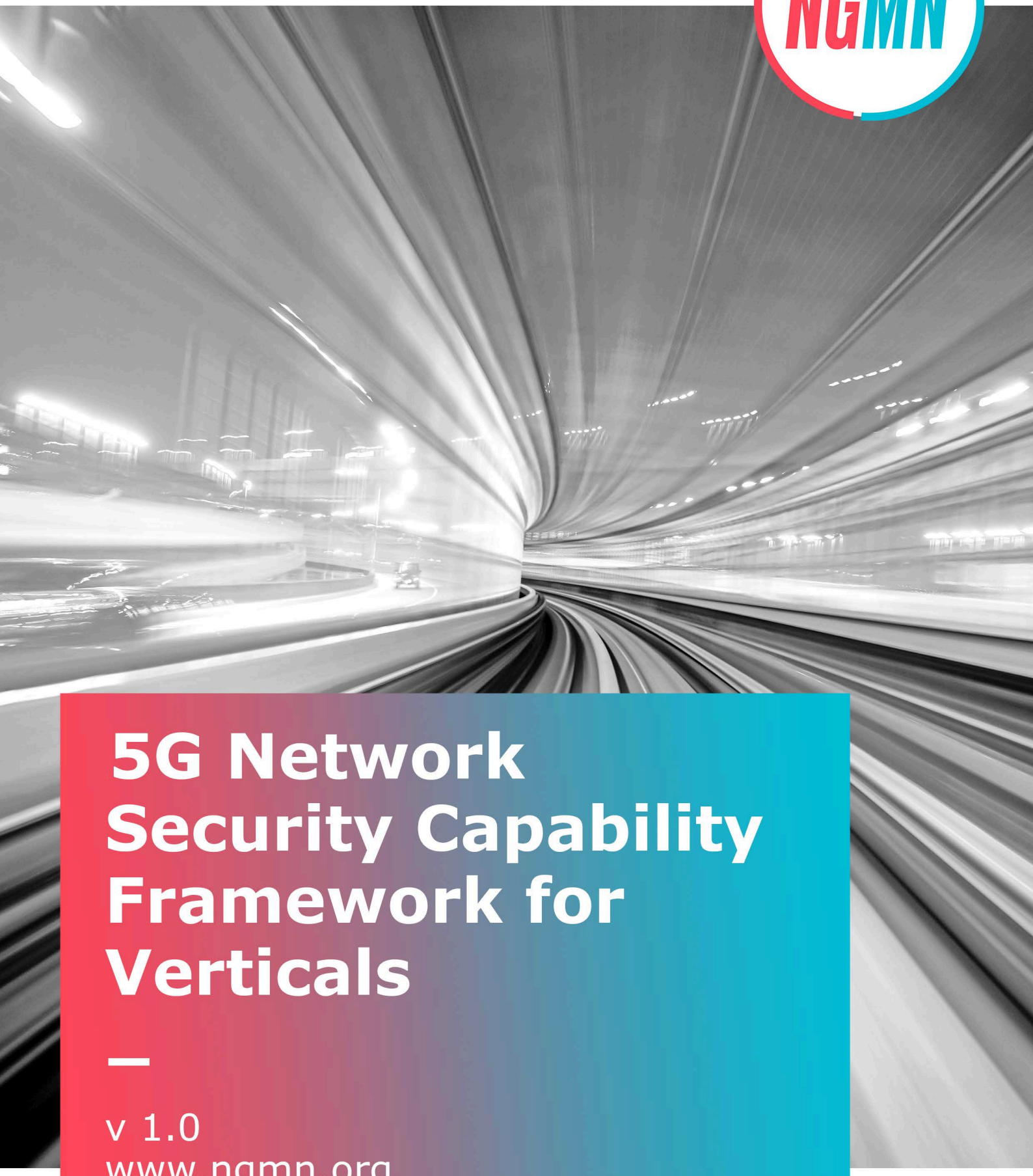

5G Network Security Capability Framework for Verticals

—

v 1.0

www.ngmn.org

WE MAKE BETTER CONNECTIONS

5G NETWORK SECURITY CAPABILITY FRAMEWORK FOR VERTICALS

by NGMN Alliance

Version:	1.0
Date:	23.05.2022
Document Type:	**Final Deliverable (approved)**
Confidentiality Class:	**P - Public**
Authorised Recipients: (for CR documents only)	

Project:	Security Competence Team
Editor / Submitter:	**Hua Song (China Mobile)**
Contributors:	**Xiaoting Huang (China Mobile), Peng Ran (China Mobile), Minpeng Qi (China Mobile), Sheeba Mary (Lenovo), Andreas Kunz (Lenovo), Stan Wong (HKT), Fei Liu (Huawei), Ivy Guo (Apple)**
Approved by / Date:	**NGMN Board, 12th July 2022**

NGMN e. V.
Großer Hasenpfad 30 • 60598 Frankfurt • Germany
Phone +49 69/9 07 49 98-0 • Email office@ngmn.org

Abstract

The launch of 5G catalyses countless new business models and use cases in vertical industries (verticals) and becomes an enabler for the connected industry and a large range of vertical sectors e.g., in automotive, smart city, manufacturing, logistics, energy, as well as finance and healthcare that currently do not fully exploit the potential of mobile services. Mobile network operators (MNOs) leverage their 5G networks and services to provide vertical industries with dedicated solutions, including security services to make vertical applications secure and robust. However, various vertical industries have different requirements related to security. They may request customised network security protection from MNOs.

In this paper, the security requirements for 5G verticals are analysed and a framework of security capabilities is proposed. A recommendation is provided to guide vertical industries on how to build and deploy appropriate security capabilities to improve the security level.

Content

1 INTRODUCTION

5G has enriched people's lives and becomes an enabler for the connected industries and a large range of vertical use cases e.g., in automotive, smart city, manufacturing, logistics, energy, as well as finance and healthcare that currently do not fully exploit the potential of mobile services. However, vertical industries are diverse, and their requirements are dictated by the service characteristics of the related vertical segment. Various vertical industries have different requirements. Some verticals may require ultra-reliable communication, whereas others may require ultra-high-bandwidth communication or extremely low latency. Different vertical industries may also have specific security requirements. So, they may request customised network security protection from MNOs.

It is important for verticals to know what kind of security capabilities or services 5G can offer when they request 5G network services from MNOs. On the other hand, it is also beneficial for the operators to be aware of the list of security capabilities, in order to design customised security solutions for verticals and meet their security requirements. Therefore, MNOs and verticals should form partnerships and develop business models with security in mind, to deliver the full potential of 5G.

This paper analyses the security requirements for a few selected use cases across the vertical industries and provides the references for security services.

The security requirements and the reference framework in this White Paper are considered as a best practice.

2 SECURITY RISK ANALYSIS FOR VARIOUS VERTICAL INDUSTRIES

This chapter provides a non-exhaustive list of security risks and the corresponding security requirements for a few vertical industries, based on MNOs' experience.

2.1 Security Risk for Smart Grid

This section analyses the main service characteristics and application scenarios of smart grid and identifies the major security risks facing 5G smart grid.

2.1.1 Industry Introduction

The smart grid refers to power communication using 5G technologies to achieve intelligent, unattended, and secure power production and control.

There are two types of wireless communication application scenarios: control and collection. Control scenarios include intelligent power distribution automation, demand response (DR), and distributed energy control, while collection scenarios mainly involve advanced metering. The application scenarios of 5G in smart grid are classified into five types.

- **Type 1:** Differential protection for grids by using the low latency and new technologies of 5G such as slicing. Examples include differential protection for power distribution networks of smart grid.
- **Type 2:** Telemetry, remote communication, and remote control for grids with the use of 5G low latency and new technologies such as slicing and edge computing. Examples include automated telemetry, remote communication, and remote control for power distribution networks of smart grid.
- **Type 3:** Secure operations of power grids with the use of 5G large bandwidth and new technologies such as slicing and edge computing. Examples include unattended inspection of smart grid and emergency grid communication.
- **Type 4:** Secure power grid operations with the use of 5G large bandwidth and low latency. Examples include smart grid power monitoring unit (PMU) and precise load control.
- **Type 5:** Secure operation for the services of smart grid with the use of 5G capabilities of large bandwidth and massive connection. Example includes advanced smart grid metering.

2.1.2 Security Risk

Based on the analysis of the above scenarios, the smart grid industry is facing the following key security risks:

- Data leakage/theft risks with high-definition video in scenarios such as intelligent inspections due to the devices being hacked; the risk of dissemination of inappropriate information; and the risk of insufficient protection of existing security equipment.
- Impact of DDoS attack on network reliability and delay in scenarios such as differential protection and precise load control in a distribution network. Other risks include data security and restricted deployment of complex security mechanisms.
- The security risks of new IoT devices: large-scale attacks on air interfaces and service platforms from massive IoT devices in the smart energy industry, and the risks caused by insufficient security supervision.
- Network slicing: some scenarios require extremely low latency which may require customised dedicated slicing, which introduces the security risks of terminal access to slicing, slicing security threats to the core network due to the opening of the interface, and slicing management risks.
- Edge computing: the access risks for the edge nodes deployed in some smart grid, and the management risks including in NFV system, MEC platform, MEC orchestration management system, UPF and MEC App.

2.2 Security Risk for UAS

This section analyses the unmanned aerial system (UAS) communication related security risks when an Unmanned Aerial Vehicle (UAV) (such as drones) and/or UAV-Controller (UAV-C) operates over communication networks such as 5GS or EPS.

2.2.1 Industry Introduction

UAS is gaining importance in defense, commercial and civil spheres and UAVs are increasingly getting integrated into the airspace recently. Applications in commercial and civil spheres can be numerous ranging from exploration of inaccessible terrains, search and rescue operations, agricultural survey of crops and livestock, fire control, package delivery etc. An UAS is a combination of UAV and UAV-C, where a UAS Traffic Management (UTM) (i.e., a set of functions and services enabled by UAS supplier service (USS)) manages all range of UAV operations and supports operations such as UAS identification, tracking, authorisation, enforcement, regulation of UAS operations, and storage of data required for the UAS(s) to operate. The communication requirements for UAS should consider both:

- Command and Control (C2) messages
- Uplink and downlink data security between UAS components and the serving communication network/UAS network servers.

The malicious use of UAS can lead to hostile surveillance, smuggling, disruption and weaponization, where an adversary may use UAS as a mobile platform to interrupt and modify digital services to gain unauthorised access to data systems [2]. A breach in data security or lack of sufficient data security (i.e., confidentiality and integrity) between UAS components and communication network/network servers can expose sensitive private data and tampering/modification of C2 data can lead to hijack of UAVs.

2.2.2 Security Risk

Based on the above scenarios, the UAS industry can face the following key security risks [3] if the communication links are not sufficiently protected:

- Drones can be potentially hacked, if the command-and-control signal between the operator and the drones are hijacked. In such a case hacker can gain full control over the drones and their system.
- A hijacked UAV/UAV-Controller can launch collision attack, which threatens the safety of urban population, property, air traffic etc.
- As UAVs are equipped with high resolution and sophisticated cameras, a compromised UAV/UAS communication link can lead to invasion of privacy or espionage.

2.3 Security Risk for Healthcare

2.3.1 Industry Introduction

Combining the high-speed, low-latency characteristics of 5G, mobile smart healthcare can enable everyone to enjoy timely and convenient medical services, and improve the performance and effectiveness of existing medical methods. Healthcare will benefit from 5G technology from various aspects, such as mobile emergency vehicles, remote assisted diagnosis and treatment, virtual reality teaching, and smart diagnosis and other application scenarios.

1) Ambulances/medical examination vehicles

   As part of the urban emergency rescue system, 5G emergency vehicles equipped with various first-aid equipment such as ventilators and defibrillators, as well as patient vital signs monitoring equipment can provide patients with the services as in hospital. The

emergency vehicle can transmit patients' real-time information in the form such as multi-channel high-definition live video, medical images, signs and condition records to the emergency centre, to assist doctors in making the treatment plan.

2) Remote diagnosis

Remote diagnosis services include remote consultation, remote ECG, remote medical imaging diagnosis etc. Various applications of remote diagnosis have specific requirements for image transmission. Remote diagnosis generally requires real-time video with the quality of 1080P, 30FPS or more. At the same time, it requires the real-time transmission of information collected by local medical equipment to the remote end.

3) Remote surgery

Due to the security of the public network and the characteristics of 4G networks, remote surgery has not yet been applied on a large scale. Remote surgery has higher demand for network transmission:

- Low latency, the RTT (Round-Trip Time) latency from the doctor's end to the patient's end is required to be less than 10ms;
- Minimum data transmission rate and bandwidth to ensure the smooth operation;
- Security, mainly the connection security and the security during execution. The reliability of the connection must reach 99.9999%, and the network should not be affected by security attacks.

4) Medical imaging cloud

5G medical imaging cloud using cloud computing and cloud storage technology transmits the patient's ultrasound, CT, X-ray and MR to the medical edge cloud through 5G. In order to realise the secure data sharing, the medical edge cloud determines the edge storage, cloud storage after data desensitization, or the cross-region storage according to different data application scenario.

2.3.2 Security Risk

5G will change how we communicate, work and deliver patient care both inside the hospital and externally via telemedicine, the Internet of Things and wearables. However, 5G also presents potential security risks.

- The greater number of devices, different types of users and diversified terminals accessing the network, including:
  - Public users, patients' family members who inquire about hospital information;

- Medical staff and network maintenance personnel who visit the hospital, medical information system and network management system;
- Medical equipment including wearable equipment, monitoring equipment, treatment equipment, etc.

To support the above users and terminals, the smart healthcare service faces the following security challenges from terminals, network, service and data.

- The large attack surface due to the massive increase in connectivity may lead to DDoS risk.
- More challenging medical data management due to massively increased number of devices and greater usage of virtualisation and the cloud. The data may be transmitted externally outside the hospital or the restricted area leading to the risk of privacy leakage of sensitive information.
- The need to extend security policies to new types of devices that will be impacted by 5G access.

2.4 Security Risk for Automotive

2.4.1 Industry Introduction

The automotive industry is changing towards autonomous driving and the always-connected paradigm also known as Connected and Automated Mobility (CAM). Electric cars as well as new business models regarding car sharing require mobile internet connectivity on several aspects, e.g., up-to-date navigation systems, guiding to the next free quick charger station, booking a car on the mobile phone application and finding the specific location where it was parked. The high-speed, low-latency communication between cars and the network is crucial for autonomous driving, accident prevention, as well as speed adjustments for an authorised speed and safe driving considering traffic lights.

The 5G system is already optimised for CAM services, known in 3GPP as Vehicle to Everything (V2X). Different use cases and scenarios from vehicles platooning to remote driving are supported. In addition, different attack scenarios and security risks were studied for the mitigation by the design of the specifications.

2.4.2 Security Risk

Recently vehicles (e.g., cars) have a vast amount of control units as well as millions of lines of code and together with the mobile connectivity the attack surface increases dramatically. This technical complexity also affects the end-to-end security of the overall system, even if there is

security by design in place for individual services and products. Cyber attackers can try to manipulate the system at different layers of the car communications and its services [4] e.g., in-vehicles services like the infotainment system, back-end services like remote car door opening, infrastructure and 3rd party services like car specific applications, enterprise technologies like the cloud servers or the production and maintenance systems. Attackers can target at privacy incidents, protocol attacks, data breaches etc. which can lead to vehicle tracking, malicious navigation, service malfunctions resulting in accidents or dangerous situations. Worst case examples include spoofed messages with wrong control information for automated driving that could lead to wrong steering decisions of the car, or taking remote control of driving, i.e. hijacking the car and passengers.

2.5 Security Risk for Smart City

2.5.1 Industry Introduction

With the adoption of 5G, smart city can provide advanced services in healthcare, industry and entertainment, enhance the efficiency of public services and governance capabilities, improve the accuracy and transparency of city services. Examples of services that can be enabled include:

- Smart city critical infrastructure: management and monitoring of numerous remote systems for traffic, energy and water facilities.
- Smart city transport systems: traffic and vehicle flow orchestration based on the collected data from numerous sensors around the city.
- Smart city post and delivery services highly dependent on communication schemes and remote communications.
- Smart city financial services: all payment machines are connected and require not only high-speed connected services but also secure communications for transactions.
- Smart city government complex operations: border monitoring, coastal safety and protest safety.
- Day-to-day services: 8K streaming, real-time mobile gaming with augmented/virtual reality experiences.
- Smart city emergency interventions: services for saving lives, drones delivering first aid and equipment, transport of a victim to the closest medical centre.

2.5.2 Security Risk

With the dramatic increase in the number of services and connected devices, attack surfaces and the intensity of the threats grows. The following are the key security risks:

- 5G network capability openness such as the introduction of network exposure function (NEF) and service-based architecture (SBA) may increase the risk of exposure, which brings security threats to the 5G core network and consequently the services in smart city.
- Serious DDoS attacks could put critical infrastructure and public safety at risk. Water or power could be stopped from reaching certain regions, endangering the lives of many.
- Regarding data and privacy security, e.g. in traffic systems, private information such as vehicle locations and driving trajectory may be leaked, and illegally traced and used.
- Critical infrastructure can't afford any malicious attacks, and public safety should be protected from false alarm messages.

3 5G NETWORK SECURITY CAPABILITIES AND REFERENCE FRAMEWORK FOR VERTICALS

To deliver the full potential of 5G, a reference framework of 5G network security capabilities that MNO can provide for the vertical industries is proposed. The architecture can be modelled into five security capability sets:

- Access security capability
- Network security capability
- Service security capability
- O&M security capabilityData security capability

Figure 1 illustrates the reference architecture with five security capability sets.

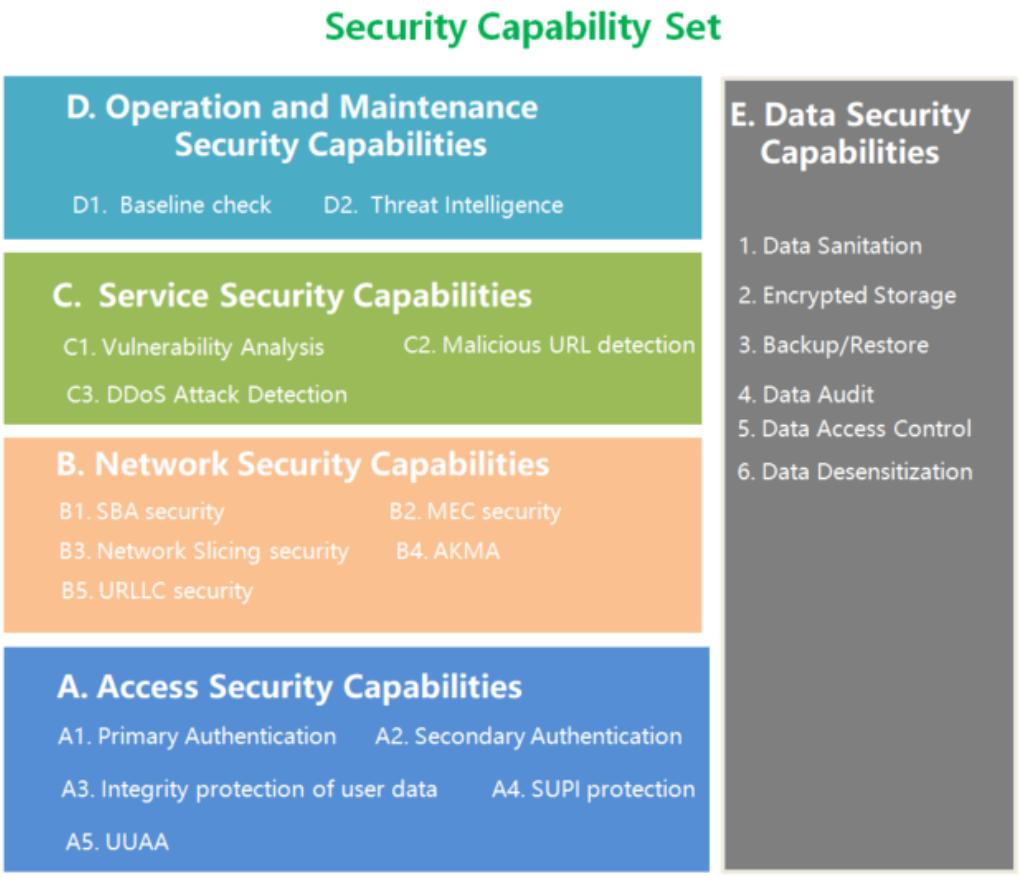

Figure 1: 5G Security Capability Sets for the Verticals

3.1 Access Security Capabilities

The access security includes the security mechanisms provided between the end user (UE) and the network, most of which are related to the air interface.

3.1.1 Primary Authentication

Primary authentication is one of the biggest enhancements in 5G security. Now, besides the 3GPP defined 5G-AKA, the IETF defined EAP-AKA' can also be used for primary authentication over the 3GPP and the non-3GPP access. While 5G-AKA requires NAS transport, EAP-AKA' is less restricted and can be used for devices that do not support NAS over non-3GPP access. While those two algorithms are mandatory in public networks, they are not applied in private networks where EAP-TLS is documented as an example for primary authentication. 5G-AKA and EAP-AKA' are key generating methods from which the resulting symmetric key in the UE and the network is further derived and then used to protect the NAS signalling between the UE and the AMF and to protect the RRC and UP on the air interface with the gNB.

3.1.2 Secondary Authentication

With the help of the secondary authentication, the UE can authenticate with an AAA-Server in an external data network. After the UE sends a PDU Session Establishment request, the SMF takes the role as EAP-authenticator and initiates the secondary authentication if required, based on the received subscription information from the UDM. The EAP messages are carried between the UE and the AMF in NAS messages and then forwarded to the SMF, which selects an UPF to relay the messages towards the external AAA-Server in the data network via IP connectivity. If the authentication is successful, i.e. the SMF receives the EAP-Success from the AAA-Server, the SMF proceeds with the PDU Session Establishment procedure and the UE has IP connectivity to the data network.

3.1.3 Integrity Protection of User Plane

While the RRC signalling messages over the air interface are always integrity protected, this was not the case for the user plane traffic in previous generations. The biggest issue was the required UE processing power for high data rates. Since Rel-15, the operator can set for specific PDU sessions a security policy for the user plane integrity protection (required, preferred, not needed). The security policy is provisioned to the gNB and the UE and the gNB can decide based on its capabilities whether to accept a PDU session with the policy set to "required". If the gNB cannot support a PDU session with the policy set to "required", the PDU session will be released.

So far for NSA deployments, the user plane integrity protection is not activated in SgNB when connected to EPC.

3.1.4 SUPI Protection

The transmission of the permanent subscription identifier was one of the biggest security issues of the previous generations, which made it easy with a simple identity request to retrieve the IMSI at a false base station (IMSI catcher) and to track the victim UE. In 5G, the permanent identifier SUPI is only transmitted concealed over the air interface, i.e. the UE is provisioned with a public key from the home network operator to encrypt the SUPI. The resulting concealed identifier SUCI is then provisioned over the air interface in case no NAS security is set up yet. So far two profiles with Elliptic Curve Integrated Encryption Scheme (ECIES) and a NULL scheme are specified. The NULL scheme which does not provide any protection may be used in case the home network operator does not provision a public key or the UE initiates an unauthenticated emergency call.

3.1.5 UUAA

UAV USS Authentication and Authorisation (UUAA) procedure [5] is initiated by the 3GPP network (i.e., 5GS and EPS) for an UAV after a successful primary authentication. The AMF initiates UUAA via UAS NF during registration if the UAV provides a CAA-level UAV ID and has an Aerial UE subscription. Or the SMF initiates UUAA via UAS NF during the PDU session establishment if the UAV requests access to UAS services. The UUAA is performed between the UAV and the USS, where the 3GPP network acts as the transport to support authentication related message exchange. The actual authentication method used for the UUAA is up to the USS. After a successful completion of an UUAA, the USS informs the UUAA result and provides an UUAA authorisation payload that contains UAS security information (if provided by the USS) to the serving AMF/SMF which initiates the UUAA via the UAS NF. The AMF/SMF upon receiving a successful UUAA, stores the successful result and CAA-Level UAV ID to allow the subsequent UAS service for the UAV and provides the authorisation payload to the UAV. Following a successful UUAA, if the UAV requests any PDU session establishment or modification related to pairing with a UAV-C, a pairing authorisation is performed by the USS. The USS and the AMF can anytime be triggered to re-authenticate (i.e., UUAA) the UAV. Similarly, the USS may anytime be triggered to revoke the UUAA.

3.2 Network Security Capabilities

The security aspects of 5G network include SBA security, MEC security, network slice security and AKMA.

3.2.1 SBA Security Mechanisms

5G has brought the SBA into the mobile networks, which introduces the paradigm shift from the classical model with point-to-point interfaces between network elements to service-based interfaces (SBI). The functionalities of each network element are provided by services which could be invoked by other network elements in an on-demand manner. This type of service orientation comes with new security implications. 3GPP has specified the security protection mechanisms for SBA including using TLS at the transport layer. All network functions support mutually authenticated TLS and HTTPS. In addition, the OAuth 2.0 framework is used to ensure that only authorised network functions are granted access to a service offered by another function. The usage of both TLS and OAuth 2.0 in SBA relies on the Public-Key Infrastructure (PKI) in place in the network. The Certificate Authority (CA) issues certificates to the network functions guided by proper management functions and policies. The public/private key pairs associated with the certificate can then be used for the asymmetric cryptography used in mutual authentication and signing/verifying of tokens that is required in SBA.

3.2.2 MEC Security

3GPP has defined the security features and mechanisms [6] based on the application architecture for edge application in 5G specified in [7]. The main security considerations include the authentication and authorisation between the entities of the application architecture, e.g. between the Edge Enabler Client (EEC) deployed in the UE and the Edge Configuration Server (ECS)/Edge Enabler Server (EES)/Edge Application Server (EAS) in the network. Apart from 3GPP, ETSI has also defined the MEC reference architecture, which considers a more comprehensive model including mobile edge host, virtualisation infrastructure, as well as mobile edge orchestrator and mobile edge platform manager. Based on the ETSI defined MEC architecture, the infrastructure security (physical or virtual) is provided to ensure the overall MEC security.

3.2.3 Network Slice Security

5G system provides optional-to-use network slice-specific authentication and authorisation [1] between a UE and an AAA server (AAA-S) which may be owned by an external 3rd party enterprise. The network slice-specific authentication and authorisation can be triggered based on the S-NSSAI after the primary authentication. Multiple EAP methods [8] are possible for slice-

specific authentication. Furthermore, since the ng-eNB/gNB can decide whether to activate user plane confidentiality and/or user plane integrity protection per PDU session according to the received user plane security policy, different slices can have the option to activate user plane integrity protection depending on the PDU session associated with.

3.2.4 AKMA

Authentication and key management for applications (AKMA) [9] is a cellular-network-based delegated authentication system in 5G specified by 3GPP. Using AKMA, a user can log in to an application service only based on the 3GPP credential which is the permanent key stored in the user's tamper-resistant smart card UICC. The user does not need any other credentials than his phone. The application service provider can also delegate the task of user authentication to the mobile network operator by using AKMA. Earlier generations of cellular networks include two similar standards for delegated authentication systems: generic bootstrapping architecture (GBA) [10] and a system called battery-efficient security for very low throughput machine type communication devices (BEST) [11]. The AKMA mechanism can be seen as a successor of these systems. AKMA helps to establish a secure tunnel between the user and the application server based on the AKMA key derivation and related procedures defined in [9].

3.2.5 Ultra-Reliable Low-Latency Communication Security

Ultra-Reliable Low-Latency Communication (URLLC) is a feature used for many vertical services like V2X or Industrial Internet of Things (IIoT), where reliability and low latency of the communication is crucial for the service. URLLC security features specified in [1] comprise redundant user plane paths based on dual connectivity and redundant transmission on N3/N9 interfaces.

When the redundant user plane paths are based on dual connectivity, the UE will establish two PDU sessions to two different gNBs (Master Node and Secondary Node), where the PDU sessions then take different paths in the network towards two different UPFs. These two PDU sessions must have the same security policy for integrity and confidentiality protection, which both gNBs must support.

For the redundant transmission on N3/N9 interfaces, the UE has a single PDU session towards one gNB. Then the data is transferred over different transport layer paths within two duplicated N3 tunnels from the NG-RAN to the UPF. NDS/IP mechanisms are used to protect the data transferred over the two duplicated N9 tunnels (UPF to UPF).

3.3 Application Security Capabilities

The application security consists of the security capabilities protecting various application system functions provided to vertical services.

3.3.1 Vulnerability Scan

Vulnerability scan provides the capability of vulnerability inspection, evaluation and management for application or network devices. Vulnerability scan includes functions such as:

- Website vulnerability scanning, web application vulnerability scanning and the detection of hidden links as well as Trojan horses.
- Various types of vulnerability detection on various scanned systems, including but not limited to vulnerabilities such as remote information disclosure, remote data modification, remote execution of commands, remote denial of service, missing patches and unnecessary services.

3.3.2 Malicious URL Detection

Known malicious URLs and suspected malicious behaviours can be detected or predicted earlier by collecting network traffic, DNS logs etc., combining the malicious feature information database with detection technology based on "feature + behaviour", which helps the 5G vertical industries to improve the security incident response and handling capabilities.

The operator's malicious URL detection capabilities include but not limited to the following functions:

- Collection of traffic data, DNS logs and other data with HTTP and WAP traffic feature collection and identification functions, to identify the domain name, URL, and IP address from the user requests.
- Real-time detection of known malicious domains/URLs based on the malicious feature database.
- Acquisition of information such as suspected malicious domain name/URL web page content, web page structure and web page source code, based on active crawling technology.
- Real-time monitoring and alert.

3.3.3 DDoS Attack Detection

MNO should quickly detect DDoS attacks and accurately schedule the traffic by collecting, analysing and scrubbing the traffic of the whole network, to provide the DDoS protection capability for 5G verticals.

The types of DDoS attacks that MNO can detect include: UDP Flood, UDP Fragment, ACK Flood, SYN Flood, FIN/RST Flood, TCP Misuse, TCP Connection Flood, TCP Fragment, ICMP Flood, ICMP Fragment, HTTP Flood, HTTP CC Attack, HTTP Slow Attack, HTTPS Flood, SIP Flood, DNS Query Flood, DNS Reply Flood, DNS Amplification, etc.

The basic capabilities of the operators' DDoS attack detection include but not limited to:

- Data collection capability: collect traffic related information from DDoS components.
- Data processing and modelling capability: statistically summarise the traffic data and the log information of related devices, analyse the correlation between them, and build the forecast model.
- Monitor and alert capability: the attack can be identified by setting dynamic threshold for the protected target based on the analysed result of the traffic data.

3.4 Operation and Maintenance Security Capabilities

The complexity and exposure of 5G networks, access of large numbers of IoT devices, and diversified security requirements of industry customers increase the complexity and workload of security management. Proactive and intelligent security O&M can reduce issues such as slow response and high costs caused by manual security management. The operators can provide different security operation and maintenance capabilities including baseline check, threat intelligence and so on.

3.4.1 Baseline Evaluation

Baseline evaluation provides vertical industries with the ability to check the security configuration of operating system, database and router, such as passwords, account permissions, identity authentication, access control, and security audits, identify security risks, perform security hardening, and meet local regulatory compliance requirements.

The contents of baseline evaluation include but not limited to the following:

- Credential: the complexity of the credential, credential update cycle, configuration of the encrypted storage.
- Account permission: the configuration for anonymous/default accounts, redundant accounts, expired accounts, management accounts, and RBAC.
- Identity authentication: the uniqueness of the identity, the handling of login failures, the restriction of illegal logins, and the information protection of remote management.
- Access control: the configuration of access rule, unauthorised access, and access control granularity.

- Security audit: the audit configuration of the user's operations, and the configuration of the security audit cycle, remote transmission of audit information, audit process protection, and operation permission of audit information.

3.4.2 Threat Intelligence

Operators generate an intelligent database based on a large number of data samples after analysis, and output the latest threat intelligence to vertical industries. Vertical industries can also transform intelligence into security rules and strategies, and then distribute them to the security devices so as to prevent threats in advance, detect and respond to attacks more quickly, and trace the source of subsequent attacks more efficiently.

The threat intelligence security capabilities have but not limited to the following functions:

- Real-time collection of data on operators' entire network;
- Regular collection of data on operators' entire network;
- Collection of vulnerability information from public vulnerability publishing platform;
- External warning interfaces to report the warning information to the relevant systems;
- Threat information online/offline query;
- Threat detection function to proactively discover threat attack behaviour;
- Traceability analysis function to accurately trace the source of attacks;
- Attack chain display function to provide basis for analysis and judgement;
- File sandbox detection function to perform in-depth detection of APT attacks.

3.5 Data Security Capabilities

Based on the data life cycle (collection, transmission, storage, processing, exchange and sanitisation), data security capabilities include the following:

- Encrypted transmission and storage: for sensitive data with high security requirements, the transmission and storage should be encrypted.
- Data access control: access to the storage data should be based on strong authentication and fine-grained authorisation (i.e., at the column or table level in a database).
- Data desensitisation capability: to prevent the over-privileged access, the data desensitization capability should be used according to the user's permission in the process of data storage, processing and exchange.
- Data sanitation: to prevent illegal restoration, data should be completely sanitised after migration and deletion.

- Data backup and recovery: data backup and recovery capability can help to ensure the data availability.
- Data audit: the data operations of authentication, authorisation, audit, desensitisation, traceability should be manageable, controllable and traceable.

4 GENERAL GUIDANCE ON USING THE 5G SECURITY CAPABILITY FRAMEWORK FOR TYPICAL VERTICALS

This paper provides a security capability framework for operators and vertical industries. In actual practice, the relevant entity needs to analyse the network and application scenarios, and perform security risk analysis to determine the mapping between the security requirements and 5G security capabilities for specific service scenario. It is recommended to use this white paper as a reference to select the best combination of security capabilities and measures to meet specific security requirement.

Figure 2 describes the recommendation for operators and vertical industries on how to use this white paper. The main process is as follows:

1) Operators and verticals communicate and clarify the Code of Conduct and Security Ethics requirements, and identify the assets to be used.
2) Analyse the security risks and threats of 5G network in different service scenarios with the methodology of threat modelling, risk assessment etc.
3) Map security risks and threats to specific security requirement, so as to clarify the security objective and core security requirements for vertical industry applications.
4) According to the security requirements, find the security templates in the Appendix. You can refer to the security capability in the security practice template if it fits for relevant scenario. If you have customised security requirements, you can refer to the security capabilities summarised in Chapter 3 to form a customised security capability set.
5) Based on the security practice template and the customised security capabilities set, verticals can request the corresponding security capability from the operator. Then the operator can select the security measures that meet the corresponding security capability.
6) Operators and verticals evaluate how security capabilities meet security requirements, including risk elimination assessment, security capability verification etc., then recalibrate and adjust the design according to the evaluation results.

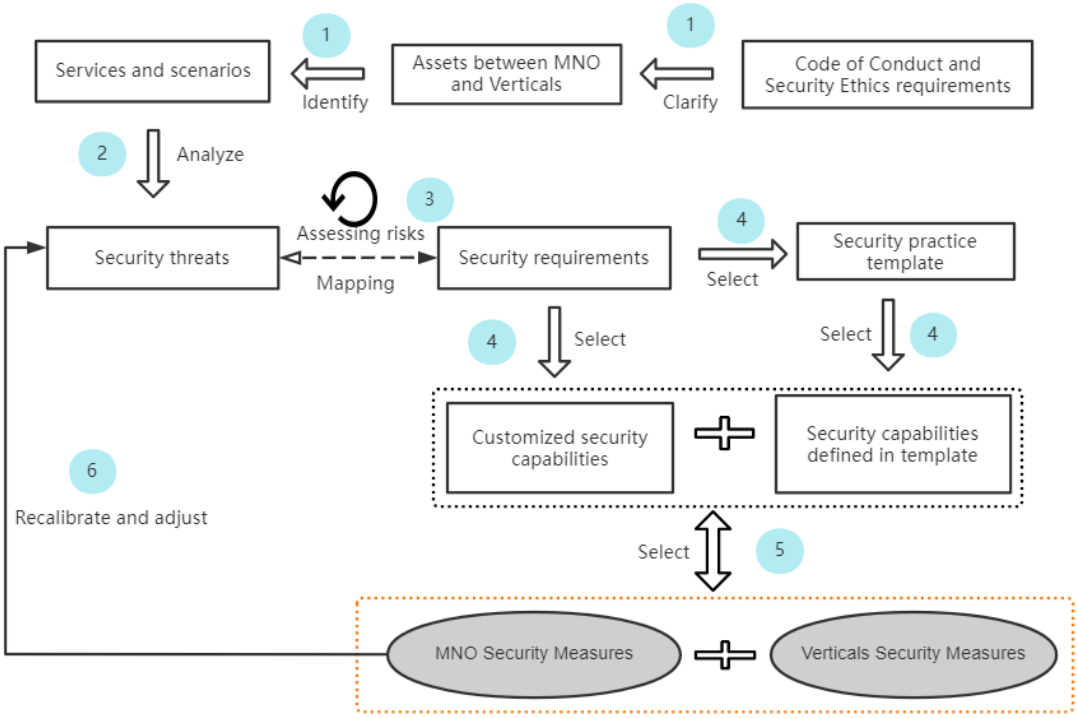

Figure 2: Guidance on How to Use the 5G Security Capability Framework

5 CONCLUSION

5G introduces brand-new network architecture and breakthrough technologies which bring huge development opportunities for social and economic transformation and provide key information infrastructure for the connection of everything. Specifically, the new capabilities provided by 5G include large bandwidth, low latency, high reliability, as well as network slicing, virtualisation, and artificial intelligence, which can more effectively empower vertical industries such as transportation, healthcare, augmented reality, emergency rescue, energy and power with wide range of application scenarios.

The integration of 5G with vertical industries has broken the boundaries between various organisations. Network security is more intertwined than before with potential security issues in vertical fields which put forward higher requirements for 5G security. During the development of 5G, operators and vertical industries have common concerns but different security requirements. Operators need to understand the security requirements from various vertical industries and provide customised and flexible security solutions. Vertical industries also need guidance to establish comprehensive and objective understanding of the security capabilities that 5G networks can provide, then form a consensus on 5G security and facilitate effective cooperation and implementation of 5G security measures. With efforts from operators and vertical industries, 5G can be more securely deployed in vertical industries and has greater economic and social advancement.

Based on the above purposes, this white paper provides a reference for all parties involved in the 5G network and vertical industries, so as to promote the rapid development of 5G in various vertical industries while effectively protecting the security of systems and data. 5G networks are evolving to a more open and intelligent architecture with new technologies rapidly emerging such as blockchain and artificial intelligence. We expect the continuous improvement of 5G security capabilities to meet the evolving needs of vertical industries.

LIST OF ABBREVIATIONS

AMF	Access and Mobility Management Function
AKMA	Authentication Key Management for Application
CA	Certificate Authority
CP	Control Plane
DoS	Denial of Service
DDoS	Distributed Denial of Service
EAP	Extensible Authentication Protocol
eMBB	enhanced Mobile Broadband
GBA	Generic Bootstrapping Architecture
IDS/IPS	Intrusion Detection System
IMSI	International Mobile Subscriber Identity
IPS	Intrusion Prevention System
MEC	Multi-access Edge Computing
mIoT	massive Internet of Things
MNO	Mobile Network Operator
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualisation
NAS	Non Access Stratum
NSSAI	Network Slice Selection Assistance Information
O&M	Operations & Maintenance
OS	Operation System
PDU	Packet Data Unit
PKI	Public-Key Infrastructure
RAN	Radio Access Network
SBA	Service-based Architecture
SBI	Service-based Interface
SMF	Session Management Function
SUPI	Subscription Permanent Identifier
S-NSSAI	Single Network Slice Selection Assistance Information
TLS	Transport Layer Security
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle

UE	User Equipment
UP	User Plane
UPF	User Plane Function
UUAA	UAV USS Authentication and Authorisation
URLLC	Ultra Reliable Low Latency Communications
VLAN	Virtual Local Area Network
VNF	virtual network function
VR	Virtual Reality
V2X	Vehicle to everything

REFERENCES

[1] 3GPP TS 33.501, Security Architecture and Procedures for 5G System (Release 17)

[2] Protecting Against the Threat of Unmanned Aircraft Systems (UAS), An Interagency Security Committee Best Practice, U.S. Department of Homeland Security

[3] Kaspersky, Security and Drones

[4] McKinsey & Company, Cybersecurity in Automotive, March 2020

[5] 3GPP TS 33.256, Security Aspects of Uncrewed Aerial Systems (UAS) (Release 17)

[6] 3GPP TS 33.558, Security Aspects of Enhancement of Support for Enabling Edge Applications (Release 17)

[7] 3GPP TS 23.558, Architecture for Enabling Edge Applications (Release 17)

[8] IETF RFC 3748, Extensible Authentication Protocol (EAP)

[9] 3GPP TS 33.535, Authentication and Key Management for Applications (AKMA) based on 3GPP Credentials in the 5G System (5GS) (Release 17)

[10] 3GPP TS 33.220, Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 17)

[11] 3GPP TS 33.163, Battery Efficient Security for Very Low Throughput Machine Type Communication (MTC) Devices (BEST) (Release 17)

APPENDIX

5G Service Security Best Practice Template

5G security capabilities can provide differentiated security assurance for vertical industries. With the combination of security capabilities, security best practice templates for specific vertical industry service can be created, copied and applied to different service scenarios, which provide certain security assurance such as edge protection, data privacy protection and access control. This section analyses the industries where 5G security solutions are relatively mature, summarises the universal security templates, and provides the reference of 5G service security construction and deployment for operators and vertical industries.

Table 1: 5G + Smart Grid Security Best Practice Template

Template Name	5G + Smart grid security best practice template
Template introduction	This template provides a set of security capabilities for 5G + grid services, and solves the security requirements of 5G network for differentiated grid services through network slicing capabilities, service security monitoring capabilities, access security capabilities, and data security capabilities, etc. It also enhances grid terminal access authentication and edge platform data protection capabilities.
Security capability set	A/B1/B2/B3/C/D/E
Applicable industry scenarios	• Production control service: including dispatch automation (e.g. PMU), differential relay protection, distributed automation system based remote power, FA of intelligent power distribution, etc., the security priority of this type of service is the highest. • Information management service: power transmission and transformation status monitoring, comprehensive monitoring of power distribution stations, video monitoring of electric substations, power consumption information collection, power measurement. • Mobile application service: on-site mobile construction operations, drone/robot inspection, manual inspection, power emergency communication.

Table 2: 5G + Smart Healthcare Security Best Practice Template

Template Name	5G + Smart Healthcare security best practice template
Template introduction	This template provides a set of security capabilities for 5G + Smart Healthcare services to solve the key security requirements, such as the isolation of internal and external hospital network, the protection of medical data through network slicing isolation, enhanced access security capabilities, and data security protection at edge, etc.
Security capability set	A/B1/B2/B3/C/E
Applicable industry scenarios	• Remote diagnosis, remote teaching • Remote surgery, remote imaging (ultrasound, CT, X-ray and MR), ambulances/medical examination vehicles

Table 3: 5G + Smart City Security Best Practice Template

Template Name	5G + Smart City security best practice template
Template introduction	This template provides a set of security capabilities for 5G + City services to solve the key security requirements, such as the secure access of various types of terminals, sensitive data protection and security situation monitoring and detection through network slicing isolation, access security capabilities, data security capabilities, and O&M capabilities, etc.
Security capability set	A/B/C/D/E
Applicable industry scenarios	• Smart city government operations, critical infrastructure management • Smart city transport system: traffic and vehicle flow orchestration • Smart city emergency interventions: water/fire disaster management, pandemic management

Table 4: 5G + UAS Security Best Practice Template

Template Name	5G + UAS security best practice template
Template introduction	This template provides a set of security capabilities for 5G + UAS services to solve the key security requirements, such as the access security capabilities which includes UUAA to access UAS services in addition to other general security functionalities, secure access for UAS related aerial services for various types of UAVs, UAV-Controllers which includes sensitive UAS data and C2 message protection, slicing isolation for UAS services, where requires service security capabilities and data security capabilities.
Security capability set	A1/A3/A4/A5/B1/B2/B3/C/E
Applicable industry scenarios	• Defence applications: Monitoring, securing ground troops, Precise identification and tracking of threat factors etc. • Commercial and Civil applications: Search and rescue operations, Agricultural and livestock survey/monitoring, oil and gas facility surveillance, package delivery, fire control, infrastructure inspection, aerial photography for journalism and film industry etc.

Table 5: 5G + Automotive Security Best Practice Template

Template Name	5G + Automotive security best practice template
Template introduction	This template provides a set of security capabilities for 5G + automotive services to solve the key security requirements, such as security for high speed, high reliable, low latency communication between cars and the network, as well as between applications in the car and the service provider in the network or at the mobile edge, e.g. traffic lights. V2X communication may be provided over dedicated slices with high requirements, thus network slice security and slice isolation have to be considered. Sensitive data on application layer for sensor data, car states and control information need to be protected on the different links between cars, network and mobile edge.
Security capability set	A/B/C/D/E
Applicable industry scenarios	• Autonomous driving • Real time traffic information exchange between cars and infrastructure • Platooning services • Application services such as navigation, free parking slot search, charging station search etc. • Fleet management • Remote driving