ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3128 (12/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Future networks

Requirements for network function communication between public networks and public network integrated non-public networks in IMT-2020

ITU-T Y-SERIES RECOMMENDATIONS

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
General	Y.100-Y.199
Services, applications and middleware	Y.200-Y.299
Network aspects	Y.300-Y.399
Interfaces and protocols	Y.400-Y.499
Numbering, addressing and naming	Y.500-Y.599
Operation, administration and maintenance	Y.600-Y.699
Security	Y.700-Y.799
Performances	Y.800-Y.899
INTERNET PROTOCOL ASPECTS	Y.1000-Y.1999
General	Y.1000-Y.1099
Services and applications	Y.1100-Y.1199
Architecture, access, network capabilities and resource management	Y.1200-Y.1299
Transport	Y.1300-Y.1399
Interworking	Y.1400-Y.1499
Quality of service and network performance	Y.1500-Y.1599
Signalling	Y.1600-Y.1699
Operation, administration and maintenance	Y.1700-Y.1799
Charging	Y.1800-Y.1899
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
Frameworks and functional architecture models	Y.2000-Y.2099
Quality of Service and performance	Y.2100-Y.2199
Service aspects: Service capabilities and service architecture	Y.2200-Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250-Y.2299
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	**Y.3000-Y.3499**
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

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

Recommendation ITU-T Y.3128

Requirements for network function communication between public networks and public network integrated non-public networks in IMT-2020

Summary

Recommendation ITU-T Y.3128 specifies requirements for network function communication between public networks (PNs) and public network integrated non-public networks (NPNs) in IMT-2020. These requirements build on the analysis of relevant use cases and related network problems.

There are two types of NPN: public network integrated non-public networks (PNI-NPN); and stand-alone non-public networks (SNPN). The requirements specified in this Recommendation concern the first type.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3128	2023-12-14	13	11.1002/1000/15739

Keywords

IMT-2020, network function communication, non-public network, NPN, public network, PN, public network integrated non-public network, PNI-NPN, requirements.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Recommendation ITU-T Y.3128

Requirements for network function communication between public networks and public network integrated non-public networks in IMT-2020

1 Scope

This Recommendation specifies requirements for network function (NF) communication between public networks (PNs) and public network integrated non-public networks (NPNs) in IMT-2020.

There are two types of NPN: public network integrated non-public network (PNI-NPN); and stand-alone non-public network (SNPN). The requirements specified in this Recommendation concern the PNI-NPN type.

Relevant use cases are provided in Appendix I.

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.

[ETSI TS 123 501] Technical Specification ETSI TS 123 501 V17.10.0 (2023-09), *System architecture for the 5G System (5GS); Stage 2.*

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 direct communication: Communication between network functions or network function services without using a service communication proxy.

NOTE – Based on [ETSI TS 123 501].

3.2.2 indirect communication: Communication between network functions or network function services via a service communication proxy.

NOTE – Based on [ETSI TS 123 501].

3.2.3 non-public network: A network that is intended for non-public use.

NOTE – Based on [b-ITU-T X.1813].

3.2.4 public network integrated non-public network: A non-public network deployed with the support of a public land mobile network.

NOTE – Based on [ETSI TS 123 501].

3.2.5 stand-alone non-public network: A non-public network not relying on network functions provided by a public land mobile network.

NOTE – Based on [ETSI TS 123 501].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASF Authentication Server Function

DC Data Centre

IE Information Element

NACF Network Access Control Function

NF Network Function

NPN Non-Public Network

PCF Policy Control Function

PLMN Public Land Mobile Network

PN Public Network

PNI-NPN Public Network Integrated Non-Public Network

SCP Service Communication Proxy

SMF Session Management Function

SNPN Stand-alone Non-Public Network

UPF User Plane Function

USM Unified Subscription Management

5 Conventions

In this Recommendation:

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

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

The phrase "can optionally" indicates an optional requirement which 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 or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview of public network integrated non-public network

With the IMT-2020 enablement of vertical industries, more and more customers are interested in using a non-public network (NPN) [b-ITU-T X.1813] to provide their private data network services.

Two types of NPNs can be distinguished: Stand-alone non-public network (SNPN); and public network integrated non-public network (PNI-NPN) [ETSI TS 123 501]. An SNPN is operated by an NPN operator and does not rely on network functions (NFs) provided by a public land mobile network (PLMN) [b-ITU-T Q.1741.7]. A PNI-NPN is supported by PLMNs, e.g., by means of dedicated data network names [b-ETSI TS 123 003] or by one (or more) network slice instances [b-ITU-T Y.3100] allocated for the NPN.

This Recommendation addresses in particular the PNI-NPN type, which is an easy and rapid way for operators to provide private data network services.

Figure 1 illustrates the PNI-NPN type where all NFs are deployed in the operator's data centre (DC).

NOTE 1 – The example NFs shown in Figure 1 (as well as in Figures 2 and 3) include NFs specified in [b-ITU-T Y.3102] and, as far as the service communication proxy (SCP) is concerned, in [ETSI TS 123 501].

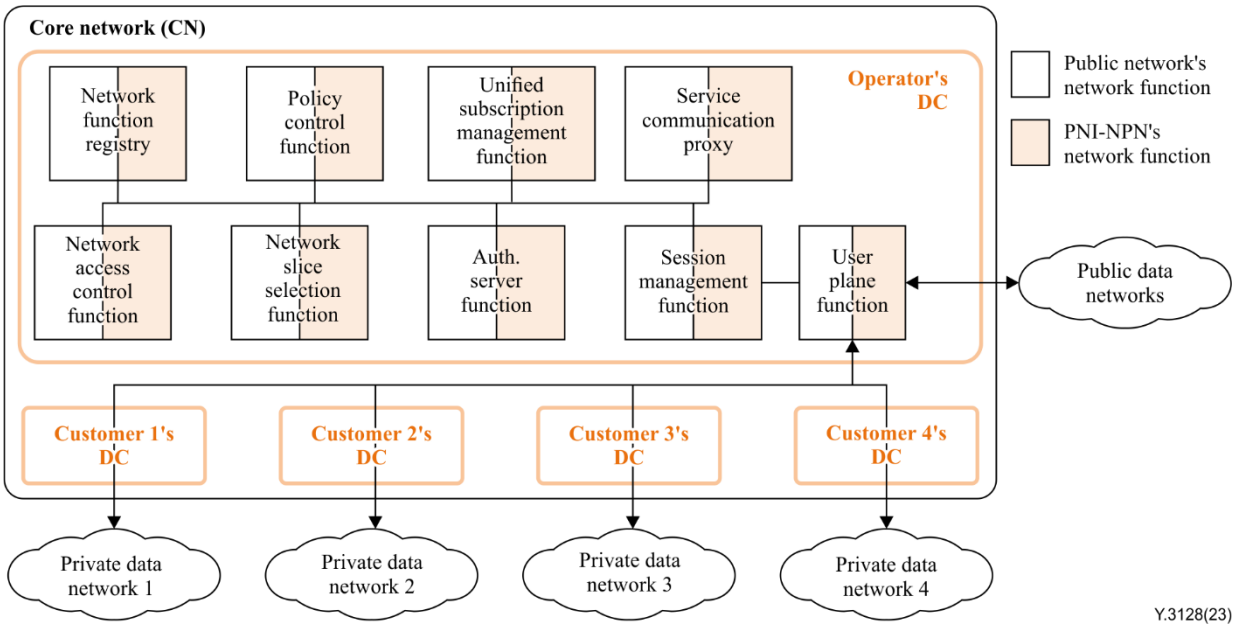

Figure 1 – The PNI-NPN type with all NFs deployed in the operator's DC

As shown in Figure 1, the operator provides private and public data network services to end users via access network and core NFs. All NFs of the core network are deployed in the operator's DC and none in those of customers. There are four customers, which use the NFs of the operator's DC and have no control over them. Each customer holds their own private data network.

NOTE 2 – The two-colour boxes in the two upper rows of Figure 1 illustrate NFs deployed in the operator's DC serving both a PN and PNI-NPN.

In Figure 2, in order to meet the individual needs of private data network services, some NFs may be deployed as dedicated NFs in customers' DCs, located then in an untrusted domain out of control of the operator.

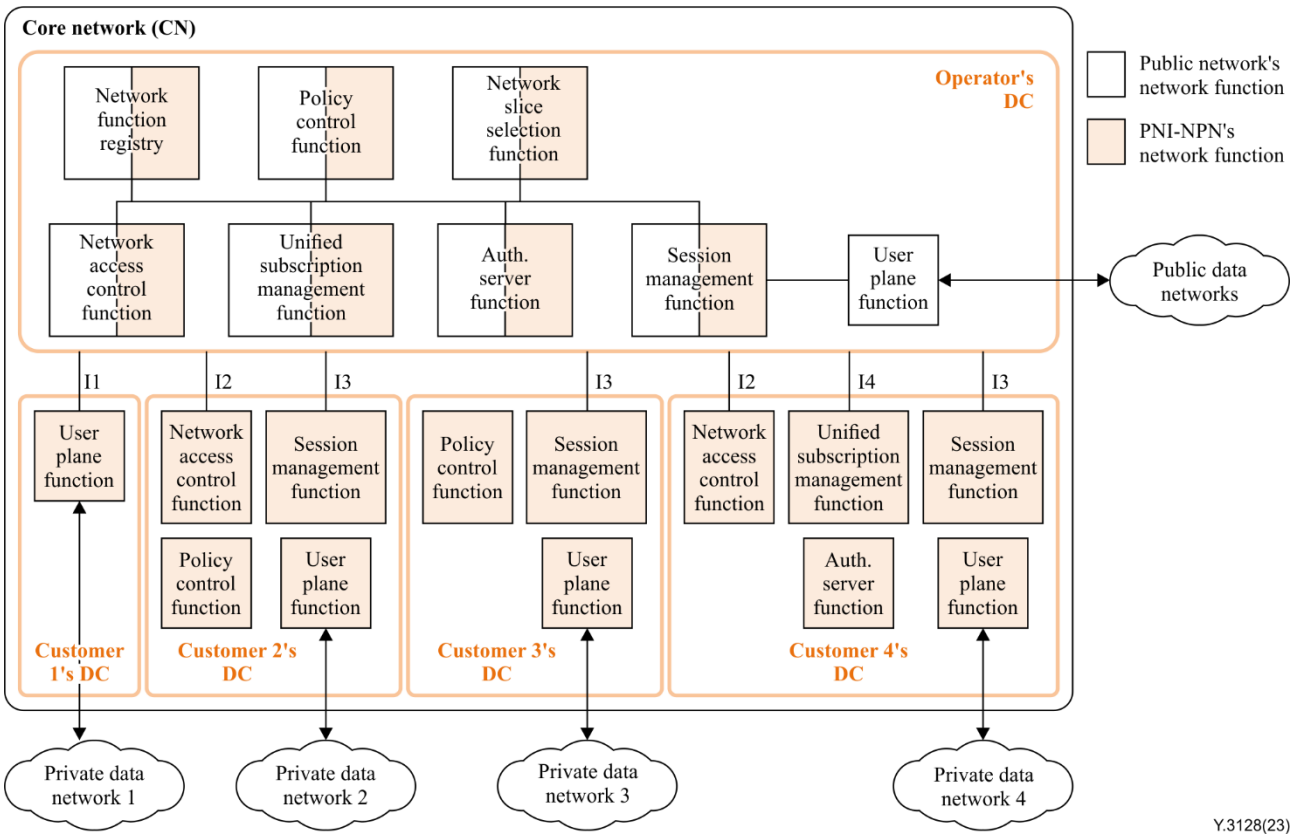

Figure 2 – The PNI-NPN type with some NFs deployed in the customers' DCs

Public data network services are provided by NFs deployed in the operator's DC, while those that are private are provided jointly by NFs deployed in both the operator's and customers' DCs.

NOTE 3 – In the operator's DC of Figure 2, similarly to Figure 1, the two-colour boxes in the two upper rows represent NFs serving both the public network (PN) and PNI-NPN, and the user plane function (UPF) deployed in the operator's DC only serves the PN. The NFs, including UPF, deployed in customers' DCs only serve PNI-NPNs.

There are four main deployment options of the PNI-NPN type with some NFs deployed in the customers' DCs, as described in Appendix I. The options differ in the set of NFs deployed in the customers' DCs, e.g., that for customer 2's DC includes a network access control function (NACF), session management function (SMF), policy control function (PCF) and UPF. These different sets provide various network capabilities and communicate with NFs of the PN with different types of interface. The interfaces of each customer's DC to connect to the operator's DC are shown in Figure 2 as I1 for UPF, I2 for NACF, I3 for SMF and I4 for unified subscription management (USM) function. For example, in customer 1's DC, the UPF communicates with the PN through interface I1, and in customer 2's DC, the NACF and SMF communicate with the PN respectively through interface I2 and I3. Moreover, in one customer's DC, there may be multiple types of interface to communicate with the PN, as shown for customer 2's DC.

In addition, as specified in [ETSI TS 123 501], two types of communication mode are possible for the PNI-NPN type with some NFs deployed in the customers' DCs: direct, which supports the communication between NFs directly as shown in Figure 2; and indirect, which supports the communication between NFs via a SCP as shown in Figure 3.

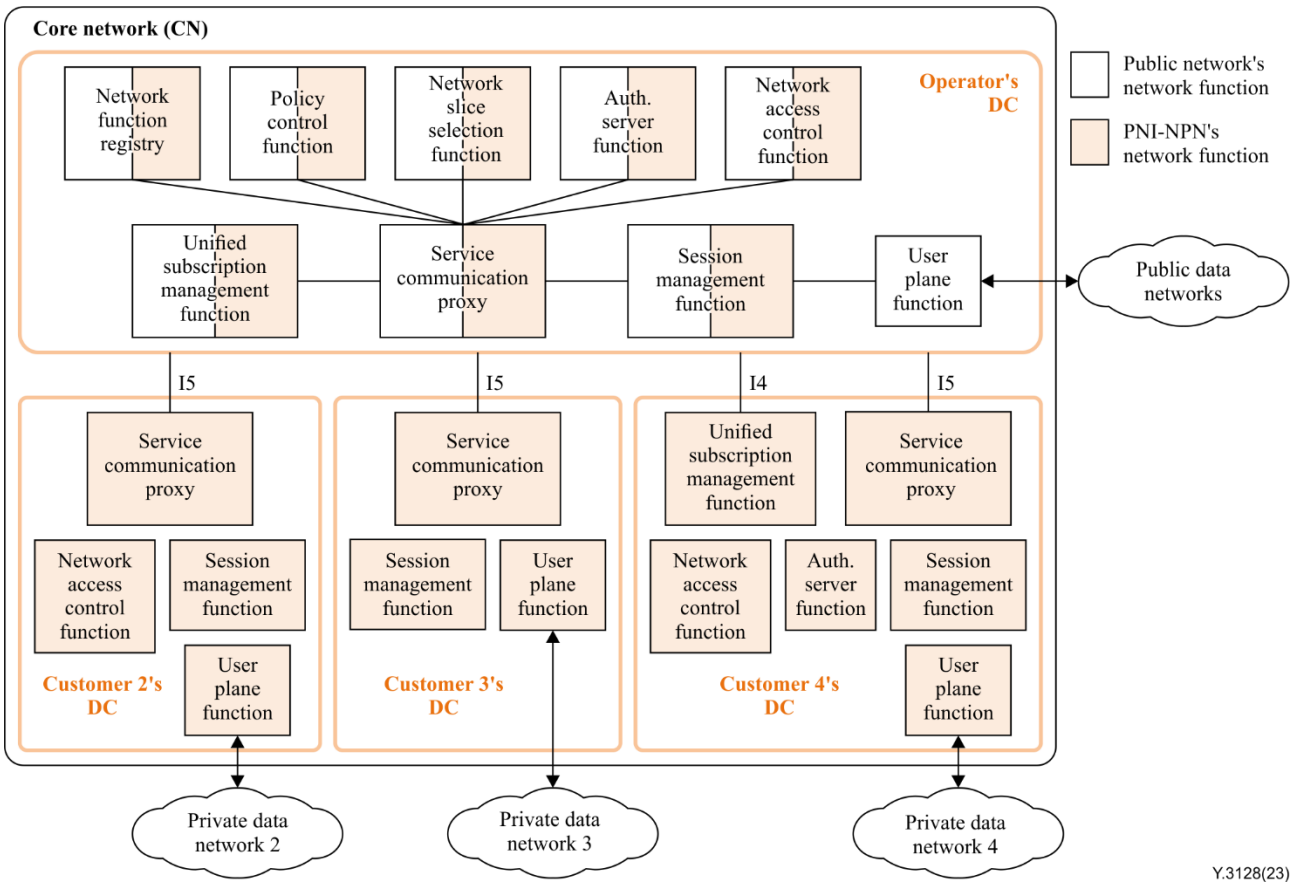

Figure 3 – The PNI-NPN type with some NFs deployed in customers' DCs and usage of the indirect communication mode

The SCPs deployed in customers' DCs communicate with the PN through the interfaces I5.

NOTE 4 – The two-colour boxes in the two upper rows of SCP deployed in the operator's DC serve both PN and PNI-NPN, while the single colour boxes of SCP deployed in the customers' DCs only serve PNI-NPN.

The same communication mode is used between the NFs within a given customer's DC (direct communication mode in Figure 2 and indirect in Figure 3) and between the NFs in the operator's DC (direct communication mode in Figure 2 and indirect in Figure 3). However, different communication modes may be used between one (or more) NF in a given customer's DC and one (or more) NF in the operator's DC.

7 Network function communication problems between public networks and public network integrated non-public networks in IMT-2020

According to the use cases provided in Appendix I, some NFs of NPNs are located in customers' DCs, with some NPNs having only one NF, while others have multiple NFs.

Different NPNs may connect to the PN through various types of interface. NPNs may also connect to the PN through one or multiple types of interface (e.g., in Figure 2, in customer 1's DC or customer 3's DC, there is one type of interface to communicate with the PN, while in customer 2's DC or customer 4's DC there are multiple types).

The support of the described use cases causes the following problems from a network perspective.

– Complex topology: As the number of NPNs continues to increase, and the number of point-to-point connections between the NFs of NPNs and the NFs of the PN rises, IMT-2020 network topology becomes more and more complex. For example, in the use case described in clause I.2, NACF, SMF, PCF and UPF are all deployed in a single NPN, communicating

with an authentication server function (ASF) and USM function in the PN through different interfaces. Complexity of network topology particularly affects the direct communication mode.

– Complex interworking: As NFs can be provided from different vendors, the interface between those of NPNs and the PN require interoperability testing. The more interfaces and more vendors there are, the more interoperability testing is required. The message information elements (IEs) on one interface are divided into three categories: mandatory; conditional; and optional. The optional IEs make interoperability testing between NPNs and the PN more complex as different vendors may implement message information elements differently, e.g., some vendors include them and others not.

  On the other hand, several IMT-2020 core network implementations based on 3GPP 5G core network specifications can be deployed, and the related 3GPP specifications continue to evolve in terms of version updates. There are compatibility issues when different versions for NPNs and PN work together. The version applied in a given NPN depends on customer demand and the time of network deployment. After network set up, the version in the NPN may not be updated at the same time as the PN upgrade. For example, various customers can deploy NPNs based on different versions of 3GPP specifications. In order to adapt to different versions of NPNs, the NFs of the PN may need to support multiple versions at the same time.

– PN instability: Every time an NPN is deployed, data configuration, including configuration updates, must be performed on the NFs in the PN. Each data configuration and related modifications can cause a risk to the PN, as well as in terms of interworking with NPNs.

– Failure due to different communication modes: When an NF in the PN tries to communicate by using the indirect (direct) communication mode with an NPN that adopts one that is direct (indirect), the communication fails.

8 Requirements for network function communication between public networks and public network integrated non-public networks in IMT-2020

In order to address the problems identified in clause 7, while deploying NPNs for customers on the basis of their specific requirements, and simultaneously reducing the impact of these deployments on the PN, the requirements in clauses 8.1 and 8.2 for NF communication between the PN and NPNs apply.

8.1 PN requirements

– The PN is required to support signalling aggregation in order to reduce the number of point-to-point connections between the NFs of NPNs and the NFs of the PN.

– The PN is required to synchronize NPN user data with the NPN unidirectionally (i.e., from the PN to the NPN), in order to avoid modifications of the user data in the PN by customers.

  NOTE 1 – This applies when a dedicated USM function is deployed in a given customer's NPN.

– The PN is required to distinguish different NPN user data and synchronize with each NPN respectively.

  NOTE 2 – This applies when a dedicated USM function is deployed in a given customer's NPN.

– The PN is required to support the identification of the communication modes of NPNs, such as by their pre-configuration or their identification through communication requests from NPNs, so that the PN can adapt as needed.

– The PN is required to support adaptation between different communication modes.

  NOTE 3 – Adaptation applies when a given NPN adopts a communication mode different from that of the PN.

NOTE 4 – Adaptation can include, but is not limited to, modification of the parameters in the HTTP header.

– The PN is required to identify and process abnormal traffic from NPNs according to the operator's policy.

NOTE 5 – Examples of abnormal traffic in a given operator's policy include unknown users and traffic carrying sensitive information.

NOTE 6 – A firewall may be used by the PN to identify and process abnormal traffic from NPNs. The types and processing policies of abnormal traffic may be configured on the firewall.

– Traffic from high-priority NPNs is recommended for processing first by the PN.

NOTE 7 – This is particularly beneficial in the case of a signalling storm or large amounts of traffic from NPNs.

NOTE 8 – The priority of NPNs may be configured in the PN, e.g., NPNs of high-value customers may receive preference.

– The PN is recommended to avoid modifying NF configuration data frequently during the deployment of new NPNs or the modification of existing NPNs.

8.2 NPN requirements

– An NPN is required to support signalling aggregation in order to reduce the number of point-to-point connections between the NFs of NPN and those of the PN.

– An NPN is required to receive the synchronization of NPN user data from the PN in order to avoid modifying them in the PN by customers.

NOTE 1 – This applies when a dedicated USM function is deployed in a given customer's NPN.

– An NPN is recommended to support high network reliability.

NOTE 2 – Network reliability for NPN indicates that it works properly also when its connection with a PN fails.

NOTE 3 – If a connection fails between NFs of the NPN and those of the PN, such as operator's DC server shut down, accidental cable breakage or NF version update in the PN, private data network services offered to NPN users, such as important production lines, will not be interrupted, minimizing the impact of the connection failure.

NOTE 4 – An NPN may deploy a dedicated NACF, SMF, ASF, USM function and UPF to support network reliability.

Appendix I

Use cases of communication between public networks and public network integrated non-public networks in IMT-2020

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

In order to meet the individual needs of private data network services, e.g., in terms of low latency, high reliability and controllability, some NFs may be deployed as dedicated in customers' DCs. Clauses I.1 to I.4 present some possible application scenarios.

I.1 UPF deployed in a customer's DC

Figure I.1 illustrates user plane function (UPF) deployed in a customer's DC.

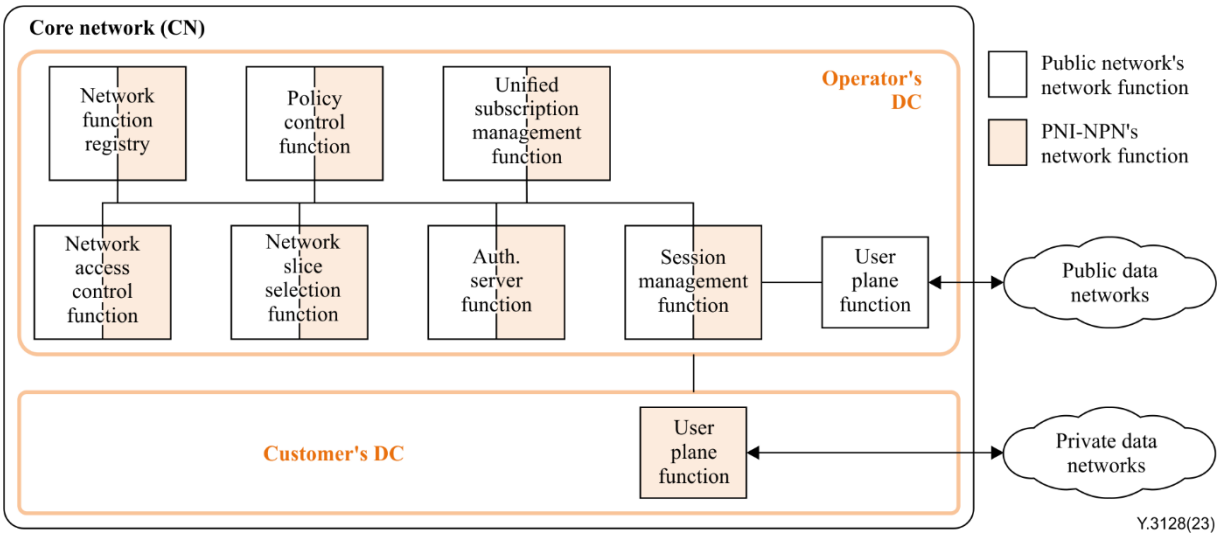

Figure I.1 – UPF deployed in a customer's DC

In order to meet the industry's requirements for low latency and to keep the user plane [b-ITU-T Y.3100] traffic in the customer's domain, the UPF may be deployed in the customer's DC. The UPF in the customer's DC communicates with the SMF deployed in the operator's DC.

I.2 NACF, SMF, PCF, UPF deployed in a customer's DC

Figure I.2 illustrates NACF, SMF, PCF, UPF deployed in a customer's DC.

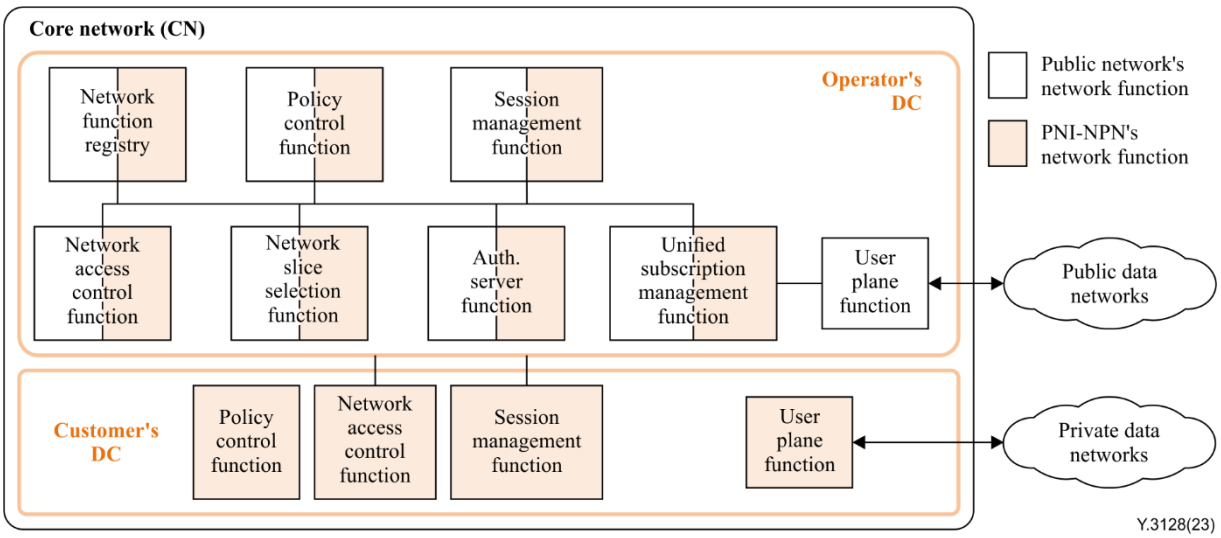

Figure I.2 – NACF, SMF, PCF, UPF deployed in a customer's DC

In addition to the low latency requirement, some customers also want to apply some policies for customized access control and session management to their users, so NACF, SMF, PCF and UPF may be deployed in the customer's DC.

In this case, there are different types of interface used for communication between the operator's and the customer's DCs.

The interfaces between the NACF and SMF in the customer's DC and the USM function in the operator's DC are used to retrieve and subscribe to user data from the USM function.

The interface between the NACF in the customer's DC and the ASF in the operator's DC is used for user authentication.

The interface between the NACF in the customer's DC and the NACF in the operator's DC is used for the NACF re-allocation procedure. If the user equipment of an industry customer initially registers with the NPN without the single network slice selection assistance information [ETSI TS 123 501], the access network selects the NACF in the operator's DC by default. The NACF in the operator's DC then initiates the re-allocation procedure for the NACF in the customer's DC.

I.3 SMF, PCF and UPF deployed in a customer's DC

Figure I.3 illustrates an SMF, PCF and UPF deployed in a customer's DC.

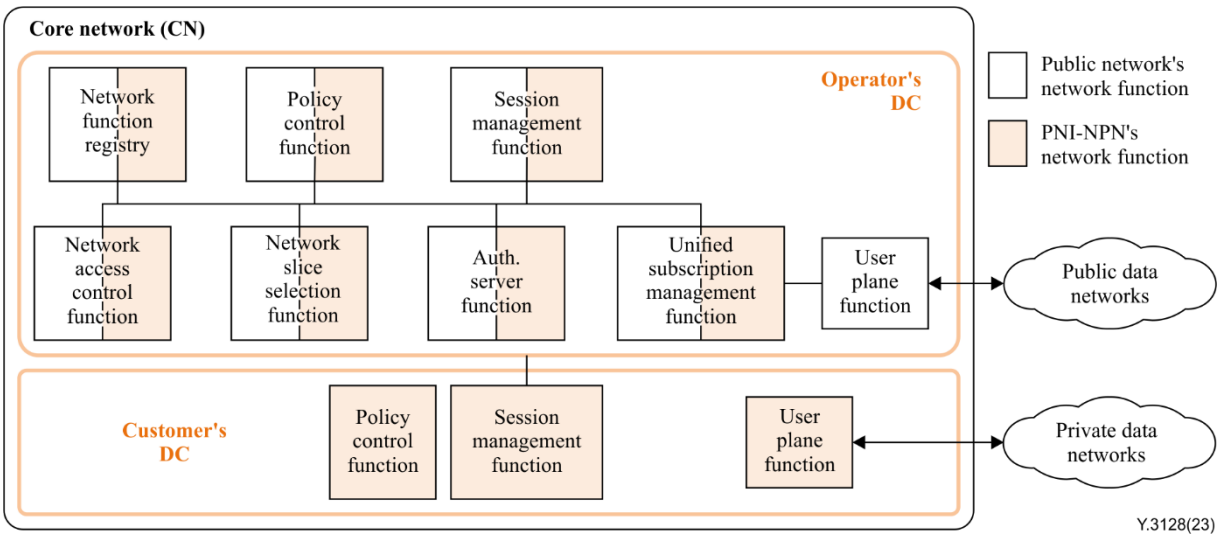

Figure I.3 – SMF, PCF and UPF deployed in a customer's DC

Some vertical industry customers are mainly concerned with session management policy control, low latency and keeping the user plane traffic in the customer's domain, so only SMF, PCF and UPF may be deployed in a customer's DC.

The SMF in the customer's DC retrieves user data from the USM function in the operator's DC and communicates with the NACF in the operator's DC while establishing protocol data unit (PDU) sessions.

I.4 ASF, USM function, NACF, SMF and UPF deployed in a customer's DC

Figure I.4 illustrates an ASF, USM function, NACF, SMF and UPF deployed in a customer's DC.

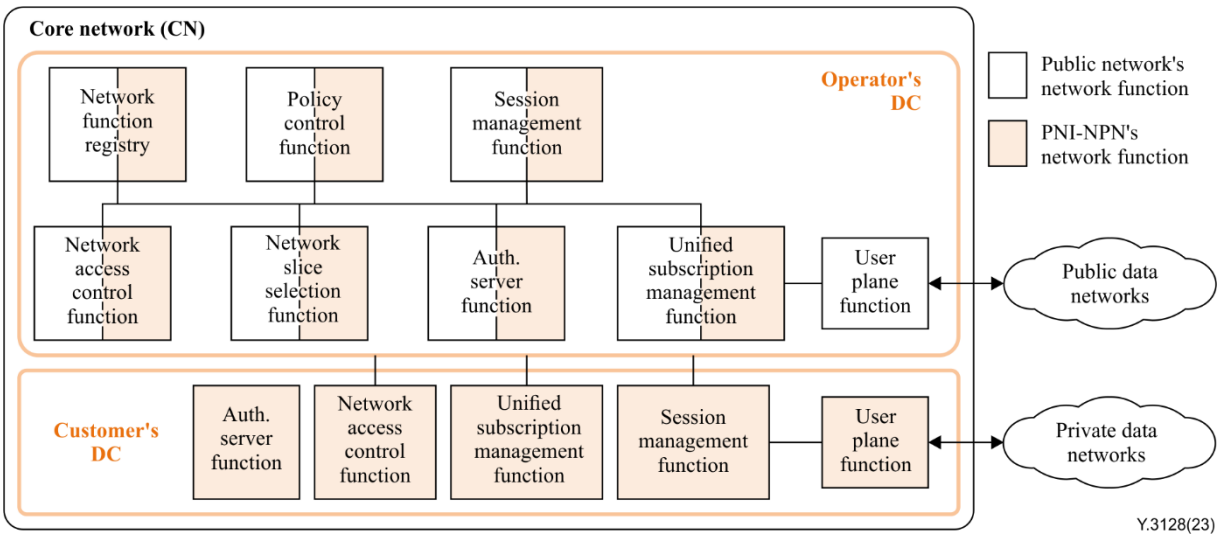

Figure I.4 – ASF, USM function, NACF, SMF and UPF deployed in a customer's DC

To maintain normal running if the connection between the DCs of the operator and customer breaks down, the ASF, USM function, NACF and SMF are deployed in the NPN.

In this case, the NACF and SMF in the customer's DC communicate with the USM function and ASF in the operator's DC when the connection between the NPN and PN works. When the connection between the NPN and the PN breaks down, NACF and SMF in the customer's DC still communicate with the USM function and ASF in the customer's DC keeping the NPN ongoing: not

only the registered devices and the established PDU session can operate, but also a new device can access the NPN. The data between the USM function and ASF in the operator's DC and the USM function and ASF in the customer's DC are synchronized unidirectionally, i.e., only the synchronization of the USM function and ASF in the operator's DC with the USM function and ASF in the customer's DC is allowed. Meanwhile, for security purposes, the user data of the ASF and USM function in the customer's DC cannot be modified by the customer.

The NACF re-allocation procedure is the same as that described in clause I.2.

Bibliography

[b-ITU-T Q.1741.7] Recommendation ITU-T Q.1741.7 (2011), *IMT-2000 references to Release 9 of GSM-evolved UMTS core network.*

[b-ITU-T X.1813] Recommendation ITU-T X.1813 (2022), *Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low-latency communication (URLLC) in IMT-2020 private networks*.

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

[b-ITU-T Y.3102] Recommendation ITU-T Y.3102 (2018), *Framework of the IMT-2020 network.*

[b-ETSI TS 123 003] Technical Specification ETSI TS 123 003 V17.10.0 (2023-07), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification.*

SERIES OF ITU-T RECOMMENDATIONS

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

Published in Switzerland
Geneva, 2024