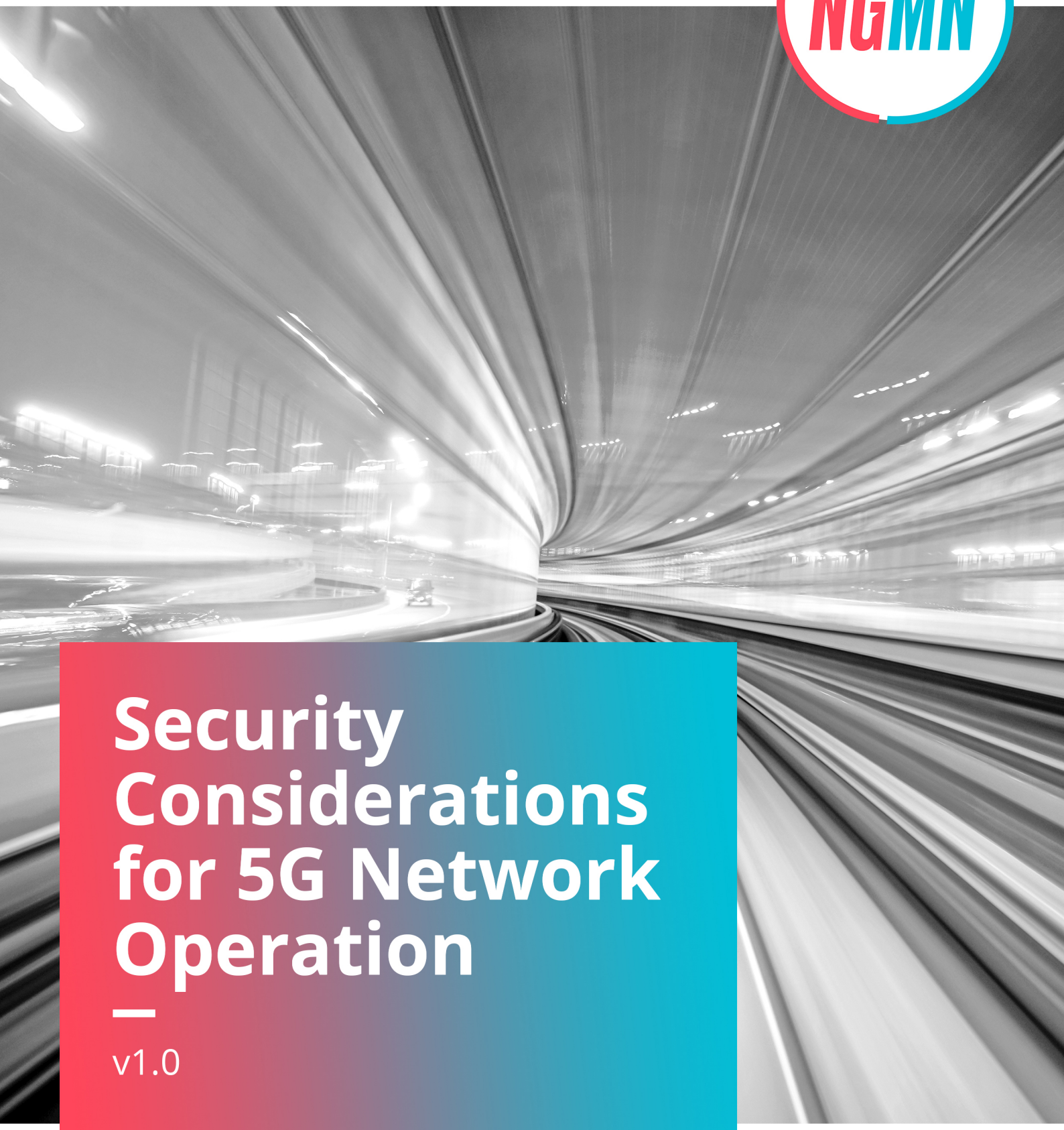

Security Considerations for 5G Network Operation

v1.0

www.ngmn.org

WE MAKE BETTER CONNECTIONS

SECURITY CONSIDERATIONS FOR 5G NETWORK OPERATION

by NGMN Alliance

Version:	1.0
Date:	04-August-2021
Document Type:	Final Deliverable (approved)
Confidentiality Class:	P - Public

Project:	Security Competence Team
Editor / Submitter:	**Minpeng Qi (China Mobile)**
Contributors:	**Minpeng Qi (China Mobile), Stan Wong (Hong Kong Telecom), Sheeba Mary (Lenovo), Colin Blanchard (BT), James Calme (UScellular), Mona Ghassemian (InterDigital), Hua Song (China Mobile), Douglas W. Varney (UScellular), Ru Yan (China Mobile)**
Approved by / Date:	**NGMN Board, 16th July 2021**

© 2021 Next Generation Mobile Networks e.V. All rights reserved. No part of this document may be reproduced or transmitted in any form or by any means without prior written permission from NGMN e.V.

The information contained in this document represents the current view held by NGMN e.V. on the issues discussed as of the date of publication. This document is provided "as is" with no warranties whatsoever including any warranty of merchantability, non-infringement, or fitness for any particular purpose. All liability (including liability for infringement of any property rights) relating to the use of information in this document is disclaimed. No license, express or implied, to any intellectual property rights are granted herein. This document is distributed for informational purposes only and is subject to change without notice. Readers should not design products based on this document.

NGMN e. V.
Großer Hasenpfad 30 • 60598 Frankfurt • Germany
Phone +49 69/9 07 49 98-0 • Fax +49 69/9 07 49 98-41

Abstract

A 5G network relies on many new features like SDN/NFV while also introducing other new features such as slicing and MEC. New technologies and features create new challenges for operators in the 5G era to provide security protection for network operation. Moreover, the 5G network supports vertical industries where additional security requirements need to be considered by the 5G network to support vertical business services.

Although network operation depends heavily on individual operator's specific deployment and operations systems, it is still a good practice to build a common security ground for the success of 5G network deployment and operation.

The scope of this document is to:

- Analyse new challenges as well as common security issues for 5G network operation
- Investigate security requirements and guidelines in a technical and/or non-technical way for 5G network operation

Contents

1 INTRODUCTION

The deep integration of vertical industries and mobile networks in the 5G era has introduced varied scenarios, e.g., simultaneous access of massive Internet of Things devices with resource constraints, unattended Internet of Things terminals, vehicle-to-everything and/or automatic driving, cloud-based robots, and so on. As each vertical has its specific security strategy, different vertical use cases lead to diverse security policies to the network.

On the other hand, the combination of IT technology and communication technologies has brought change to the network architecture, which enables the network to flexibly support a variety of application scenarios. Those changes raise different security requirements and distinct security configurations for the network, especially for network deployment and operations.

To face above-mentioned challenges, current standard security architectures and procedures for network framework and interfaces exist but lack guidelines and recommendations on how to securely implement those standards into real mobile networks for the deployment phase and operation phase.

In order to mitigate security concerns on 5G network operation, this document studies new security challenges as well as common security issues and gives security recommendations for 5G network operation. It is recognised that different mobile network operators may face different challenges related to its specific regulation, infrastructure and deployment environment etc., and would accordingly adopt different network security policies to serve their specific needs. So, the requirements as analysed in this document are considered as best practices rather than standards.

2 SECURITY CHALLENGES FOR 5G NETWORK OPERATION

2.1 5G Network Security Challenges

2.1.1 SDN/NFV

The development of Network Function Virtualization (NFV), Software Defined Network (SDN) and other IT technologies are essential enablers for 5G network deployments but inevitably open up 5G networks to similar attacks and threats as faced by today's IT networks. For

example, an attack on an SDN controller may paralyze or hijack the whole network; and cloud computing infrastructure using virtualization technology may also be threatened by security risks such as virtual machine escape, data residue, resource storm, etc.

2.1.2 Network Slicing

Security challenges with network slicing include:

1) Privacy risk of terminal access to network

The slice selection assistance information is exposed during over-the-air transmission. For example, information like specific S-NSSAI, DNN, etc. could be exposed as the result of accessing incorrect slice or unauthorized terminal access to certain slicing services.

Such risk may lead to specific terminal devices vulnerable to be tracked or user subscription information being exposed during the access of certain slicing services (such as public safety slice, URLLC)

2) Risk of slices on the core network side

Virtualization, containerization and SDN are fundamental technologies to enable network slice on-demand services and for mobile network operators (MNO) to deploy Network Slice as a Service (NSaaS). Tenants expect NSaaS and their network slices to behave as standalone and fully independent mobile networks. In other words, tenants should be prohibited from unauthorized access to other network slices and unauthorized interception of other tenant's data. Unfortunately, network slicing is based on cloud-based and software-based approaches where faults and mistakes can propagate to other network slices via the virtualized abstraction layer. Therefore, MNO deployments of NSaaS require adequate and comprehensive defence mechanisms to protect all the various types of deployed network slices. Those defence mechanisms need to consider traditional physical network environments as well as the virtualized environments built on top of them. This nested network environment creates an extra layer of defence complexity and a wider attack surface for the entire 5G system.

The attack surface also extends to tenants and their subscribers. MNOs might offer various types of network slices coexisting on the same physical network infrastructure. Therefore, they are required to apply adequate isolation and insulation strategies in each of the network slices. Network slice isolation mechanisms can be divided into several categories: resources isolation, network segmentation isolation, service isolation, tenant isolation and tenant data isolation. What is more, quarantine takes place when a network slice has a fault or security alert.

Slice risks for the core network can be summarised as:

- Risk of shared network functions (NFs) across slices: To support a single terminal accessing multiple slices at the same time, some NFs (such as AMF) may be shared by slices. When data on the control plane of each slice uses the same security context, there may be a risk that confidentiality is not sufficient for slices that require higher security levels. In addition, malicious UEs may initiate DoS/DDoS attacks on shared NFs and so disrupt the normal operation of all slices through exhausting their shared resource, impacting slice availability.
- Risk of resource isolation: Slices run on a unified physical infrastructure but are virtually separated into isolated logical functions. With the presence of certain virtualization vulnerabilities, such as virtual machine escape etc., there exist risks of attacks, unauthorized use of shared resources and unauthorized connections between VNFs in different slices. In addition, the failure of one slice or its resources may adversely affect the operation of other slices because of the sharing of physical infrastructure between slices.
- Risk of illegal inter-operation between NFs: NFs used for general service may attempt unauthorized interaction with NFs in a specific slice that should be prohibited from being accessed.

3) Risk of slicing management

The network management system for slicing is used to manage the life cycle of network slicing instances and the relationships between the instances. There are security risks present in each stage of the life cycle of a slice. For example, an attacker can implant malware into a slicing template and threaten all network slicing instances generated using that template. An attacker can also attack slices through the configuration interface during the configuration or operation stage. Even when slices are in the revoke stage, an attacker may obtain confidential data if the data is not properly protected.

2.1.3 Multi-access Edge Computing

With current network domain security protection, core network entities are usually gathered in a secured centric environment such as a data centre (DC) that provide services to customers across a vast area. An attacker is usually not physically at the data centre and can only attack the network remotely. However, with introduction of edge computing, some core network entities are deployed at the edge which may be in unattended or less physically secure environment. Essentially, edge computing shortens the distance between attacker and operator's physical facilities. Therefore, attackers are more likely to obtain access to the physical

facilities and cause serious consequences such as equipment damage, service interruption, user privacy and data leakage.

According to the definition of ETSI, the MEC technology is mainly to deploy general servers near the radio access network, making IT and cloud computing capabilities available closer to the edge of mobile network and thus reducing service latencies. MEC enables the radio access network to have localized service and close-range deployments using high-bandwidth and low-latency transmission capabilities. On the other hand, the services at the edge shrink to form a localized deployment, effectively reducing the network backhaul bandwidth requirements and network load.

Operators usually deploy MEC instances according to the MEC deployment architecture in the NFV environment released by ETSI GR MEC 017. In this architecture, the MEC platform and MEC APP are both deployed in an NFV environment by a VNF method. The security of MEC must not only consider the security of NFV, but also the security of both the MEC platform and the MEC APP. Additionally, under the CP-UP separation principle of the 5G architecture, the UPF can shrink and be deployed close to the UE, providing local breakout traffic to the local network, i.e., appropriate MEC APP. Since the UPF is a network function of the core network, the security of the UPF must also be considered.

2.2 5G Services Security Challenges

ITU defines 5G as having three high-level use cases: eMBB, URLLC, mIoT:

- eMBB focuses on services for the needs of people's demand on digital life with high bandwidth demands, such as high-definition video, VR/AR.
- URLLC focuses on services for the needs of the digital industry that are extremely sensitive to time delay and/or jitter, such as automatic/assisted driving, remote control.
- mIoT focuses on services for the needs of the digital society with high connection density requirements, such as intelligent transportation, smart grid, and intelligent manufacturing.

2.2.1 eMBB

With the rapid development of mobile broadband Internet and the popularization of intelligent terminals, mobile video service has reached 50% of the service proportion of operators and will keep growing rapidly. At the same time, mobile immersive service based on virtual reality and/or augmented reality is gradually becoming the future trend for the development of enhanced mobile broadband services. It is predicted that demand for mobile data will keep

growing tremendously by application from 4K/8K high-definition video to mobile immersive experience services, which will be among the early killer 5G applications and greatly promote rapid 5G development.

5G eMBB brings the following security challenges:

1) Different requirements on data leakage / theft threat for various services such as VR/AR, HD video

Different services face different security risks leading to different security requirements, even though they are transported on the same network. This is especially true for eMBB. For example, for individual subscribers, VR/AR may become the major social platform applications, but only the parts of immersive interactive information which are sensitive in VR/AR need to be protected.

However, for vertical industry customers, the industrial and professional virtual reality application may require encryption for the transmission of all data collected by a VR device.

Additionally, security requirements may also be different for personal applications and public security monitoring services.

2) Risk of dissemination of malicious information

With the development of eMBB services, more categories of malicious information can be transferred through the 5G network. This includes not only plain text and audio/videos but also encrypted data. It becomes increasingly important to monitor the status of service flows in order to analyse and categorize them to identify the malicious ones.

3) Risk of privacy leakage in wider area

Many kinds of eMBB services like VR/AR contain a large amount of subscribers' sensitive information, such as personal service information or identification, device identification, address information, etc. Those kinds of information can be recognized as requiring subscriber's privacy protection. Meanwhile the 5G network architecture increases the possibility of private information disclosure based on its openness and sharing features, such as different service slices sharing the same infrastructure network.

On the other hand, due to the development of data mining technology, tools of analysing and extracting privacy information become more powerful and make it easier to associate device identification with subscriber identification such as subscriber's application or service identification, and thus to analyse subscriber's preference. Therefore, the risk for subscriber privacy disclosure in the eMBB services cannot be ignored and the privacy information must

be strictly protected when a subscriber accesses eMBB services -- the greater the volume of privacy data is available to an attacker the easier for them to perform mining and profile the target.

2.2.2 URLLC

The 5G URLLC is designed for applications that are extremely sensitive to time delay such as automatic driving / assisted driving, virtual reality, industry 4.0 and other services. Low latency is one of the most critical preconditions for above mentioned applications. Typical 5G end-to-end delay falls into the range of 1-10ms but can reach 1ms ideally, which means 5G can reduce the end-to-end delay by 90% or more compared to 4G. Ultra-reliability is another critical precondition for industrial control applications which usually require greater than the 99.999% reliability that is achieved by legacy 4G networks. If networks cannot reach these service requirements, it may lead to a bad user experience, control failure, or even an accident. For example, compromised V2X services signalling can result in an accident, or even lead to be life threatening.

URLLC has the following major security risks:

1) (D)DoS Attack

DoS/DDoS attacks can cause network congestion and data delay that impact guaranteed service quality, or even cause wireless interference leading to the interruption of the communication and service failure.

2) Data integrity risk

The service data can suffer tampering, manipulation and replay attacks due to weaknesses or vulnerabilities in the protocol and/or devices when transmitting in mobile networks or over the air, which reduce reliability of data transmission and cause service degradation. What is more, the security protection of the interface between mobile network and service provider should also be considered because of end-to-end requirement of URLLC.

2.2.3 mIoT

5G networks must be able to provide reliable network communication services for the Internet of Things (IoT). For IoT services, requirements on connection management are raised due to the huge number of IoT device sensors. For example, in V2X system, the communication of vehicle-to-network, vehicle-to-infrastructure and vehicle-to-person may involve millions of connected devices, sensors and/or users such that reliable communication is critical to ensure

traffic safety, improve urban traffic efficiency and reduce pollution emissions. For smart utilities, the number of installed smart meters can be over 10 million in a large metropolitan area. Massive amounts of data are generated and uploaded to data centres every day from this enormous number of meters. For healthcare, 5G technology can enhance the connection required for IoT devices by providing energy efficient, secure long-distance communication and control. Another example is smart manufacturing, which requires a large number of connections that can cover vast geological areas and are always online and available anywhere for non-stop machines, numerous products and mobile workers. From the above examples, it is clear that the connections among industrial factories, machines, management systems, products and workers must be guaranteed.

Due to the nature of IoT devices being low-cost, massively deployed and having limited resources such as processing, storage, energy, the following security risks exist for IoT devices:

1) Fake terminal

Resources for Internet of Thing terminals are limited. Its power is restrained so, it is likely not to have strong security capabilities like strong authentication (e.g., methods with complex processing and computations) or complex protection. It is likely to adopt a simpler mechanism for access authentication like fixed password. This raises risks to counterfeit terminals which can obtain access to the Internet of Things service platform through the vulnerability of the authentication mechanism or any other mechanisms that lead to service errors.

2) Data tampering

The amount of IoT data is usually small but important as it is generated by sensors that collect data of the real world. The attacker can tamper such data through weaknesses or vulnerabilities in the data transmission path, e.g., over the air, backhaul, network, and Internet. Therefore, it is necessary to prevent attackers from tampering with the interactive data between IoT terminal and the server to ensure data integrity.

3) Data eavesdropping

The data collected by IoT terminals deployed in special environments (such as home environment, medical environment) is sensitive and involves user privacy. Attackers can eavesdrop on service data by exploiting weaknesses in data transmission paths (air interface, backhaul links, and Internet), causing disclosure private user information. So, it is necessary to prevent attackers from eavesdropping on the data exchanged between terminals and the network, to ensure the privacy of user data.

4) Remote control

Attackers can remotely access and control IoT terminals through software and/or hardware interfaces by exploiting the capabilities of IoT terminals with limited resources and weak security. Once being compromised an IoT terminal can be controlled by an attacker to externally initiate an attack and interfere with the normal operation of IoT services.

3 SECURITY CONSIDERATIONS FOR 5G NETWORK OPERATION

3.1 General Security Considerations for 5G Network Operation

3.1.1 Security Considerations in Different 5G Phases

In order to provide security for 5G network operation, the considerations should not only focus on security in the operation phase but also involve considerations for the planning phase and the deployment phase.

In the network planning phase, a network security blueprint should be defined, and 5G network security risks analysed comprehensively, including legacy security risks from network architecture, risks from operator partners, etc, and security strategies should be defined for a 5G network with long-tailed vertical use cases.

In the network deployment phase, security protection measures like firewalls, IDS/IPS should be integrated. Security assurance on devices and evaluation on whole network and services should be performed before on-boarding. Regulatory compliance should be fulfilled at this stage.

In the network operation phase, periodic security tests should be performed in order to find possible vulnerabilities on network devices and weakness in the network itself. What is more, an end-to-end security evaluation for specific services/verticals is also recommended, involving terminal security, network security, service security, data security, O&M security and any other related security aspects.

3.1.2 General Security Considerations on 5G Network

SDN security shall provide security protection for the application layer, control layer, data layer and Northbound/Southbound interfaces.

- **Application layer:** the controller and other applications shall be authenticated based on certificates, and the application software shall be secured with hardening.
- **Control layer:** the application and forwarding device shall be authenticated based on certificates and be capable of anti-(D)DoS attack through speed limits and other mechanisms. Flow priority should be set to prevent policy conflict. Encryption shall be provided to protect sensitive data. Controller and server software shall be secured with hardening.
- **Data layer:** controller shall be authenticated based on the certificate. An appropriate expiration time for flow table shall be established and anti-(D)DoS attack through the mechanism such as speed limit shall be provided.
- **Northbound/Southbound interfaces:** confidentiality, integrity and anti-replay protection for the transmitted data shall be provided by using solutions such as encryption, HMAC and time stamps.

NFV security shall also provide security protection for NFVI, service communication system and management system, as following:

- **NFVI security:** the physical hardware of the servers can use the trusted computing technology to ensure credibility. The virtualization software, host computer and virtual machine OS should be strengthened. Virtual machines should be isolated in a secure way.
- **Security of service communication system:** secure and standardized communication protocols shall be applied. Data communication shall be protected with encryption, integrity, and anti-replay mechanisms.
- **MANO security:** the MANO entities shall be secured with hardening. The communication between the MANO entities and the external entities, as well as the communication between different MANO entities shall be mutually authenticated and protected with confidentiality and integrity protection.
- **Network security:** Independent networking hardware should be used for physical isolation of management, control, and user data traffic. Security domains shall be made to separate different network entities in different secure environments, and secure tunnels like IPsec or other VLAN shall be used for isolation between security domains.
- **Security management:** the network element of the management system shall be reinforced. Encryption, integrity and anti-replay shall be provided for the data on the internal interface of the management system and the interface between the

management system and other external systems. Security management of accounts, passwords, and logfiles shall be specified.

Network Slicing Security:

- **Privacy protection of slice selection information:** after the security context is established, confidentiality protection shall be applied for slice selection information.
- **Slice security for UE access:** Slice authentication (select correct slice for UE through NSSAI of the UE) shall be applied to ensure valid UE access to the network slice.
- **Slice Security between access network and core network:** Based on operator's policy, signalling and data transfer for different slices shall be isolated through backhaul network, using physical ways such as dedicated fibre or FlexE solution or using logical means like IPsec/TLS tunnel.

Security between NFs in slice:

- **Security of public NF:** Authentication mechanisms shall be provided to establish mutual trust between the NF in the slice and the public NF out of the slice. Firewall or constant monitoring shall be applied on public NFs like AMF or NRF, to prevent resource exhausting attacks from compromising the NF. Different security policies shall be set for communication between UEs and NFs in different slices, and separated shared NFs shall be provided for slices with different security levels.
- **Security between the NF in a slice and external network devices:** a virtual or physical firewall shall be deployed between the NFs in a slice and external network devices to separate internal and external network flows.
- **NF isolation between different slices:** NF isolation between slices shall be ensured through network division, resource isolation, SBA access control or other similar technologies. Insulation between slices can be provided based on Vertical's requirement.
- **Slice Management Security:** the slice management interface shall provide an authentication and authorization mechanism. The slice template and corresponding software image shall be integrity protected and checked when uploading and storing. Communication between slice and management systems shall be integrity and confidentiality protected. Slice related resources shall be released and cleaned after slice termination. The operator can define a set of security levels and design a group of security measures/profiles for network slice access, slice isolation and slice management to provide slice security based on different requirements.

MEC Security:

- **Security of MEC platform:** MEC platform software shall be secured with hardening. The MEC platform software and image shall be integrity protected with HMAC. Sensitive

data shall be encrypted. The application shall be authenticated and authorized in bootstrapping.

- **Security of MEC orchestration management system:** refer to the MANO security in NFV security mentioned above.
- **UPF security:** For a UPF which is deployed in a MEC environment, trusted computing technology should be provided to ensure integrity of the UPF. Sensitive data such as diverting strategy on UPF needs to be stored with encryption. An access control mechanism like RBAC shall be used. Data transferring from UEs should be restricted.
- **Security of NFV system:** refer to NFV security mentioned above.
- **Security risk monitoring system** on MEC platform is recommended to detect a security attacker, to alarm security risks and vulnerabilities, and to deal with security events, etc. For example, a local IDS/IPS agent can be deployed on the MEC platform, if applicable.

As MEC nodes are usually deployed near the service provider and out of operator control, an isolation mechanism shall be provided to prevent attacks from edge computing nodes to the core network.

3.2 Security Considerations for 5G Network Operation Based on Specific Vertical Scenarios

3.2.1 Security Considerations for Smart Industry

The Industrial Internet, as coined by General Electric (GE) [1], is the integration and linking of big data, analytical tools and wireless networks with physical and industrial equipment, or otherwise applying meta-level networking functions to distributed systems. The Industrial Internet is the result of the integration of global industrial systems with advanced computing, analysis, sensing technology and Internet connection. Through the connection between machines to reach the connection between people and machines eventually, Industrial Internet reconstructs industrial production process, that not only can improve production efficiency, but also meet the needs of various consumers accurately.

Different Industrial Internet application cases using 5G technology can be summarized into three categories:

1. To ensure precise remote control through using 5G low latency time characteristics, slicing, edge computing and other new technologies. Examples include remote control of construction machinery, robot control, on-site production line equipment control.

2. To collect terminal video data and transfer them to the application cloud for deep analysis through using 5G high bandwidth characteristics and new edge computing technology. Examples include defect detection, OCR decoding, AR assistance, VR complex assembly, production security behaviour analysis.
3. To collect the factory sensor data and transmit to the application cloud for deep analysis through using 5G massive connection, high bandwidth characteristics, and edge computing technology. Examples include 5G+ large-scale data collection.

To protect industrial control data from being revealed to others, in some cases edge computing is needed. Edge computing nodes can ensure that factory data remains private and secure as they can be deployed closely to end-users or devices. This placement can also reduce network operation delay, speed up service delivery, improve operation accuracy and user experience.

Based on the above analysis, it is advisable that Industrial Internet can be established through using virtualization, edge computing, slicing and any other 5G network technologies in a compound system containing eMBB, URLLC and mIoT categories with required security protection. Recommendations for providing security protection for such technologies and service categories are as follows.

For eMBB:

- It shall be able to counter Distributed Denial of Service attack, e.g., by deploying anti DDoS devices. It can prevent communication interruption caused by DOS/DDoS attacks to guarantee applications running continuously. It is recommended that anti-DDoS be enabled from RAN side, to mitigate attacks from compromised terminals.
- Secondary authentication can be used to prevent compromised terminal access to the service platform.
- In the case that the service requires high security protection, it is recommended to protect user data transmission over the air and between network elements in 5G networks by not only crypto mechanisms but also by physical isolation.
- In some cases, it should have dedicated connections between 5G core network and application servers with protection. It can establish secure tunnels for user data transmission outside of the 5G network.

For URLLC:

- It shall be able to counter Distributed Denial of Service attack, as described in the eMBB requirement.
- It shall provide data integrity protection and anti-replay parameters like time stamp, serial number, etc., to prevent service data from being tampered/forged/replayed and ensure data transmission reliability.

- A mutual authentication mechanism should be applied between terminals and the application, e.g., using certificate based or shared key based authentication, or relying on secure connections between UEs and the network, like GBA or AKMA which are defined/studied in 3GPP.
- In some cases, dedicated network deployment and security solutions should be used to comply with industrial requirements.

For mIoT:

- An IoT security assessment shall be performed on an IoT device before deployment. Security status shall be monitored during operation with attack being mitigated.
- Security devices should be deployed to immediately detect and prevent mIoT devices from being controlled and making further attacks from compromised devices, such as DDoS attacks on wireless connections or to business platforms. The potential results of these attacks are network congestion, leading to the failure of the normal operation of mIoT services.
- Network capacity needs to be protected. A distributed identity management and authentication solution can be applied to reduce the complexity and delay on authentication and other security mechanisms in order to provide fast and safe access, to reduce security cost, and to mitigate bottleneck risks caused by signalling storms and single points of failure during peak connection time.
- Confidentiality and integrity protection shall be provided when sensitive service data is generated and transferred by IoT devices to prevent attackers from eavesdropping, tampering and forgery of data, and the replaying of data transmissions. In the application layer, the session key can be generated based on the security credentials used between the UE and network to protect service data confidentiality and integrity with lower cost.

3.2.2 Security Considerations for Smart Utilities

Smart utilities provide infrastructure services for society. With the development of large-scale automatic distribution networks, centralized automatic low voltage meter reading functions, distributed energy access, mutual user interaction, intelligent patrol inspection, and mobile operation terminal applications etc., the demand for communication between utility customers and utility devices like network equipment and terminals have been growing rapidly. This brings new communication requirements in utility generation, transmission, transformation, distribution and use services beyond traditional fixed network communication.

5G networks can provide specific services for power utility customers as a private network, which can meet varied requirements from different kinds of utility services. In detail, 5G

networks can provide enhanced data security protection, a unified authentication mechanism for different access technologies, strong user privacy protection, and flexible inter-connection protection between networks, in order to strengthen the utility customer's security capabilities and efficiency aspects.

The typical scenarios of smart utility can be roughly divided into command case and collecting case.

1. For command case, there are strict requirements on delay and reliability aspects, compared with bandwidth and connection number requirements.
2. For collecting case, like remote monitoring, meter reading and so on, there are specific requirements for bandwidth or connection numbers, but there are typically no special requirements for delay and reliability.

To provide security protection for smart utility, a dedicated network needs to be provided for this service. Slicing can be used to provide such a feature.

In smart utility scenarios, some general security protection measures need to be provided or guaranteed. Security for URLLC, mIoT, and slicing also need to be taken into consideration. The detailed security requirements are as follows:

- The 5G network shall provide authentication and authorization for smart utility system to local and/or remote access, in order to prevent malicious terminals or users from accessing the utility system. Confidentiality and integrity protection shall be provided for communication.
- Secure VLAN tunnel, access control mechanism and other security measures shall be applied between utility systems through the 5G system to limit the direct connection between such systems.
- It shall involve an audit system to generate auditable events, which can be used by management system, warning system, IDS/IPS, and any other sensitive access subsystems.
- An anti-malicious code prevention system shall be deployed. A database with virus signatures, Trojan signatures and IDS rules should be tested and updated offline.
- Protection shall be strengthened on the border between utility systems and the terminal/Internet to prevent intrusion attacks against businesses (such as worm virus, malicious program, Trojan horse, vulnerability attacks, web class injection, password blasting, DDoS attacks).
- Set routine security scanning and monitoring tasks based on explicit requirements from utility systems. Security scanning and monitoring can be applied to the service system to provide warning and mitigation advice if problems are found.

- Provide systems to detect and prevent spoofing and spam messaging if public services are provided from a utility system.
- Establish a co-operative working framework between the operator and the utility enterprise in order to directly report security threats and work together to mitigate security risks.
- Help utility enterprises to regularly backup and archive data remotely.
- The radio spectrum used to provide services will need to be carefully considered based on the device placement. For example, ensure that devices that have to be located in basements or buildings shielded by thick walls are provided good coverage, while meeting battery life requirements. Any security features enabled must not have a disproportionate impact on that battery life.
- The 5G equivalent of the PC5 ProSE side link or local interfaces [2] may be used to create a mesh network. This is where one device in radio coverage acts as a relay node to other devices not in coverage. This could provide an alternative to the ZigBee interface to ensure communication with In Home Displays (IHD) placed a long distance from the meter, e.g., meters at the end of long gardens or top floor flats with meters in the basement. To secure these interfaces, recent work in 3GPP SA3 [3] may need to be considered.
- End user privacy, especially for houses with multiple occupants, is an important consideration. There could be cases where tenants or the landlords pay energy bills. Tenants may have their own pre-payment meters or just their own IHD.
- Smart utility use cases place stringent requirements on current consumption/battery life when the meter is for electricity, for gas, for water, etc.
- The application layer shall comply with local regulations. For example, applications used in the UK must account for smart requirements listed in [4].
- While traditional security aspects of transport security and message security within the mobile network are important, they must recognise that a change of utility by the residential customer may also require a change in operator. The utility itself may switch operators, requiring a change to many meters dispersed over a large geographical area in a limited timeframe. Therefore, a remote means to change subscriptions will be needed, such as eSIM [5].
- Mechanisms may be required that cryptographically bind the subscription to the device and/or application so that a device will only work with a defined list of subscriptions, or the subscription will only work with a defined list of devices.

For URLLC:

- It shall be able to counter Distributed Denial of Service attacks to prevent communication interruption.

- It shall evaluate security measures before applying such measures for URLLC oriented services. The security mechanism should have minimal impact on latency.

For mIoT:

- The 5G network can support a unified lightweight authentication through different access networks that is fit for various authentication protocols and different terminal types.
- Smart utility use cases define stringent response time requirements for protection and control and monitoring. For example, for protection of nodes in a smart grid, automatic circuit reclosers must operate within 10ms. At the other extreme, for privacy reasons, smart meter reading sampling intervals are restricted to no less than 15-minutes if they are shared outside the end users' premises.
- Terminal security assurance tests shall be performed before provisioning. An abnormal behaviour detection solution shall be provided to find compromised terminals and cancel network service before harm can be done.
- It shall have DDoS protection on RAN side to prevent attacks to utility systems from a large number of compromised terminals.

For slicing:

- Slice authentication (selecting the correct slice for a UE through NSSAI of the UE) shall be applied to ensure only legal UEs are granted access to the smart utility slice.
- NF isolation between slices shall be ensured through network division, resource isolation, SBA access control or any other means. Insulation between slices can be provided based on utility requirements, e.g., for a slice serving a command case.
- The confidentiality and integrity protection security policy for signalling and data transferring should be set in each specific slice.
- Security capability exposure can be provided based on the slice, followed by the requirements from utility systems.

3.2.3 Security Considerations for Smart Health

There have been significant advancements within the IoT field beneficial to healthcare applications mainly for monitoring vital signals of patients to improve medical records used for prescriptions and interventions. Therefore, through IoT monitoring devices patients can live with greater regularity without the inconvenience and restrictive task of explicitly monitoring their health conditions. The use of IoT further lightens the workload of medical professionals by providing them with immediate and accurate data from which decisions can be made without patient interaction.

As for all connected devices, especially within the healthcare field, security and privacy are of paramount importance to ensure the data is not obtained by third parties and remains confidential between a patient and their medical professional being compliant to the healthcare alliances, namely HIPAA. To protect healthcare data, 5G edge capability allows processing and storing the data closer to the end-user devices which advances both privacy as well as battery efficiency of the nodes. Furthermore, centralised authentication solution by using SUCI/SUPI in 5G provides data integrity protection and advances the operation accuracy which can be life threatening should the reported data from a patient be accessed and altered by a malicious node. To this end, a continuous low power communication platform is a solution to provide a greater level of convenience, usability, and security.

The healthcare application requirements are similar to the requirements for the industrial application highlighted in subsection 3.2.1 with further requirements of personal data privacy, reliable communication for remote operation, and the battery efficiency to address the user experience.

The typical scenarios of smart health can be roughly divided into command case and collecting case.

- Further confidentiality and privacy requirements for sensitive healthcare data privacy can be addressed by 5G non-public (aka private) networks, as reported in 5G Health Enterprise Network [6].
- Besides the access level, security solutions are required to ensure a secure and reliable communication to all authenticated users. While delay sensitive applications can be supported by URLLC capability in 5G networks and beyond, further security and reliability requirements derive applications to be run on non-public networks or to keep sensitive data in local place.
- For monitoring use cases, long battery lifetime of devices that collects bio signals (e.g., through wearables) is the main challenge.
- Use cases that require control and delay sensitive applications (e.g., haptic remote control for tele surgery) can be supported by URLLC capability in 5G networks and beyond.
- Battery energy efficient solutions: Low power requirements for reduced capability devices can be realised in 5G NR standard development such as Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST) [7].
- Device manufacturer and application identifiers for healthcare applications may reveal exactly what health problems individuals have and may need special protection in device level-storage and transmission.

LIST OF ABBREVIATIONS

AMF	Access and Mobility Management Function
AKMA	Authentication Key Management for Application
APP	Application
AR	Augmented Reality
CP	Control Plane
DC	Data Centre
DDoS	Distributed Denial of Service
DNN	Data Network Name
DoS	Denial of Service
eMBB	enhanced Mobile Broadband
GBA	Generic Bootstrapping Architecture
GE	General Electric
HIPAA	Health Insurance Portability and Accountability
HMAC	Hash-based Message Authentication Code
IDS	Intrusion Detection System
IHD	In Home Displays
IPS	Intrusion Prevention System
MANO	Management and Network Orchestration
MEC	Multi-access Edge Computing
mIoT	massive Internet of Things
MNO	Mobile Network Operator
MTC	Machine Type Communication
NF	Network Function
NFV	Network Function Virtualization
NSaaS	Network Slice as a Service
NSSAI	Network Slice Selection Assistance Information
OCR	Optical Character Recognition
O&M	Operations & Maintenance
OS	Operation System
RAN	Radio Access Network
SBA	Service-Based Architecture
SDN	Software Defined Network
S-NSSAI	Single Network Slice Selection Assistance Information
TLS	Transport Layer Security
UE	User Equipment
UP	User Plane
UPF	User Plane Function
URLLC	Ultra Reliable Low Latency Communications
VLAN	Virtual Local Area Network
VNF	Virtual Network Function

VR	Virtual Reality
V2X	Vehicle to everything

REFERENCES

[1] Industrial Internet: Pushing the Boundaries of Minds and Machines, November 2012, https://www.ge.com/digital/sites/default/files/download_assets/Industrial_Internet.pdf

[2] 3GPP TS 23.303 Technical Specification Group Services and System Aspects; Proximity-based services (ProSe); Stage 2(Release 16)

[3] 3GPP TS 33.536 Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services

[4] https://www.smartdcc.co.uk/products-services/design-and-assurance/key-infrastructures/smart-metering-key-infrastructure

[5] https://www.gsma.com/esim

[6] Secure Non-public Health Enterprise Networks, https://arxiv.org/ftp/arxiv/papers/2004/2004.13085.pdf

[7] 3GPP TS 33.163 Battery Efficient Security for very low throughput Machine Type Communication (MTC) devices (BEST)