International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# X.1813

(09/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

IMT-2020 Security

# Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low-latency communication (URLLC) in IMT-2020 private networks

Recommendation ITU-T X.1813

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.1813

## Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low-latency communication (URLLC) in IMT-2020 private networks


### Summary

Recommendation ITU-T X.1813 specifies the security requirements for the operation of vertical services supporting ultra-reliable low-latency communications URLLC in an IMT-2020 private network. It identifies threats and risks which arise when providing vertical services supporting URLLC in an IMT-2020 private network and describes security deployment scenarios of the IMT-2020 private network for operation of vertical services supporting URLLC. Monitoring of communication contents is out of the scope of this Recommendation.

IMT-2020 private network, also regarded as IMT-2020 non-public network (NPN), is intended for the sole use of a private entity such as an enterprise and may be deployed in a variety of configurations, utilizing both virtual and physical elements. It will deliver on speed, low latency and other benefits promised by the IMT-2020 to support next-generation applications.

In vertical services for smart factories and smart cities that use a private IMT-2020 network, many Internet of things (IoT) devices use massive machine-type communications (mMTC) and ultra-reliable low-latency communications (URLLC). These communications can be exposed to security threats and their associated risks. In addition, these threats can deteriorate the stable operation of the vertical services supporting URLLC. It cannot be guaranteed when the performance of vertical services is degraded due to these risks.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1813 | 2022-09-02 | 17 | 11.1002/1000/14991 |

### Keywords

DPI, endpoint detection and response, MEC, NPN, network monitoring, performance, private IMT-2020 network, security, UPF.


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

## FOREWORD

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

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

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

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

## NOTE

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

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

## INTELLECTUAL PROPERTY RIGHTS

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

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

## Table of Contents

# Recommendation ITU-T X.1813

## Security and monitoring requirements for operation of vertical services supporting ultra-reliability and low-latency communication (URLLC) in IMT-2020 private networks

### 1 Scope

This Recommendation specifies the security requirements for the operation of vertical services supporting ultra-reliable and low-latency communications (URLLC) in IMT-2020 private networks. It identifies security threats and risks that arise when providing vertical services supporting URLLC in IMT-2020 private networks and describes security deployment scenarios of the IMT-2020 private networks for the operation of vertical services supporting URLLC.

In this Recommendation, monitoring of communication contents is out of scope for privacy protection purposes.

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

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 5G non-public network** [b-3GPP TS 22.261]: A 5G network that is intended for private use.

**3.1.2 attack** [b-ISO13491-1]: Attempt by an adversary on the device to obtain or modify sensitive information or a service they are not authorized to obtain or modify.

NOTE 1 – Network functions (NF) include but are not limited to network node functionalities, e.g., session management, mobility management and transport functions, whose functional behaviour and interfaces are defined.

NOTE 2 – Network functions can be implemented on a dedicated hardware or as virtualized software functions.

NOTE 3 – Network functions are not regarded as resources, but rather any network functions can be instantiated using the resources.

**3.1.3 deployment** [b-ISO/IEC/IEEE 24765]: Phase of a project in which a system is put into operation and cutover issues are resolved.

**3.1.4 domain** [b-ISO/IEC 14888-1]: Set of entities operating under a single security policy.

EXAMPLE – Public key certificates created by a single authority or by a set of authorities using the same security policy.

**3.1.5 Internet of things (IoT)** [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

**3.1.6 network monitoring** [b-ISO/IEC 27033-1]: Process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis.

**3.1.7 network function** [b-ITU-T Y.3100]: In the context of IMT-2020, a processing function in a network.

**3.1.8 system** [b-ISO/IEC 27000]: Applications, services, information technology assets, or other information handling components.

**3.1.9 stakeholder** [b-ISO/PAS 19450]: Individual, organization, or group of people that have an interest in, or might be affected by the system being contemplated, developed, or deployed.

**3.1.10 trust** [b-ISO/IEC 25010]: Degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

**3.1.11 vertical service** [b-5G-PPP]: From a business perspective, a vertical service is a service focused on a specific industry or group of customers with specialized needs (e.g., automotive services, entertainment services, e-health services, industry 4.0).

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

**3.2.1 IMT-2020 communication system**: A system of managing IMT-2020 communication processes for IMT-2020 services.

NOTE 1 – 5G is referred to as IMT-2020 in the ITU-T context.

NOTE 2 – IMT-2020 communication system is identical to the IMT-2020 system in this Recommendation.

**3.2.2 IMT-2020 ecosystem**: A set of stakeholders who interact to form a stable functioning IMT-2020 system.

NOTE – The term relates to the development of 5G communication technology, where a community of stakeholders from industry and academia contribute their products, technology and expertise, to enable functionality at different layers of the 5G value stack e.g., infrastructure, network, platform, service, and application.

**3.2.3 IMT-2020 private network**: 5G non-public network (see clause 3.1.1) that utilizes both virtual and physical elements of an IMT-2020 communication system and is intended for the sole use of a private entity such as an enterprise.

**3.2.4 IMT-2020 service**: A benefit provided by the IMT-2020 ecosystem.

# 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

| | |
|---|---|
| 5GC | 5G Core |
| AMF | Access and Mobility Management Function |
| DDoS | Distributed Denial of Service |
| DPI | Deep Packet Inspection |
| EC | Edge Computing |
| EDR | Endpoint Detection and Response |
| GTP | GPRS Tunnelling Protocol |

| | |
|---|---|
| IoT | Internet of Things |
| MEC | Multi-access Edge Computing |
| MEC DP | MEC Data Plane |
| mMTC | massive Machine-Type Communications |
| NF | Network Function |
| NMCF | Network Monitoring Client Function |
| NMF | Network Monitoring Function |
| NMSF | Network Monitoring Server Function |
| NPN | Non-Public Network |
| PLMN | Public Land Mobile Network |
| RTT | Round Trip Time |
| SBA | Service-Based Architecture |
| SMF | Session Management Function |
| UDM | Unified Data Management |
| UE | User Equipment |
| UID | User ID |
| UPF | User Plane Function |
| URLLC | Ultra-Reliable and Low-Latency Communication |

## 5 Conventions

This Recommendation uses the following conventions:

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.

## 6 Overview

IMT-2020 system is architected to support network operators for data connectivity and services based on techniques such as network function virtualization and software defined networking. A service-based architecture (SBA) is defined by 3GPP [b-3GPP TS 23.501], whereby the control plane functionality and common data repositories of the IMT-2020 network are delivered by way of a set of interconnected network functions (NFs), each having the authorization to access each other's services. Figure 1 depicts the IMT-2020 system architecture.

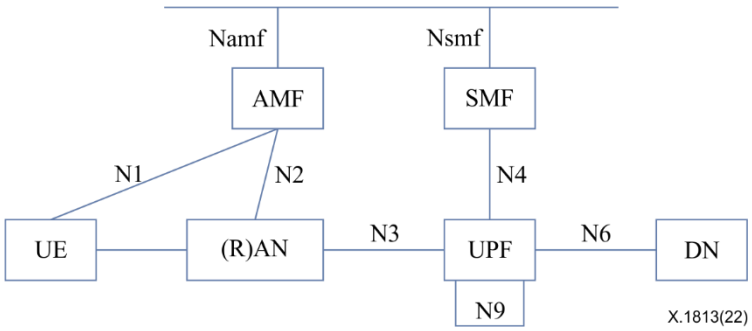


**Figure 1 – IMT-2020 system architecture**

IMT-2020 system architecture defined in [ITU-T Y.3102] and also [b-3GPP TS 23.501] consists of the following network functions:

– Access and mobility management function (AMF) which provides registration management function, connection management function, mobility management function, access authentication function, access authorization function, location services management function, user equipment (UE) mobility event notification function, etc.

– Data network (DN), e.g., operator services, Internet access or third-party services.

– Session management function (SMF) which provides session establishment, modification and release functions, user equipment (UE) IP address allocation and management functions, selection and control of user plane function, charging data collection and support of charging interfaces, control and coordination of charging data collection at the user plane function (UPF), downlink data notification, support of header compression, etc.

– User plane function (UPF) handles the user plane path of the protocol data unit (PDU) sessions. 3GPP supports deployments with a single UPF or multiple UPFs for a given PDU session. UPF selection is performed by the SMF. UPF provides allocation of user equipment (UE) IP address / prefix in response to the SMF request, packet routing and forwarding function, packet inspection function, QoS handling for the user plane, downlink packet buffering and downlink data notification triggering, etc.

– Namf: Namf identifies a service-based interface for the core access and mobility management function.

– Nsmf: Nsmf identifies a service-based interface for the session management function.

– UE: User equipment.

– (R)AN: (Radio) access network.

The IMT-2020 system architecture contains the following reference points:

– N1: Reference point between the UE and the AMF.

– N2: Reference point between the (R)AN and the AMF.

– N3: Reference point between the (R)AN and the UPF.

– N4: Reference point between the SMF and the UPF.

– N6: Reference point between the UPF and a data network (DN).

– N9: Reference point between two UPFs.

IMT-2020 private networks are intended for the sole use of a private entity such as an enterprise, and may be deployed in a variety of configurations, utilizing both virtual and physical elements of the IMT-2020 communication systems. An IMT-2020 private network shall be built on the IMT-2020 system architecture principles as defined in [b-3GPP TS 23.501], which include flexibility and modularity for newly introduced functionalities. The functional architecture for an IMT-2020 private network is illustrated in Appendix I.

3GPP specifications [b-3GPP TS 23.501] foresees a variety of private network deployment scenarios. At the highest level, private networks can be divided into two categories:

– IMT-2020 private networks deployed as completely isolated, standalone networks;

– IMT-2020 private networks deployed as a slice of a public land mobile network (PLMN) in conjunction with a public network.

Whereas, Internet of things (IoT) is defined [b-ITU-T Y.4000] as a global infrastructure for information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies. In this Recommendation, the main use case for such vertical services is the IoT service. In this context, IoT devices could be the representative devices of UEs defined by 3GPP [b-3GPP TS 22.261].

As IMT-2020 technology has entered a commercialization stage, IMT-2020 private network will be mainly used to build IMT-2020 vertical services with industrial IoT devices, such as services for smart factories and smart cities that require real-time performance with ultra-reliable and low-latency communication (URLLC). Therefore, IMT-2020 private networks must satisfy various requirements in terms of security and performance as it processes time-sensitive data in accordance with [ITU-T Y.3102]. Figure 2 illustrates the overall security architecture of IMT-2020 private networks in accordance with [b-3GPP TR 23.734].

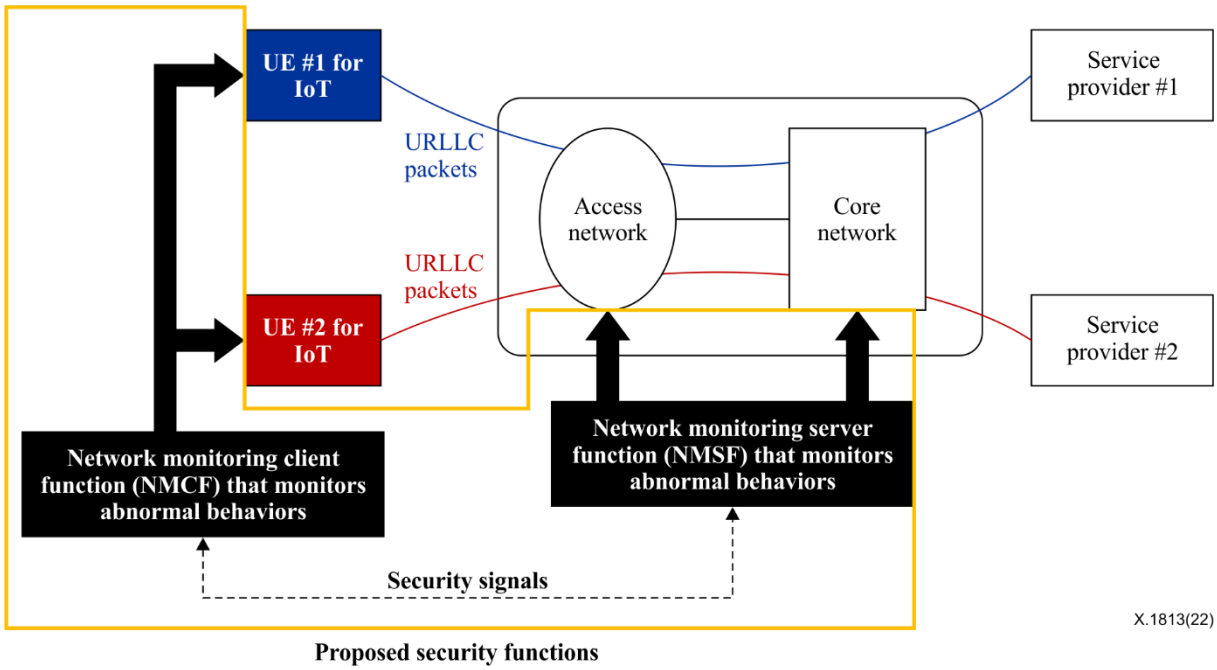


**Figure 2 – Security architecture of IMT-2020 private networks**

Referring to Figure 2, the security architecture of IMT-2020 private network enables operators to monitor security / performance for communications between network nodes and end point user equipment in an IMT-2020 private network for the operation of vertical services supporting URLLC.

## 7 Threats to vertical services supporting URLLC in IMT-2020 private networks

IoT spans a wide variety of new and exciting opportunities, such as industrial automation and control systems (IACS), autonomous vehicle communications, smart grids, highway / traffic sensors, drone communications, medical sensors, and AR/VR, mostly operated in an automated manner. IoT services might also have to meet URLLC characteristics for IMT-2020 service. According to [b-3GPP TS 22.261], private networks are intended for the sole use of a private entity such as an enterprise, and only authorized UEs shall have the right to access a private network.

In such an environment, threats to vertical services among other things are identified as any attacks that can harm components and interfaces of IMT-2020 private network in latency aspects. IMT-2020 private network can be deployed with or without a UPF / multi-access edge computing (MEC). UPF is internet accessible via the N6 interface defined by 3GPP. Therefore, if an IMT-2020 private network is deployed with a UPF and MEC, the N6 interface has significant attack exposure since attackers anywhere on the internet can access it. Such attacks take place intentionally or unintentionally from outside or inside an IMT-2020 private network.

Threats to UPF, MEC and N6 interface can be listed as follows:

– Distributed denial of service (DDoS) attacks.

– Spying on traffic / data for communication links.

– Unexpected increased traffic or abnormal traffic generated by UEs in an IMT-2020 private network.

IMT-2020 private network is privately deployed with network components and interfaces, and parts of them are new and different from those of existing networks in the security aspect. N3 interface connecting the access and core networks uses IPsec for transport security. The N4 interface connects the UPF and AMF. This N4 interface is closed in a 4G evolved packet core (EPC), but not in IMT-2020 vEPC. Compared to the X6 interface, N3 and N4 interfaces are not internet accessible, however, there is a possibility that new types of unintentional threats and obstacles may occur.

Threats to N3 and N4 interfaces can be listed as follows:

– Insufficient access control methods implemented in an IMT-2020 private network.

– Limitations in the security measures and procedures implemented by an operator of an IMT-2020 private network.

– Poorly designed or misconfigured network components in the IMT-2020 private network, that does not account for a sudden increase in access.

The lack of experts not accustomed to many new features of the IMT-2020 network may also act as an unintentional threat and obstacle.

## 8 Risks for vertical services supporting URLLC in IMT-2020 private networks

IMT-2020 private network basically provides a highly trusted network in the IoT infrastructure because IMT-2020 private network has been standardized by the 3GPP for security purposes for emerging IMT-2020 vertical services.

Despite the conventional security methods of authentication, authorization and data confidentiality, which are provided by 3GPP and other security standards, an IMT-2020 private network can still be exposed to numerous risks. For example, existing security methods cannot get rid of threats due to the abnormal behaviour of UEs camping on an IMT-2020 private network.

Since IMT-2020 networks possess stronger software-centric features, they may be exposed to a greater number of software related risks such as software development flaws, incorrect update procedures and configuration errors. As a result, an IMT-2020 network may face performance degradation due to the various risks mentioned above.

In this context, the impact of these risks may include:

– Unstable and dangerous operation of vertical services: Abnormal behaviour of IoT devices camping on an IMT-2020 network may pose a threat to the normal operation of a smart city infrastructure.

– Destruction, modification, or alteration of information stored or communicated within the infrastructure of an IMT-2020 network.

– Performance degradation of IMT-2020 URLLC service: If an IMT-2020 network cannot guarantee the IMT-2020 URLLC service requirement of low latency, the network may then face performance degradation, which would result in a negative impact on the associated time-sensitive vertical services. For example, as smart factories are designed according to URLLC requirements, production quality or speed may be degraded if low latency requirements are not met. This may not only lead to a huge economic loss but can also cause safety accidents. Another example would be the image quality for security cameras can significantly be degraded due to the connection delay of various sensors.

Thus, security requirements for the operation of vertical services supporting URLLC in IMT-2020 private networks need to be developed to address the aforementioned threats and risks.

## 9 Deployment scenarios of security functions for operation of vertical services supporting URLLC in IMT-2020 private networks

This clause identifies deployment scenarios of security functions for the operation of vertical services supporting URLLC in an IMT-2020 private network. IMT-2020 private network security architecture is configured by network monitoring functions (NMFs). NMF consists of a network monitoring server function (NMSF) and a network monitoring client function (NMCF). NMFs can be implemented by a deep packet inspection (DPI) function deployed in a network node or by a dedicated DPI network node.

NMSFs can be configured as independent network nodes separated from UPF or MEC. Specifically, NMSFs shall be coupled either to the input or output of a UPF or MEC so that they can monitor packets thereof.

There are three deployment scenarios of NMSFs as follows:

A) NMSF integrated as a node in the MEC.

B) NMSF implemented as a separate node to monitor packet output from the UPF.

C) Multiple NMSFs are configured such that a first NMSF is integrated as a node in the MEC and a second NMSF is implemented as a separate node to monitor packet output from the UPF.

In these three deployment scenarios, whether the NMSF(s) is allocated designated IP(s) or not is an implementation issue. NMCF is integrated into the UE in all these three deployment scenarios.

Figure 3 depicts the deployment scenario A in the IMT-2020 private network security architecture where multiple NMCFs and the NMSF are configured.

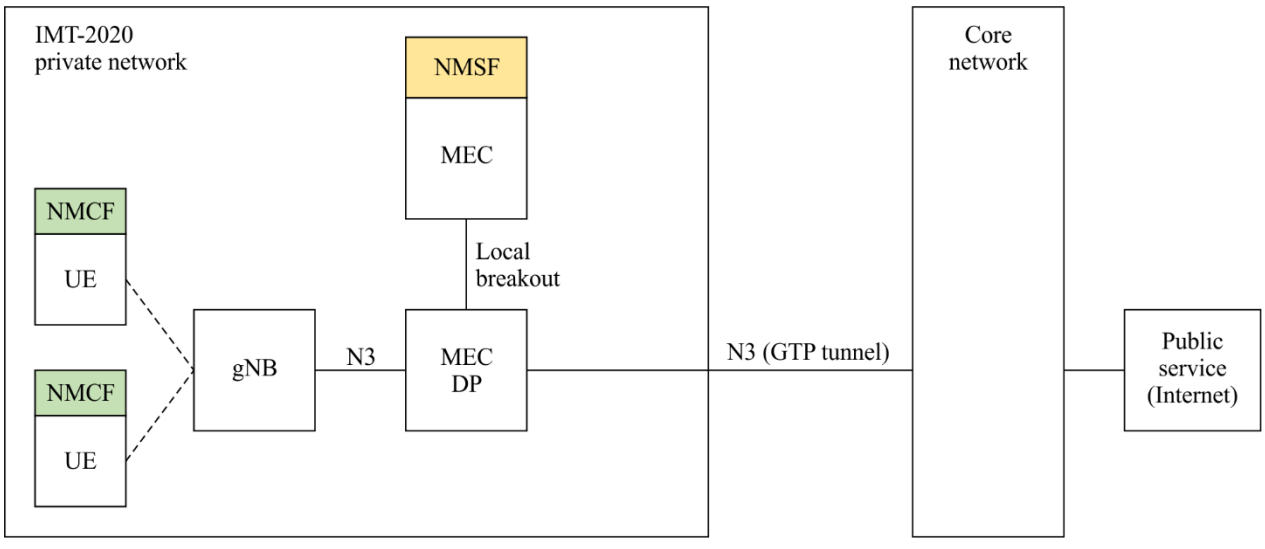


**Figure 3 – Deployment scenario A**

With reference to Figure 3, NMCFs may be integrated into their respective UEs, IoT devices in particular, communicating with a gNB. Mounting NMCFs on IoT devices is one of the effective solutions guaranteeing security and URLLC performance in the IMT-2020 private network. NMCF may be implemented in softwares and may also be referred to as an endpoint detection and response (EDR) entity or a micro engine (ME). The NMCF server may be located inside the IMT-2020 private network or an edge cloud or a public network domain (Internet). The UEs are wirelessly connected to the gNB. Each UE transmits packets to the gNB or receives packets from the gNB. The gNB is connected to the IMT-2020 core network or to a local network via N3 and N4 interfaces. The packets flow through the N3 and N4 interfaces.

If an IP address is assigned to the NMSF, then NMCF and NMSF communicate with each other via N3 and N4 to exchange security signals between NMCF and NMSF such as the monitoring result at the NMCF.

In case of scenario A, although not shown in Figure 3, additional NMSF can be integrated into the MEC data plane (MEC DP) as well, so that two NMSFs can monitor both private network traffic and public network traffic to or from the UE. NMSF can also be configured as an independent entity separated from MEC.

Figure 4 depicts the deployment scenario B in the IMT-2020 private network security architecture where multiple NMCFs and the NMSF are configured.

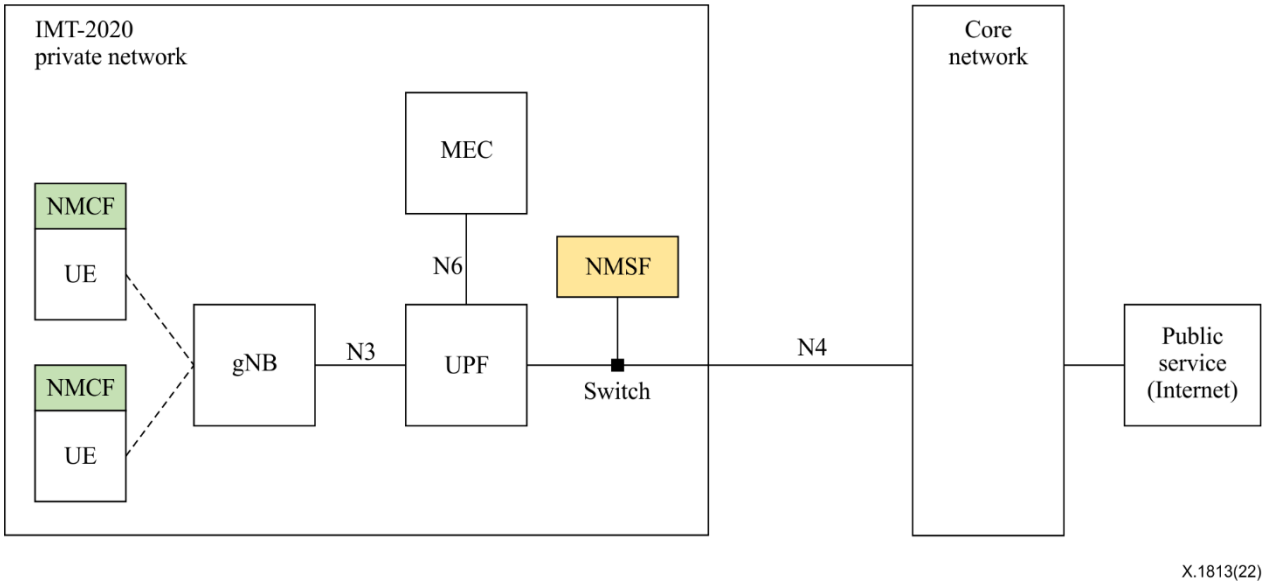


**Figure 4 – Deployment scenario B**

With reference to Figure 4, NMSF is implemented as a separate node outside the UPF to monitor packets that are output from the UPF. A switch can be used to mirror packets from the UPF. If an IP address is assigned to NMSF, then NMCF and NMSF communicate with each other via N3 and N4 to exchange security signals such as the monitoring result generated at the UE (client node). If the IMT-2020 private network uses a node-to-node encryption function such as an IPSec, NMSFs can be configured at a point where decrypted packets are output from the node.

Figure 5 depicts the deployment scenario C in the IMT-2020 private network security architecture where multiple NMFs are configured.

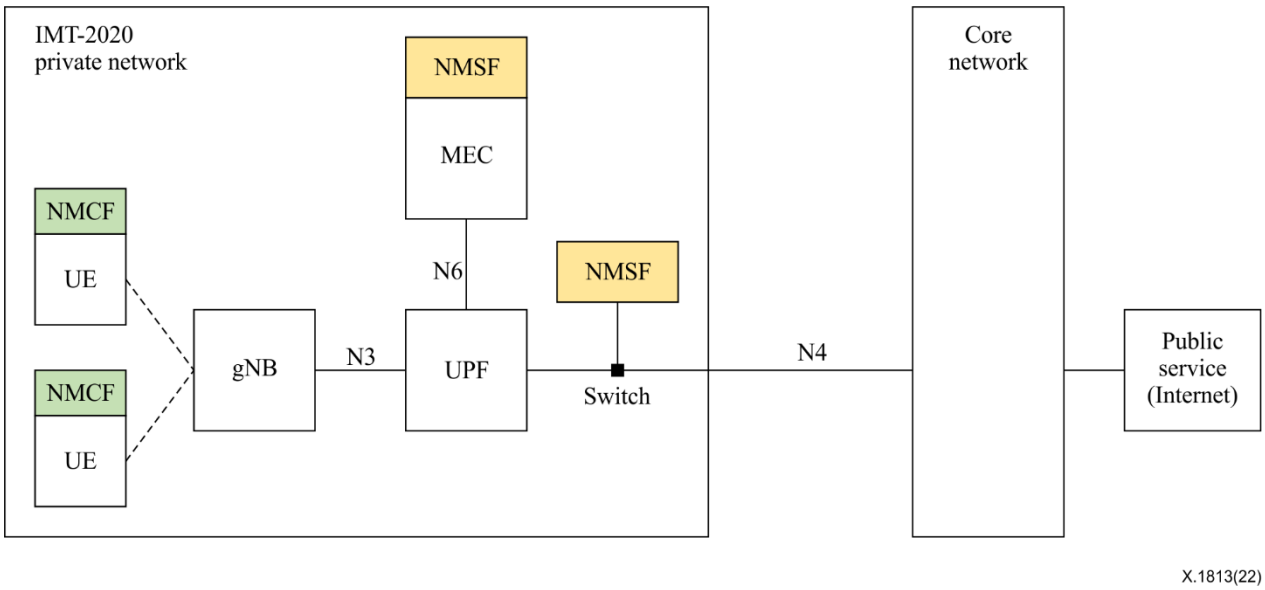


**Figure 5 – Deployment scenario C**

With reference to Figure 5, NMSF is not only integrated into MEC but also implemented as a separate node outside the UPF to monitor packets that are output from the UPF. If IP addresses are assigned to NMSFs respectively, then NMCF and NMSFs communicate with each other via N3 and N4 to exchange security signals such as the monitoring result generated at the UE (client node). If the IMT-2020 private network uses a node-to-node encryption function such as IPsec, NMSFs can be configured at a point where decrypted packets are output from the node.

The three scenarios above are not mutually exclusive, and which mode to use depends on the cost or network characteristics, etc. Various deployments of NMSFs and NMCFs are also possible. For example, NMSFs can be integrated into any of the network nodes along with the UPF and/or MEC.

Therefore, from the perspective of a network functional architecture, security and performance monitoring may be performed by using NMSF mounted on MEC and/or UPF and NMCF mounted on the IoT devices, and a signalling protocol between NMSF and NMCF.

## 10 Security and monitoring requirements for operation of vertical services supporting URLLC in IMT-2020 private networks

This clause identifies security and monitoring requirements for operation of vertical services supporting URLLC in an IMT-2020 private network. An IMT-2020 private network requires a higher level of security and performance compared to conventional networks due to the large amounts of data being exchanged between numerous client devices / sensors, and central servers that control them. In addition, the requirements of IMT-2020 URLLC must also be met at the edge in accordance with [ITU-T Y.3102].

For IMT-2020 private network deployment scenarios with NMSF(s) and NMCF, general security and monitoring requirements for the operation of vertical services supporting URLLC include the following:

a) It is required to monitor and detect the abnormal behaviour of UEs and IMT-2020 private networks to mitigate security risks.

b) It is required to monitor the performance of vertical services supporting URLLC.

c) It is required to alert the network administrator about the abnormal behaviour of UEs and IMT-2020 private networks so that issues can be resolved and URLLC capabilities are restored on time.

Optionally, it is recommended to visualize abnormal behaviours of UEs and IMT-2020 private networks so that these abnormal behaviours are resolved more effectively. The visualization of monitoring results is described in Annex C.

### 10.1 Security for NMSF

The security for NMSF include the following:

a) It is required that NMSF provide at least a function of mirroring packets transmitted and received between a client node and a server node, thereby obtaining at least one mirrored packet. The client node is a UE or an IoT device. Packet mirroring is a technique that collects and analyses packets exchanged in a specific node in real-time. NMSF can have a switching function for packet mirroring.

b) It is required that NMSF determine abnormal behaviours or security problems that threaten the security and performance of an IMT-2020 private network based on the information included in the mirrored packets.

c) If an IP address is assigned to an NMSF, it is required that the NMSF receives a security check packet using a TCP packet format from NMCF and calculates the round trip time (RTT) based on the received security check packet.

The security check packet using a TCP packet format is shown in Figure 6.

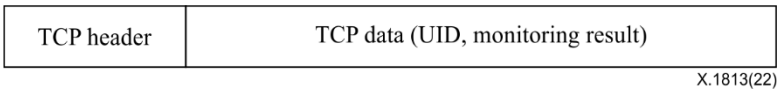


**Figure 6 – Security check packet using a TCP packet format**

**Table 1 – Fields of security check packet**

| Field | Byte length | Description |
|---|---|---|
| User ID (UID) | 4 | This field indicates a user ID of UE. |
| Length | 2 | This field indicates the byte length of the monitoring result field. |
| Monitoring result | Variable | This field indicates the alive information, CPU usage and memory usage of a UE. |

d) If an IP address is not assigned to NMSF, it is required that NMSF mirror a security check packet using a user datagram protocol (UDP) packet format transmitted from NMCF to a server node and calculates the round trip time (RTT) based on the mirrored security check packet.

The security check packet using a UDP packet format is shown in Figure 7.

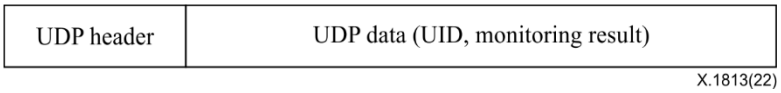


**Figure 7 – Security check packet using a UDP packet format**

**Table 2 – Fields of security check packet**

| Field | Byte length | Description |
|---|---|---|
| UID | 4 | This field indicates a user ID of UE. |
| Length | 2 | This field indicates the byte length of the monitoring result field. |
| Monitoring result | Variable | This field indicates the alive information, CPU usage and memory usage of a UE. |

e) It is recommended that NMSF provide alerting abnormal behaviours that obstruct URLLC requirements based on the security and performance status. When an abnormal behaviour threatening security and performance is detected, NMSF alerts the user so that the user can respond properly to the abnormal behaviour. Then, NMSF sends an alerting information to a security controller which instructs the security controller to take proper measures for the abnormal behaviour, i.e., shutting down the network. The alerting information is sent via N3 and N4 interface which is provided by the 3GPP signalling protocol.

Detailed features of NMSF mirroring-based performance / security monitoring can be performed by the normative algorithm of Annex A.

## 10.2 Security for NMCF

The security for NMCF include the following:

a) NMCF is required to operate on the computing resources of individual client nodes or IoT sensors and is recommended to use the minimum number of resources such that the functions perform in an appropriate manner.

b) NMCF is required to collect packets or internal information transmitted or received by client nodes over the network.

c) NMCF is required to monitor and determine a network security threat associated with the client node including NMCF itself based on the collected packets or internal information. If a value indicated by the internal information is equal to or greater than a threshold, NMCF determines that there is a network security threat. Examples of internal information include CPU usage of a client node, memory usage of a client node, etc.

d) If an IP address is assigned to NMSF, NMCF is required to generate a security check packet using a TCP packet format including the monitoring result shown in Figure 6 and sends the security check packet to NMSF.

e) If an IP address is not assigned to NMSF, NMCF is required to generate a security check packet using a UDP packet format including the monitoring result shown in Figure 7 and sends the security check packet to a server node so that NMSF can mirror the security check packet.

f) NMCF is recommended to display an alert of any abnormal UE operation to a user of IoT devices.

In the case of NMCF, it is more likely to collect more accurate data; the NMCF may also stop operating in the occurrence of a problem where, for example, power of equipment in a normal operation is turned off. Therefore, performance and security monitoring by NMSF is essential.

However, monitoring every data flow of a lot of UEs connected to the IMT-2020 private network may be a large burden on the NMSF, and in this case, collaboration with the NMCF is needed to effectively monitor threats to the network.

Detailed features that implement the requirements of the NMCF can be performed by the normative algorithm of Annex B.

# Annex A

## NMSF characteristics

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

According to the present recommendation, based on mirrored packets or information related to mirrored packets, NMSF determines the occurrence of abnormal behaviours threatening security and performance. NMSF determines the occurrence of abnormal behaviours by calculating indices or parameters related to the performance or security of the IMT-2020 private network and comparing the calculated results with reference values according to the communication service requirements (IMT-2020 or LTE). Here, communication service requirements may be known from the access information of an IoT device.

Figure A.1 shows a method for measuring round trip time (RTT) using a mirrored packet as an indicator related to the performance or security of IMT-2020 private network and determining abnormal behaviours threatening the security and performance of the IMT-2020 private network based on the RTT.

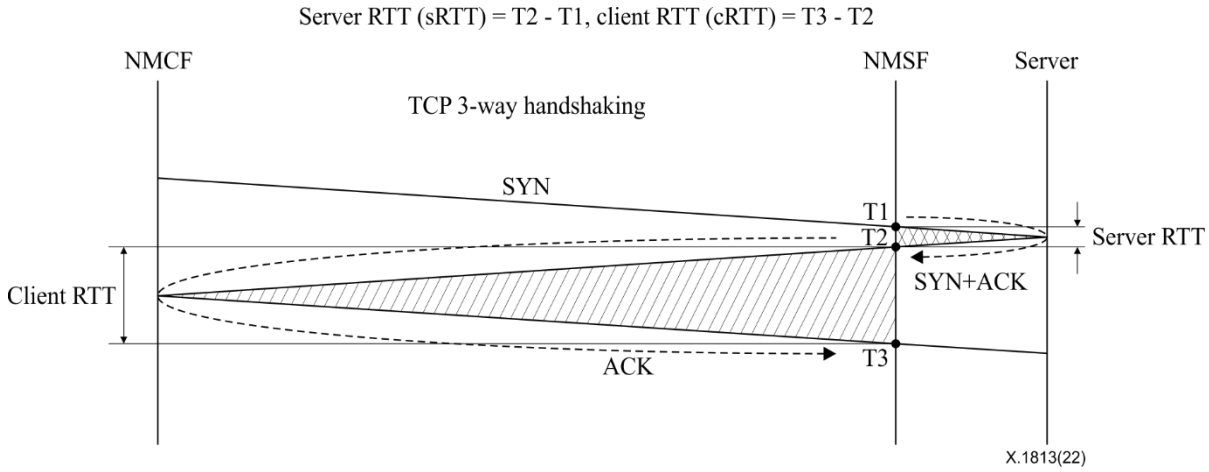


**Figure A.1 – RTT measurement**

With reference to Figure A.1, in the 3-way handshake scenario with respect to transmission and reception of a synchronization signal (SYN), NMSF calculates the RTT of a network by using mirrored packets between a user and a server over the network. For example, after extracting and storing transmission and reception time points of three packets (SYN, SYN + ACK, and ACK) exchanged between NMCF (namely, a client) and NMSF server (or MEC), NMSF secures at least one piece of time information among T1, T2, and T3. NMSF calculates the RTT (sRTT) due to the NMCF server by subtraction of T1 from T2 (T2 – T1), calculates RTT (cRTT) due to the client from T3 – T2, and calculates the total network RTT from sRTT + cRTT or T3 – T1. By performing the calculation for each transaction, NMSF calculates the RTT of the whole network.

NMSF analyses the existence of threats to the performance or security of the IMT-2020 private network by determining whether sRTT, cRTT, and network RTT satisfy URLLC requirements of the IMT-2020 private network. Figure A.2 shows how to identify performance deterioration regions by using sRTT and cRTT in the IMT-2020 private network.

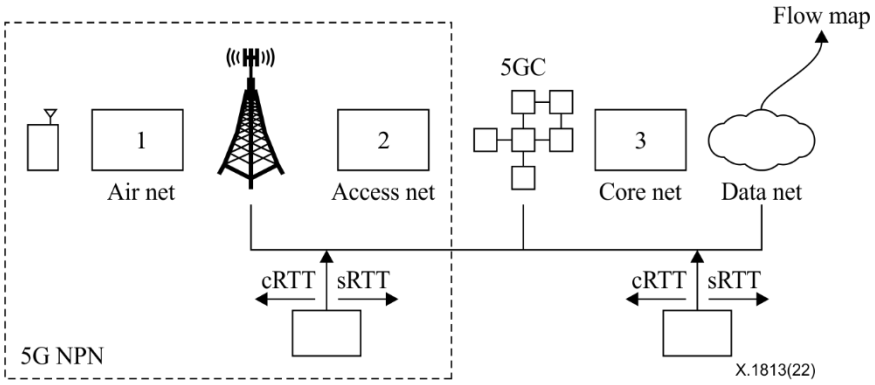


**Figure A.2 – Identifying performance deterioration regions in an IMT-2020 private network**

In addition to RTT, various other indices may be used as an index for determining performance or a security threat. Typical examples of the index include, response waiting time information representing the response latency time until the NMSF server (or MEC) receives first data associated with content from a URL associated with a request of a client for the content; response waiting session number information representing the number of sessions in a state not receiving a response to a request sent from the client; BPS, CPS, TPS, HTTP 40x or 50x error; information on data transmission and reception obtained from a mirrored packet; statistics information obtained from a plurality of mirrored packets; and alive information representing the possibility of connecting to an IoT device or NMCF server.

By using these indices, an algorithm for determining performance and security threats may be implemented in various ways. For example, NMSF determines the existence of a network security threat based on the traffic information (OSI 3 or OSI 4 layer) including information on a packet flow and information on a protocol (OSI 7 layer).

In addition to the above, various techniques may be adopted, including security threat detection based on packet information for detecting a network security threat (for example, when the number of connections over a section from a predetermined source IP to a destination IP, or BPS of a server, or a request for a URL, exceeds a predetermined threshold value, it is determined as a security threat), security threat detection based on traffic information (for example, using a clustering technique based on a traffic distribution graph in order to determine that traffic exceeding a predetermined threshold value has occurred, it is then determined that a security problem has occurred in a IMT-2020 private network), security threat detection based on protocol information, anomaly-based detection, signature-based detection or misuse-based detection, stateful protocol analysis detection, and specification-based detection. Communication content between NMCF and NMCF servers may also be included in the analysis content of NMSF.

# Annex B

## NMCF characteristics

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

For the integration of the NMCF server and NMSF, a protocol for exchanging information related to the security between NMCF (or NMCF server) and NMSF is required.

Firstly, NMCF determines whether there exists a network security threat by using the states of IoT devices required for its own service, system state or log information, and the RTT. The state of an IoT device required for the service includes CPU load, memory usage, storage usage and alive information. For example, when memory usage is equal to or larger than a preconfigured threshold value or the RTT is larger than a preconfigured threshold value, NMCF determines that abnormal behaviour threatening the security and performance has occurred. Another example includes, when the log information indicates that an entity whose IP is prohibited has tried to login to a client node, or that an unknown process has taken place, then NMCF determines that abnormal behaviour threatening the security and performance has occurred.

NMCF then transmits the determined monitoring result value about whether there exists a security threat to the NMCF server or NMSF. In other words, NMSF receives a monitoring result about a network security threat as perceived by an endpoint in real-time. At this time, an IoT device should be identified from the information collected by the NMCF server with respect to the NMCF and analysis content of the NMSF so that the content generated by the same IoT device may be distinguished from the others.

The method described above may reduce a burden on the central NMSF by performing threat monitoring at endpoints such as NMCF and as a result, may improve the monitoring performance against network performance and security threats.

# Annex C

## Visualization of monitoring results

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

Figure C.1 illustrates an example of visualization of network / system performance and security monitoring using NMSF.

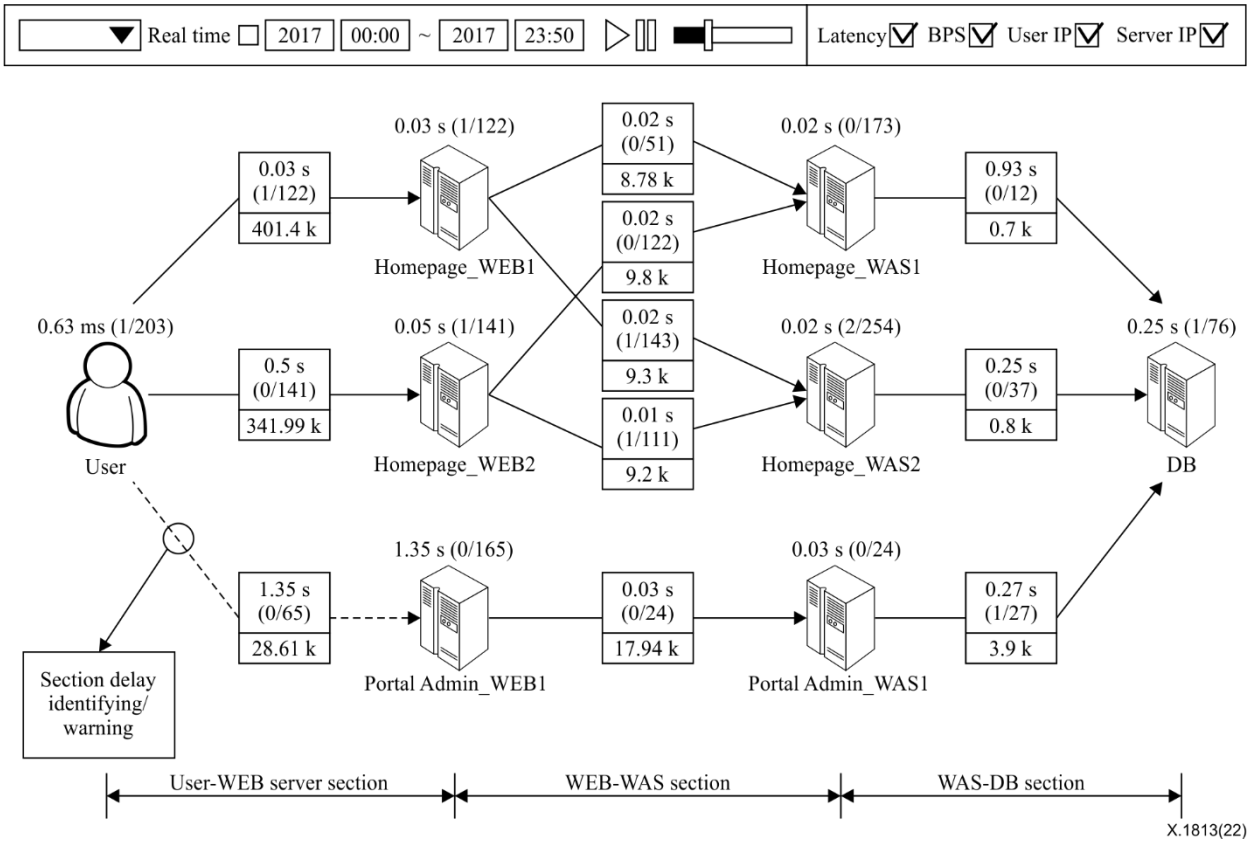


**Figure C.1 – Example of visualization of network / system performance and security monitoring**

With reference to Figure C.1, analysed results based on performance indicators or security indicators are visualized in real time and then provided to users as an alarm. The network managers are able to cope with threats immediately by using these results. That is, the analysed results are interpreted in terms of performance and security perspective. As soon as abnormal behaviours are detected the warning sign goes to the network managers.

It is desirable that visualization intuitively and clearly expresses links between entities in a network. Visualization is implemented such that the NMSF generates performance and a security related indicator as an object, implements the generated object in a visualized space, and generates a flow map that represents the traffic flow of the network. For this, objects shall be obtained by generating performance / security related indicators in association with a first entity, generating performance / security related indicators in association with a second entity, and generating performance / security related indicators in association with a link connecting the first entity and the second entity.

To improve clarity, a line between the first entity and the second entity is represented on the flow map based on the objectification of the performance / security related indicators in association with the links. Colour elements can be added for distinction. In other words, at least one from among the colours, shapes and thickness is distinctively visualized according to the performance / security related indicators in association with the links.

By using this visualization function, visibility, and clarity throughout all the service sections can be achieved. It not only improves the prevention of network service problems by managing them, but it gives the network the ability to easily cope with the threats in a vast IoT infrastructure such as smart factories and smart cities.

# Appendix I

## Use cases of IMT-2020 private network for vertical services

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

This Recommendation is based on three types of IMT-2020 private network architecture as shown in Figure I.1.

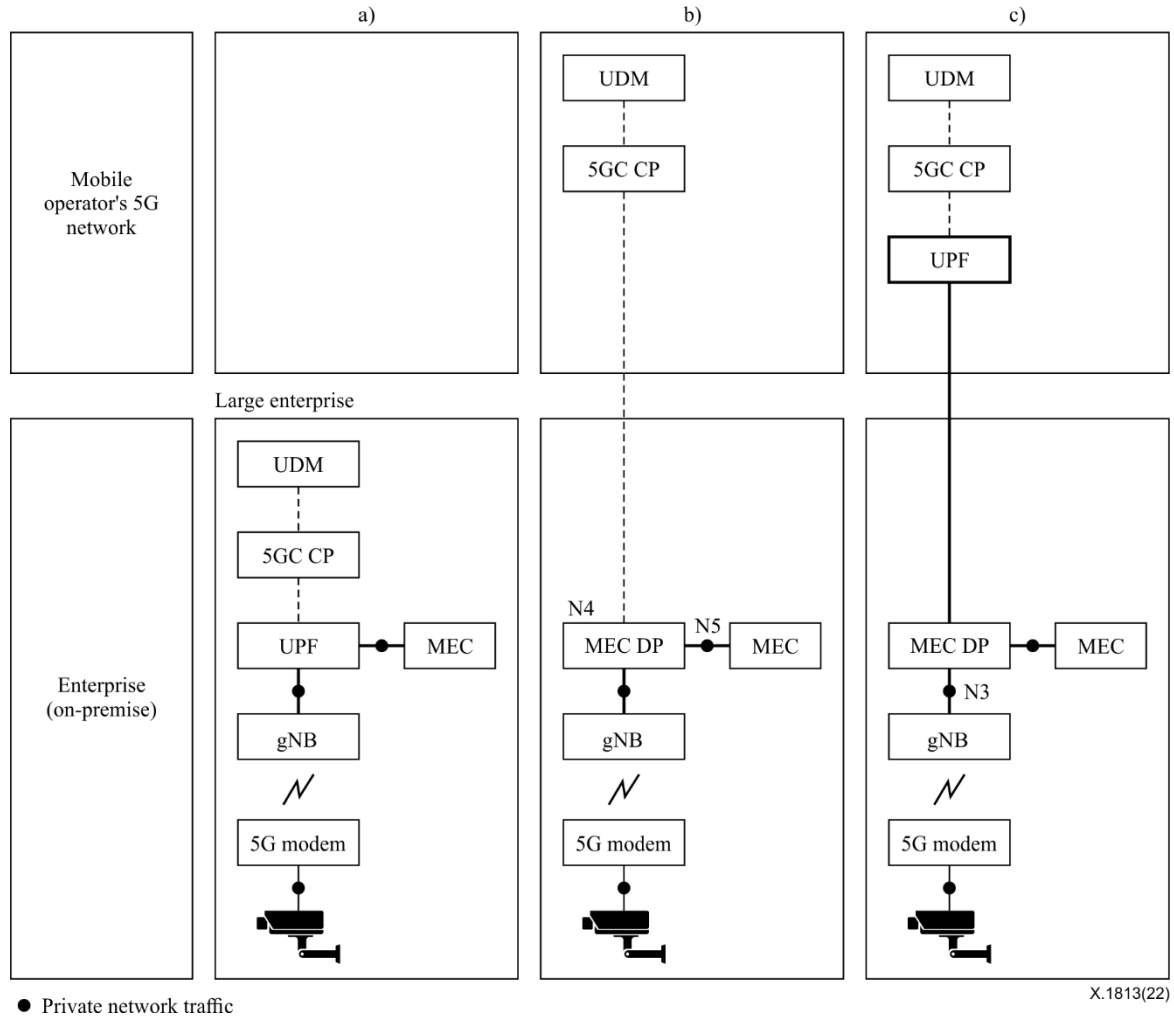


**Figure I.1 – Three types of IMT-2020 private network deployment**

According to [b-Harrison], IMT-2020 private networks can be deployed as completely isolated (a), standalone networks or can be deployed as a slice of a PLMN in conjunction with a public network (b or c) as shown in Figure I.1.

With regard to (a), the private network is physically separated from the public network, providing complete data security. Since the network delay between the device and the application server is within several ms, URLLC application services can be implemented.

With regard to (b), gNB, UPF and MEC are deployed inside the enterprise. In this architecture, RAN and the control plane is shared between private and public networks, and enhanced security and delay reduction can be provided.

With regard to (c), gNB, MEC data plane (DP), and MEC are deployed inside the enterprise, and the UPF is located in the edge cloud of the mobile operator far from the devices. The MEC DP looks at the destination IP addresses of the packets belonging to all the GPRS tunnelling protocol (GTP) tunnels coming up from the gNB (GTP decap) and routes the user IP packet to the internal private network if it is local traffic. In this architecture, enhanced security and delay reduction can be provided.

According to [b-Harrison], deployment type (b) of Figure I.1 can be depicted as Figure I.2 from the vertical view using network slicing. Figure I.2 illustrates a detailed functional architecture for deployment type (b) in Figure I.1, which is shared by IMT-2020 private and public networks.

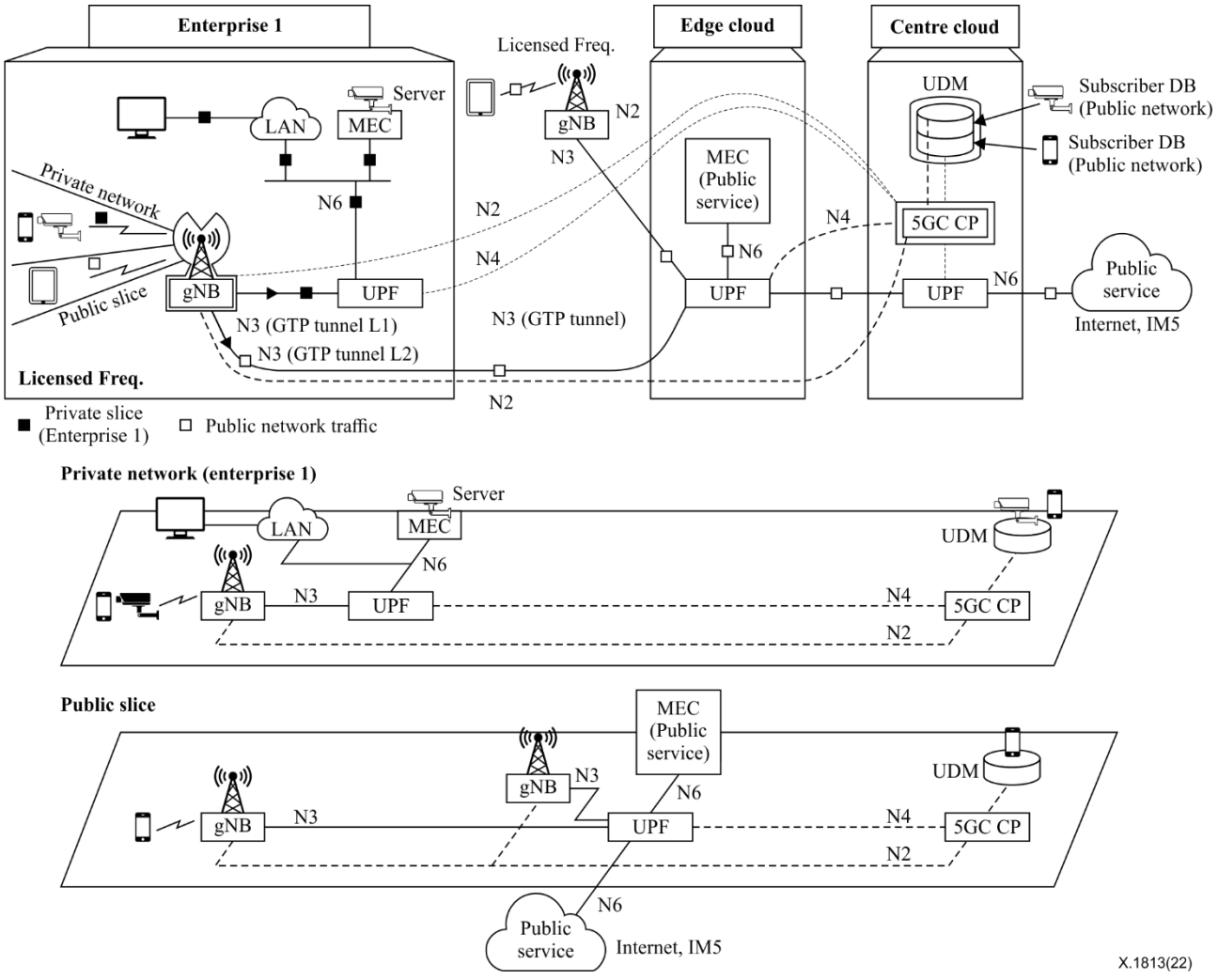


**Figure I.2 – Detailed functional architecture for deployment type (b) in Figure I.1**

According to [b-Harrison], deployment type (c) of Figure I.1 can be depicted as Figure I.3 from the vertical view using network slicing. Figure I.3 illustrates a detailed functional architecture for deployment type (c) in Figure I.1, which is shared by IMT-2020 private and public networks.

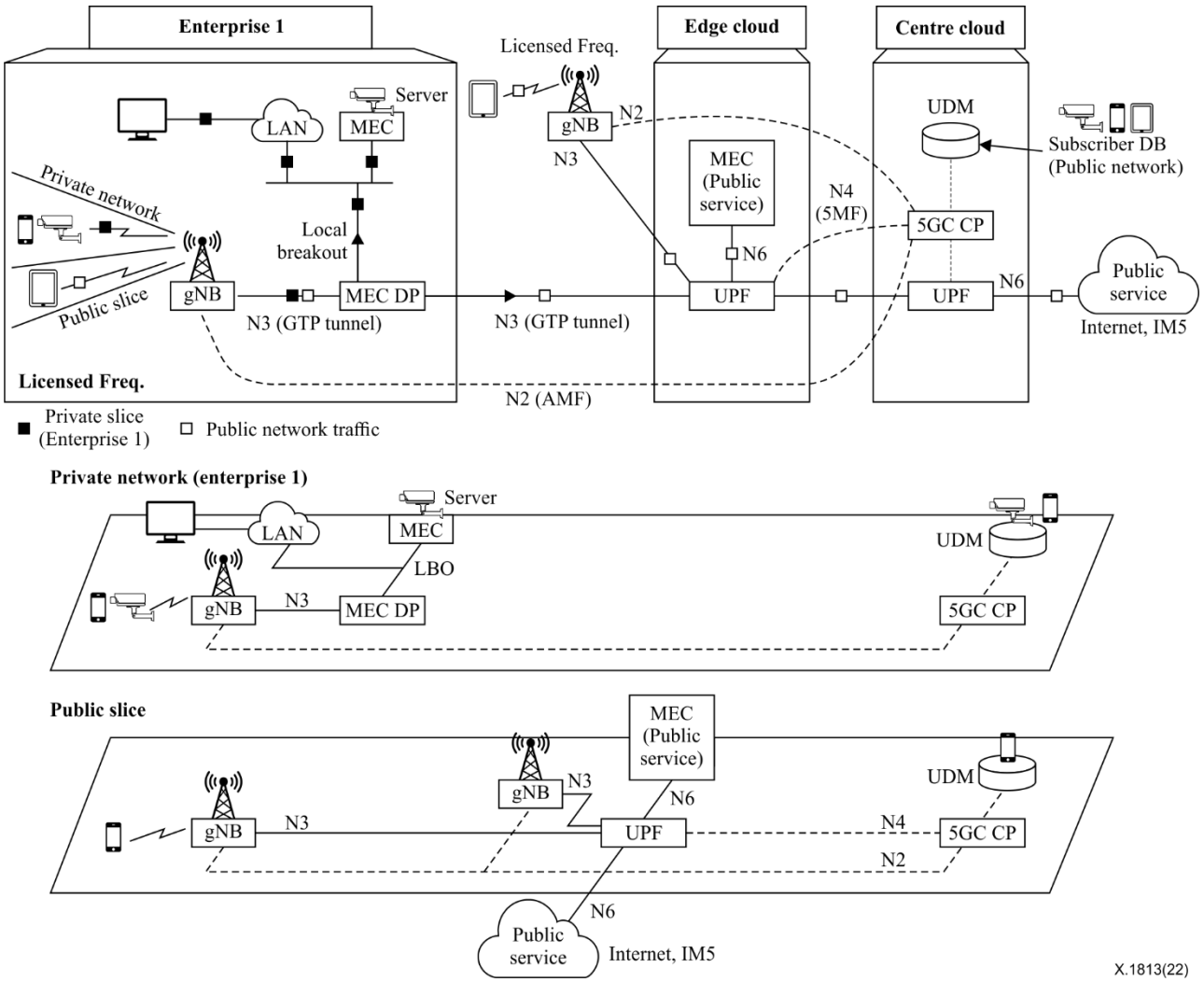


**Figure I.3 – Detailed functional architecture for deployment type (c) in Figure I.1**

All the functional architectures of the IMT-2020 private network mentioned above are deployed by network operators for security and URLLC performance enhancement. Maintaining network performance and security in a IMT-2020 private network is one of the most important factors for vertical services supporting URLLC. One of the candidate methodologies is called deep packet inspection (DPI), which is also described in [b-ITU-T Y.2774] and [b-ITU-T Y.2775]. However, the scope of these Recommendations is only limited to general mobile networks and thus cannot be applied to the IMT-2020 private network, and more specifically, to vertical services supporting URLLC.

# Bibliography


[b-ITU-T Y.2774] Recommendation ITU-T Y.2774 (2019), *Functional requirements of deep packet inspection for future networks*.

[b-ITU-T Y.2775] Recommendation ITU-T Y.2775 (2019), *Functional architecture of deep packet inspection for future networks*.

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

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ISO13491-1] ISO-13491-1:2016, *Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods*. <https://www.iso.org/standard/61137.html>

[b-ISO/IEC 14888-1] ISO/IEC 14888-1:2008, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*. <https://www.iso.org/standard/44226.html>

[b-ISO/IEC/IEEE 24765] ISO/IEC/IEEE 24765:2017, *Systems and software engineering – Vocabulary*. <https://www.iso.org/standard/71952.html>

[b-ISO/IEC 25010] ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*. <https://www.iso.org/standard/35733.html>

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. <https://www.iso.org/standard/66435.html>

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*. <https://www.iso.org/standard/63461.html>

[b-ISO/PAS 19450] ISO/PAS 19450:2015, *Automation systems and integration – Object-Process Methodology*. <https://www.iso.org/standard/62274.html>

[b-3GPP TS 22.261] 3GPP TS 22.261 v17.2.0 (2020), *Service requirements for the 5G system (Stage 1, Release 17).* <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107>

[b-3GPP TS 23.501] 3GPP TS 23.501 v17.0.0 (2021), *System architecture for the 5G System (5GS); Stage 2 (Release 17).* <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>

[b-3GPP TR 23.734] 3GPP TR 23.734 v16.2.0 (2019), *Study on enhancement of 5G System (5GS) for vertical and Local Area Network (LAN) services*. <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3487>

[b-5G-PPP] 5G PPP Architecture Working Group (2019), *View on 5G Architecture, Version 3.0*. <https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf>

[b-Harrison] Harrison J. Son, (2020), *Private 5G network strategies of Mobile operators and None-mobile operators*. <https://www.netmanias.com/en/?m=view&id=reports&no=14585>

## 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, 2022