/resources/technical-report/tr279-csp-use-cases-utilizing-blockchain-v3-1/

[b-Bihannic] Bihannic, N., Lejkin, T., Finkler, I., Frerejean, A. (2018). *Network slicing and blockchain to support the transformation of connectivity services in the manufacturing industry*. IEEE Softwarization. Available [viewed 2021-06-06] at: https://sdn.ieee.org/newsletter/march-2018/network-slicing-and-blockchain-to-support-the-transformation-of-connectivity-services-in-the-manufacturing-industry

[b-Hu] Hu, Z., Yin, Y. (2017). *A framework for security on demand.* 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 378-383. Valencia, Spain. IEEE doi: 10.1109/IWCMC.2017.7986316. https://ieeexplore.ieee.org/document/7986316

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

Printed in Switzerland
Geneva, 2021