5G Security Architecture White Paper

November 2017


5G

Contents

Foreword

We are now seeing the first incarnations of 5G technology. It provides many capabilities that make it a preferred platform for the digitalized world. Solid security is one of the strengths of 4G networks and the same is expected from 5G. This cannot, however, be achieved just by adapting 4G security features to 5G system because the 5G service palette is more than just an extension from that of 4G. Completely new security functionalities and services are needed in addition to enhanced versions of 4G security features.

Cybersecurity is one of the defining characteristics of the modern world where leading trends are digitalization and globalization. Improving cybersecurity translates into improved prosperity and safer society. All tools are needed in the quest of better cybersecurity, and 5G technology holds a big promise in this quest. What is needed is to open up the strong security features of mobile networks in order to benefit also third parties and their various security needs. Of course, this needs to be done in a controlled manner so that this kind of opening does not jeopardize carriers' ability to secure their own operations.

We are going to show how two different goals can be achieved by 5G security. First goal is to secure the 5G platform itself. Second and at least as important goal is to provide tools for securing those many services that are built on top of the 5G platform.

01

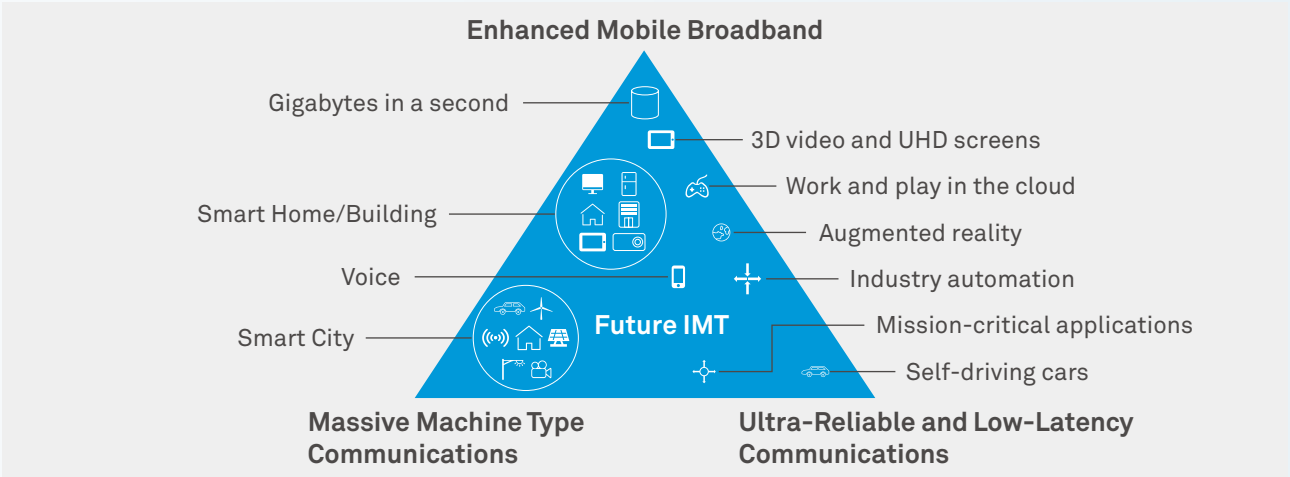
5G Security Requirements and Challenges

5G use cases defined by ITU-T widely support the digitalization of vertical industries (transportation, logistics, automated driving, healthcare, manufacturing, energy, and media and entertainment), and the development of public utilities (smart city, public security, and education). With the popularization of high-bandwidth, low-latency, and multi-connection 5G networks, a common network platform will be created to catalyze the technological and service development of various industries.

The expansion of mobile network services enriches the telecommunications ecosystem but also brings new challenges and requirements to mobile network security.

1.1 Diversified Business Requirments for 5G

5G is the next generation of mobile networks and the key to enabling the future digital world. 5G is neither a single piece of wireless access technology nor simply a combination of new wireless access technologies. Rather, 5G is a truly converged kind of network that offers seamless support for a variety of new network deployments. The International Telecommunication Union (ITU)has classified 5G mobile network services into three categories; enhanced mobile broadband (eMBB), massive machine type communications (mMTC), and ultra-reliable and low-latency communications (uRLLC).



- eMBB aims to meet user demands for an increasingly digital lifestyle, and focuses on services that have high requirements for bandwidth, such as high definition (HD) video, virtual reality (VR), and augmented reality (AR).
- mMTC aims to meet industry and governmental demands for an increasingly digitalized society, and focuses on scenarios that require high-density connections, such as intelligent transportation, smart grid, and intelligent manufacturing.

- uRLLC aims to meet market and enterprise requirements for increasingly digitalized industries, and focuses on latency-sensitive services, such as automated and assisted driving, and remote control.

Differentiated Security Protection Mechanism

In order for a single physical network to meet a range of different service requirements, the network generalizes corresponding network topology and functions through virtualization based on a unified physical infrastructure, generating a network slice for each service type. Each network slice is physically derived from the unified network infrastructure, which greatly reduces network construction costs for carriers operating multiple service types. Meanwhile, network slices are logically isolated and independent of each other, enabling different service types to be separately operated and maintained. This independency enables network function customization and independent O&M for each service type.

Different services will have different security needs. 5G networks accommodate a variety of services to meet the diverse needs of individual users and industry customers. When it comes to network architecture, end-to-end (E2E) network slices based on native cloud architecture have a rising prominence. Similarly, the 5G security design also enables the security requirements of a diverse range of services to be met.

Multi-dimentional Trust Models, and Scalable Identity Management Mechanism

The 3G and 4G era focused mainly on voice, text messages, and mobile broadband. In traditional mobile communications networks, the network and user authenticate each other. Users and networks constitute a mutual trust model.

5G mobile communications networks serve not only individual consumers, but also vertical industries in providing diverse services. The 5G era does not just entail faster mobile networks or more powerful smartphones, but also new services (such as mMTC and uRLLC services) that connect the world.

5G networks integrate traditional mutual trust models to construct multi-element trust models. Networks and vertical industries can collaboratively implement service identity management and increase the operational efficiency to fulfill users' diversified requirements.

4G networks mainly implement identity management on mobile broadband users, and adopt a symmetric key management system with a long-term key per device. These mechanisms fulfill carrier requirements. However, 5G networks are faced with a large number of new IoT and wearable devices, and traditional identity management mechanisms, with their rather expensive registration and account creation, may be unable to fulfill 5G network user management requirements. Therefore, identity management mechanisms must be expanded and optimized according to service features and new threats.

Security Capability Exposure

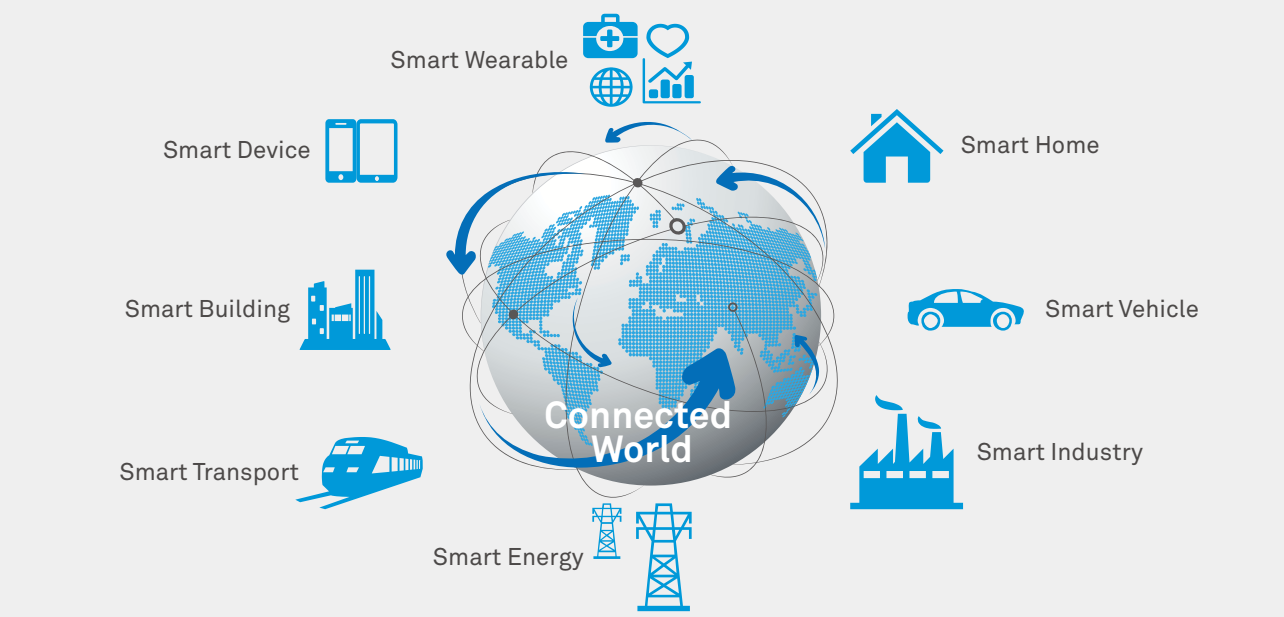
Service exposure brings both security challenges and more opportunities for carrier security services. As the provider and operator of the 5G infrastructure platform, telecom carriers are the enablers of service providers, and are trusted business partners of industry customers.

Vertical industries can directly use security capabilities exposed by carriers, reducing their service thresholds and costs, as well as shortening time to market (TTM). With security capability exposure, carriers can mobilize carrier network assets and infrastructure, creating new profit growth points. Security capability exposure can also change closed network operation mode, build a security ecosystem based on telecom networks, improve differentiated competitiveness, and form an ecological chain for carriers, vertical industries, security vendors, and individual users.

1.2 Widely Connected High-Coverage IoT Access

5G networks need to provide reliable network communications services for IoT, where high numbers of IoT devices have 5G networks need to provide reliable network communications services for IoT, where high numbers of IoT devices have higher demand of connection management. For example, in the Internet of Vehicles (IoV), vehicle-to-vehicle, vehicle-to-people, vehicle-to-road, and vehicle-to-network communications involve connections between hundreds of millions of sensor devices. The connection between these devices is vital to ensure traffic security, increase the operation efficiency of urban transportation, and reduce pollution. Smart meters installed in large cities upload large amounts of metering data

to grid data centers daily. Smart manufacturing demands always-online wide coverage and high-volume connection for continuously-operating machines, large numbers of products, and workers. This kind of constant connection that works anywhere anytime ensures the seamless connection between each and every links in the production chain.



There are a large number of unmanned IoT devices, and as a result the development of IoT raises new challenges to cyber security management and network defense. Therefore, 5G networks need to provide secure, reliable, and cost-effective network access control for large numbers of IoT devices.

Unified Security Management

5G systems use various access technologies and terminals. From a security management perspective, a unified security framework that includes common security core features can better meet the security requirements of 5G networks.

The heterogeneous access network is one of the key technological features of next-generation access networks. Access networks with multiple modes, access, and sites require coordination between concurrent access from different network standards (5G, LTE, and Wi-Fi), as well as concurrent connections of different site forms (macro, small, and micro sites).

Intelligent Security Defense

5G networks may be more exposed than previous generations, connect to outdoor IoT devices, have less hardware resources, be unmanned, and be more vulnerable to attack. It is likely that 5G networks will come to face a large number of network attacks. Existing manual defense mechanisms are not only slow in response, but also increase costs significantly as volume increases. Using necessary artificial intelligence methods can help provide mass threat protection for IoT devices. In addition network attacks are becoming increasingly automated, raising the likelihood of zero-day attacks. The security defense mechanism needs to change from passive to active in the new 5G system.

Unlike traditional devices, vertical industry IoT devices are numerous and therefore one network access point serves a great many more devices. 5G systems need to be able to handle distributed denial-of-service (DDoS) attacks that work by hijacking massive-IoT devices. A DDoS attack by many of devices against single network nodes will do much more damage than attacks by a single device. For example, at present, 3GPP is considering introducing public keys to verify permanent identity of devices to enhance privacy protection. However, this could increase the computation load on network nodes. Once attackers exploit this function to initiate verification requests from masses of devices simultaneously, the risk of a DDoS attack will increase significantly.

1.3 New IT Technologies and Architecture in 5G

To improve the flexibility, scalability, and rapid deployment of communications systems while reducing costs, the 5G network architecture uses new IT technologies, including NFV/SDN and a service-based architecture. While enabling flexibility, scalability, and rapid deployment, new IT technologies have also brought with them new security challenges for 5G.

System-level Security Protection and Access Authorization Mechanisms

The application of NFV virtualization technologies on a 5G network can further simplify the deployment and updating of network functions, enabling some network entities to be deployed as virtual NEs on cloud-based infrastructure. 5G needs to take infrastructure security mechanisms into account to ensure that 5G services can run properly in a virtualized environment. In addition, a better-defined security isolation method is required to enhance the security management between virtual NEs.

The 5G service-based architecture decouples network functions, defines common service-based interfaces; supports independent expansion, independent evolution, and on-demand deployment of each network slices; and allows other NEs to flexibly invoke network functions of all slices under authorization. Therefore, 5G security needs to consider the security of network function discovery, authorization, and invocation from the perspective of the overall security architecture.

New End-to-End Security Evaluation

Because of the exposed nature of carrier networks and diversified requirements of devices, it is required that a cautious security assessment be implemented when deploying network functions in virtualization environments, where the software and hardware are decoupled. Although 4G also proposes the concept of end-to-end security evaluation, the existing security assessing standards do not apply to virtualized network function infrastructure and system-level evaluation. Therefore, 5G security requires a new end-to-end security assessment mechanism to ensure secure deployment of 5G networks after the introduction of IT technologies.

02

5G Security Architecture Transformation

The following changes are needed in the 5G security architecture to support its expansion of industry customers, handle security challenges associated with mass IoT devices, and provide E2E security protection and defense measures.

2.1 New Security Features in 5G

2.1.1 Scalable Identity Management

5G needs a diversified identity management mechanism and an extensible identity management framework to address the security management needs of vertical industries and massive-IoT terminals.

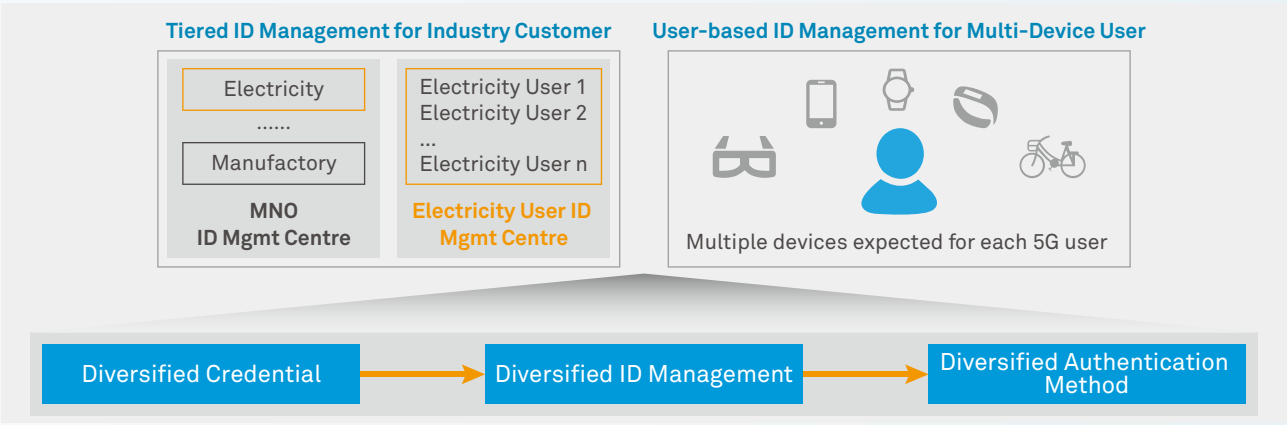
Diversified Identity Management Mechanism

Provide industry customers with tiered identity management mechanisms

Carriers can implement tiered identity management on huge numbers of IoT devices. One method of doing this is share the responsibility of user management between carriers and industry customers: carriers manage industry customer identities while industry customers manage end-user identities. For the masses of devices belonging to industry customers, network authentication and authorization can be connected to each industry customer, facilitating billing management. Industry customers can flexibly increase and reduce the number of devices to meet their own needs, if it is within the scope permitted by the carrier.

Provide individual users with user-based identity management mechanisms

In the future, individual users are likely to have numerous IoT devices and want to be able to flexibly manage multiple devices (such as wearable devices) within a specific scope, including network access and service attributes. For example, data traffic can be shared between the users' various devices either online or offline. The identity used by the same user on different devices should be interrelated. The authorization and identification of these devices should be associated with the user identity, and be managed through this single identity.



(U)SIM-based Scalable Identity Management Framework

Using symmetric key–based identity management for eMBB devices

5G eMBB services are mainly targeted at mobile broadband users. The symmetric key–based identity management used in 4G can still satisfy the requirements of people-oriented service requirements. Symmetric key–based identities can also help carriers to manage devices and issue other types of credentials. Thus, even if the 5G requires diversified credential and identity management mechanisms, the identity management based on (U)SIM cards and symmetric keys will still be used and play an important role in the 5G era.

Extend identity management to support asymmetric keys for numerous IoT devices

IoT devices are widely used in 5G scenarios, including mMTC and uRLLC. Symmetric key–based identity management usage in IoT devices has some disadvantages, such as long authentication chains and high authentication costs. These may lead to high overall costs of authentication, and hinder the integration of carrier networks and vertical industries, and is hard to provide efficient support for mass IoT devices. Therefore, in providing services to large numbers of IoT devices in 5G, an asymmetric key-based identity management mechanism is needed. Such a mechanism allows carriers to flexibly and efficiently manage IoT devices and wearable devices belonging to industry customers, and improves the authentication efficiency in network access.

The identity management functions of symmetric and asymmetric keys may be deployed according to different service slices on the network side, but carriers must establish unified identity management systems.

2.1.2 Flexible Deployment and Orchestration of Security Functions

An important feature of the all-connected 5G network is network capability exposure, which enables vertical industries to control some network resources to independently create third-party services. Network capability exposure facilitates the diversity of services and introduces differences in security requirements due to different service security requirements. If the 5G network has a security mechanism that ensures the security of every service and breaks it down into fine-grained, usable, and combinable security capabilities, it can establish security mechanisms and defense measures that meet service security requirements through deploying and orchestrating corresponding security capabilities when new services are created.

The diversity of 5G service security requirements also complicates security configuration and management. If it continues to rely on manual configuration, management, and responses, it would lead to inefficiencies and high costs. Therefore, security capabilities should be managed automatically, including the deployment, scheduling, configuration, and invocation of security functions.

Fast Deployment of Security Functions and Exposure of Security Capabilities

The 5G service-based architecture decouples network functions. Once these functions are decoupled, independent network expansion, independent evolution, and on-demand deployment are enabled. Therefore, based on the service-based architecture, the security functions can be deployed quickly through modularizing security functions.

Fast deployment and invocation of security functions

Based on the service-based architecture, specific security functions or capabilities of network functional entities can be defined as services, so that other NEs can independently invoke security functions on the basis of authorization. The security functions or capabilities herein may include security context management, key management, and so on. The service-based definition of security functions enhances the refined and flexible management and support invocation of security functions and support the authorization of such invocation

The variety of 5G business security requirements also complicates security provisioning and management, which can lead to inefficiencies and costs if relied on manual approach to configure and manage the security features. Therefore, based on the automatic management of network functions, it is also necessary to have automatic management of security functions, including the deployment, arrangement, configuration and invocation of security functions.

Security Capability Exposure

The exposure of network capabilities to industrial partners requires corresponding security mechanisms to ensure service security. Just like network capabilities, security capabilities of 5G networks can be exposed to vertical industries.

Security capability exposure requires modularized security function deployment in order to enable easy invocation through APIs. Then by combining different security functions, the end-to-end security requirements for various vertical services can be quickly satisfied. Benefiting from security capability exposure, vertical industries can deploy services in a highly secure way without building the security system themselves, which makes it easier to launch a new service while reducing the time-to-market (TTM). Carriers can fully utilize their network security infrastructure, enrich service experience, and create and share value with vertical industries.

The exposed security capabilities can include user identity management, security context management, authentication, and key management.

2.1.3 Agile and Efficient Distributed Security Deployment

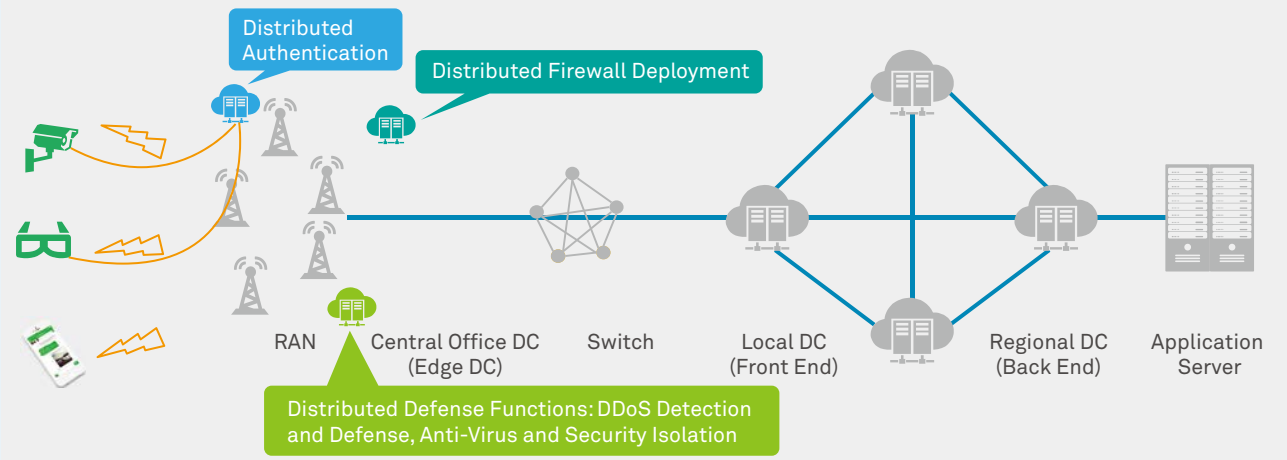
In the future, interconnection and service exposing modes will bring with them new security challenges, including large-scale network attacks and mass device authentication signaling storms. Therefore, 5G requires a distributed security mechanism to cope with security challenges and to deploy distributed security functions according to requirements of service defense, authentication, and management. This distributed security mechanism includes distributed authentication and distributed defense.

Distributed Authentication Mechanism

Mass IoT device connection is an important 5G service scenario, but mass concurrent access authentication of IoT devices poses high requirements on network data processing. In the traditional centralized authentication mechanism, each authentication on devices requires the invocation of the core identity management node, which causes signaling overload on this node. Therefore, the 5G security architecture requires a distributed authentication mechanism to meet the authentication requirements of large numbers of devices. In the distributed authentication mechanism, device authentication can be performed on multiple distributed authentication nodes at the same time, reducing access to core identity management nodes and supporting centralized and simultaneous mass IoT device authentication. Distributed authentication nodes can be deployed flexibly based on the distribution of IoT devices, reducing costs and complexity of authentication. Distributed authentication mechanisms include certificate-based security mechanisms and identity-based security mechanisms.

Distributed Security Defense Mechanism

The fundamental concept behind distributed security defense technologies is to prevent attacks from the source by deploying distributed defense capabilities on network edge nodes, achieving more agile security defense. Specifically, to implement an access defense mechanism for large numbers of IoT devices, 5G security can deploy security defense capabilities on access points closer to IoT devices, such as RAN or edge DC. Defense capabilities include DDoS defense mechanisms and distributed antivirus technologies. In this way, 5G networks can cope with attacks immediately, and reduce access attacks threats.



2.1.4 Network Slicing Security

Network slicing is one of the important enabling technologies of 5G and future communications networks. It is service-oriented and critical to the support of vertical industries' digital transformation. Slicing security is also customizable and enables the network to provide differentiated and tailored security features, functions, and performances to suit the customers' needs. It uses one shared physical network infrastructure to meet various requirements of applications and industries, enable vertical industries to shorten the TTM when launching new security services, simplify security O&M, and reduce operation costs.

Network slices share a single physical infrastructure. While this does bring with it significant advantages, it also exposes the network to new potential security risks that need to be addressed carefully. Network slicing encompasses multiple domains, each of which contains a variety of network functions, resources, and links. Each domain's own security issues and mitigations should be considered, for example terminal security, access network security, core network slicing security, and bearer transmission security. More importantly, network slices are end-to-end logical networks and the security should be considered holistically.

Differentiated Slice Security Mechanisms

Different devices may have different requirements for security protection and performance in different application scenarios. For example, eMBB devices used for video playback have similar security requirements to those used in LTE in terms of device authentication and encryption/decryption. Low-cost sensors, due to their limited computing power and constrains in energy consumption, may not have high security requirements, and so light-weight authentication, encryption, and decryption algorithms may be more suitable. For uRLLC devices, fast access and strong encryption algorithms are desirable. Therefore, differentiated security mechanisms must be provided for network slices for a wide variety of devices and applications.

Secure Isolation of Slices

A defining characteristic of slices is that different slices are logically isolated, but share common physical resources. So the primary issue is how to achieve secure isolation of slices. Without proper isolation, attackers with legitimate access to one slice can use the slice as a springboard to easily attack other slices. For example, attackers may use the slice to illegally occupy the resources of the targeted slices, causing them to fail to provide services for authorized users. In another example where a device can access multiple slices simultaneously, a lack of slice isolation may result in beaches of data confidentiality (such as data leakage) and integrity.

Slice isolation should be considered throughout every part of its life-cycle, from the slice generation stage to the running phase. A slice involves multiple domains, such as devices, the access network, core network, and bearer network. The isolation of each domain needs to be considered, together with holistic considerations of links and communication between them.

Slice Access Control

One of the objectives of end-to-end slicing is to support diversified business models and meet the requirements of different industries and applications. Due to the broad diversity of slice and device types, the slice access control of devices should also be diverse and should be optimized accordingly, so that users can access slices rapidly and receive efficient security protection against a wide range of attacks.

Slice Management Plane Security

The slice management architecture describes the functions and relationships of the components in the life-cycle of network slices, which is comprised of the slice design and preparation, configuration and activation, operation, and de-commissioning phases. Security risks may potentially exist in each phase. For example, attackers may compromise a slice template through malicious software and steal data from all generated slice instances. Attackers may also attack a slice through the configuration interface during the operation phase. In the de-commissioning phase, attackers may obtain confidential data if the slice is not properly handled. As some network capabilities and interfaces can be exposed to customers, each party must be authenticated and authorized before being allowed access to these capabilities and interfaces.

2.1.5 Proactive and Intelligent Security Automation

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. Manual security management may result in issues such as slow response, high costs, and errors. So it is recommended that 5G introduce AI-based proactive defense technologies and integrates with the traditional IT network defense mechanism to establish an intelligent network defense system based on unified intelligence analysis and automatic threat response.

Abnormal Event Detection and Analysis

The complexity and exposure of the 5G network greatly increase the types of security threats. Therefore, artificial intelligence is being introduced to detect unknown and complex attacks. For example, in the software and virtualization scenarios, the detecting and tracing of the sources of complex attacks require the use of machine learning to combine VM anomaly monitoring, malicious code detection, and core network traffic anomaly detection. It is also useful for intelligent detection and comprehensive analysis of abnormal systems, codes, and traffic.

ICT Security Intelligence Sharing and Collaboration

Collaboration among carriers and industry customers needs to be established to rapidly cope with security threats, exchange security intelligence in real time, and achieve automatic and intelligent security collaboration. For example, when a carrier detects an abnormal device, it is required to inform industry customers to install patches or clear malicious codes on the device. Carriers and industry customers can exchange exception information with each other to detect, analyze, and locate abnormal attacks quickly, and reduce the response delay that comes from manual intervention.

Automatic Defense

Multiple security functions, such as vulnerability scanning, security hardening, firewall, malicious code detection, and traffic anomaly detection, are deployed at each layer of a network. Collaboration between multiple security functions is becoming more and more complex, which makes the introduction of artificial intelligence significant in reducing the workload of manual security management. Adoption of AI in network defense can improve the automation of attack prevention, security monitoring, security detection, attack blocking, and attack isolation, achieving the goal of agile security management.

2.2 Enhanced and Carried-Over 4G Security Features

Enhanced mobile broadband is one of the main ingredients of 5G networks. It is also a straight-forward extension from 4G networks. Therefore, it is quite natural that security features for eMBB can be built based on 4G security features. The standards for 5G are developed in a phased manner, and eMBB is dominant in the first phase. It follows that eMBB security plays a great role in the first release of 5G security standards. Putting all this together, the natural way to build

5G security is to begin with 4G security and extend it as required by new security requirements stemming from novel 5G features.

From the identity management, device and network element security, security algorithm, and service-based architecture points of view, a comparison for 4G and 5G has been made in the following table.

	4G	5G
Identity management	(U)SIM-based identity management	Reuse the (U)SIM-based identity management in eMBB scenario, meanwhile support diversified identity management mechanism
Device security	Key storage, security parameter transmission, and security calculation	Reuse 4G device security for UE, meanwhile support lightweight IoT device security
Network element security	4G network element (e.g. base station) security	Reuse 4G device security for UE, meanwhile support network element security under NFV scenario
Data protection algorithm	4G security algorithms	Reuse 4G security algorithms, meanwhile may support longer keys and new algorithms for future attacks
Network domain security	Secure end-to-end tunnel establishment mechanism Security association establishment mechanism	Reuse 4G network domain security, meanwhile support network domain security under service based architecture

(U)SIM-based Trusted Root for eMBB Scenarios

Users' permanent identity and root key form the basis for identity management and authentication. For 4G terminal applications, the (U)SIM-based identity management mechanism provides secure storage protection and an interactive security environment for root keys. In addition, based on the (U)SIM authentication mechanism, bidirectional authentication can be established between devices and networks. Therefore, the 4G (U)SIM identity management and authentication mechanism can be used on 5G networks for service types such as eMBB.

New Device Types

Key storage, security parameter transmission, and security calculation on 4G user devices can be implemented in the security protection state, so 5G user terminals can inherit these existing mature security mechanisms. In addition, 5G is expected to introduce various IoT devices with limited hardware resources, low costs, and low power consumption. It is not recommended to continue to use the security mechanism of traditional mobile devices. Instead a lightweight data protection and secure transmission mechanism should be designed and deployed.

Network Equipment Security Enhancement

LTE base stations are located in relatively unsecure environments, so base stations are required to support equipment startup, key storage, and security calculation in a secure environment to defend against attacks. 5G needs to continue the security environment of 4G base stations. In addition, 5G also involves the participation of other mass network equipment and NFV deployment. Therefore, 5G needs to further enhance basic security capabilities of network equipment in accordance with a range of different deployment modes.

Defense Against Attacks to New Encryption Algorithm

Network access security prevents attacks from air interfaces, including air interface signaling from the UE to the AN, signaling protection from the UE to the CN, and mobility management security of the UE. 5G security needs to extend this type of protection, which forms a basic security requirement for mobile communications. In addition, 5G may use a

stronger security protection algorithm and a longer security key to defend against future attacks.

New Protocols in the SBA Architecture

As a lower-layer protection method for data communication between the backhaul network and core network, network domain security provides a secure end-to-end tunnel establishment mechanism and a security association establishment mechanism. A 5G core network must also support data transmission between NEs and between security domains. Therefore, the mature network security mechanism can continue to be used. In addition, 5G security also needs to take into account the SBA architecture when selecting the security mechanism of the network domain, and which communication method is best suited to secure communication between different operators.

2.3 Scalable, Orchestrated, and Intelligent 5G Security Architecture Framework

5G security architecture should be based on core security functions in early eMBB scenarios, and expanded to support mMTC and uRLLC. A scalable and orchestrated intelligent 5G security architecture needs to be built, quick deployment of differentiated security capabilities needs be implemented, and security capability exposure needs to be supported.

5G Security Architecture Design Principles

Logical security architecture is built on top of the 5G network architecture. The security architecture should implement security defense and protection on the overall 5G features. All security features are decoupled from other network features or functions, and have the ability to self-update and expand without affecting the overall 5G network.

The security architecture is designed based on domains and planes, in accordance with the layer-based and plane-based principles of the protocol design. A range of security features are included in the architecture to facilitate efficient security function invocation. Logical security functions tend to be independent from other network functions, and the security plane could be interpreted to a group of security functions independently deploy or configured or tailored in carrier networks. From the perspective of security, different network connections have different security risk levels. In the design, border defense should be based on security domains. A distributed security framework enables defense measures to be deployed on a position close to the potential point of attacks to improve the response speed and reduce the impact range.

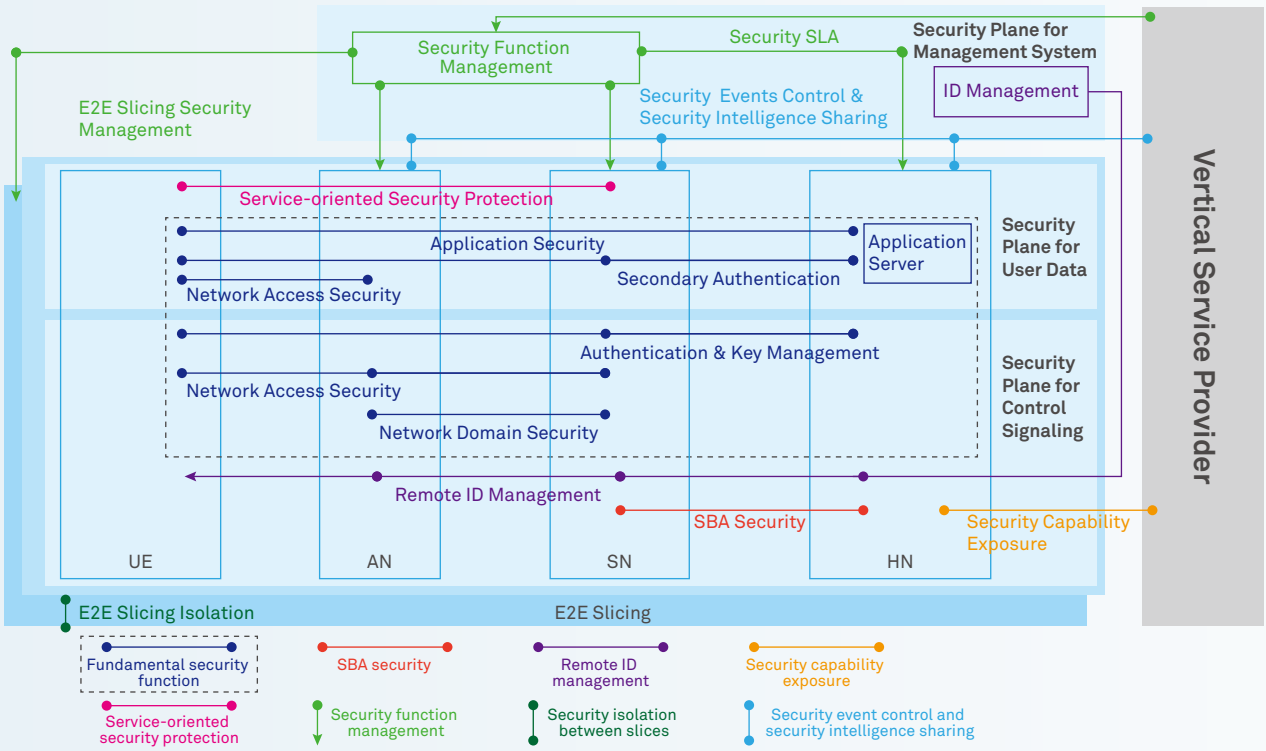
The security architecture is scalable and orchestrated. In different service scenarios, customers have different expectations for security, and different events may also trigger the adjustment of security capabilities as well as the reconfiguration of security functions. Therefore, only a scalable and orchestrated security architecture can support flexible and rapid service deployment.

Logically independent and service-based security interfaces are needed, which support security capability exposure. 5G architecture is service-based architecture, because security is a logical capability of 5G, it needs to be service-based also. Service independent interfaces may be invoked at any time to provide security capability exposure for vertical industries.

An end-to-end full-service security management system needs to be established. The potential hijacking of single-point devices or equipment puts equipment across the network at risk. So setting up a set of sophisticated end-to-end management systems with high security levels is a basic necessity for network-wide security.

5G Security Architecture Framework

The framework in this paper has extended fundamental security functions in eMBB scenarios, to cope with security requirements and challenges in mMTC and uRLLC scenarios ,and support slice security and security capability exposure, as well as, enhancing the intelligence of network security management. The security functions in the blue dashed box correspond to the security architecture in the “Overview of 5G security architecture” sections in 3GPP TR33.899 version 1.3.0. The grey solid box corresponds to the security functions and interfaces related to vertical industries, and the security functions and interfaces in other part of the figure correspond to MNO.



Three Security Planes and Two Security Mechanisms

Logical security functions tends to be independent from other network functions, and so the security plane could be interpreted to a group of security functions independently deploy or configured or tailored in carrier networks.

Security Plane for Management System

Based on traditional security basic capabilities (account management and security logs) on the management plane, security capabilities on the management system are as follows.

Service-oriented security function orchestration

During the life-cycle management of network and network slicing generation, the security function orchestration entity of the management plane tailors security functions and security protection mechanisms according to the security SLA of service providers in a differentiated manner, orchestrates network security functions within corresponding service slices, and efficiently deploys security functions required by slices.

The security function orchestration entity obtains the security SLA from the northbound interface, generates a security policy based on the security SLA, and establishes security functions for the corresponding slice. In addition, the security function orchestration entity delivers the security function orchestration policy to the carrier's home network, service network, and access network through the corresponding network security function orchestration interface. The security domain of the network control plane configures the security protection mechanism in the slice based on the security orchestration policy.

The process of obtaining the security SLA depends on the process of obtaining the SLA of the vertical industry. The process of the security function orchestration depends on the orchestration process of other network functions in the slice.

Scalable identity management

The scalable identity management mechanism continues to inherit identity management based on (U)SIM cards, and supports the identity management mechanism based on the asymmetric key to uniformly manage the identities of industry customers, users, and terminals.

eMBB terminals will continue to use identity management through the symmetric key, while industry customers' IoT terminals, such as the Internet of Vehicles (IoV), smart grid, and smart manufacturing industry terminals may consider to use asymmetric identity management mechanisms. Carriers that use the public key to distribute identities may delegate industry customers to remotely manage identities of IoT terminals.

Security Plane for User Data

Based on traditional security basic capabilities on the user plane, security capabilities on the user plane are as follows.

Service-oriented differentiated security protection

The security protection mechanism of the user plane is tailored according to the relevant security policies to meet differentiated data transmission protection requirements of different services. Based on the service security policy delivered by the security function orchestration function, a user plane data protection mechanism that connects the user equipment and the network is configured on the control plane, such as the key length and cryptography algorithm, and the security protection corresponding to the policy is implemented on the user plane. The carriers' network is responsible for deciding, negotiating, and configuring user plane security protection based on service security policies, network policies, and terminal policies.

Security Plane for Control Signaling

Based on the traditional security basic capabilities on the control plane, security capabilities on the control plane are as follows.

Carriers can flexibly invoke security functions

According to the security orchestration policy on the management plane, the network security function can be flexibly deployed based on the service-based architecture and virtualization technology. Flexible security function deployment and invocation can efficiently support security capability exposure.

The data protection mechanism between the user device and network is decided and negotiated based on service security policies, network policies, and terminal policies, including the key length and cryptography algorithm of the user plane protection.

supports scalable authentication mechanism and remote identity management

Tiered identity management mechanisms enable remote identity management of IoT terminals and wearable devices, provide authentication mechanisms based on symmetric keys, and can be expanded to support asymmetric authentication.

Slicing Management Security Mechanism

In general, slicing management security includes three aspects: Slicing Security as-a-Service or SSaaS, the slicing lifecycle security, and the intelligent slicing security O&M. SSaaS enables operators to provide differentiated and customized security packages for vertical industries and monitor the performance of the packages. Operators may adjust the packages or delete parts of them and rearrange resources based on the monitored results or other requirements. Security packages may include encryption algorithms, encryption parameters, capabilities for blacklist and whitelist configuration, authentication methods, and isolation strength etc. SSaaS is provided through specific interfaces on the management plane, which must be securely protected, and can only be accessed by authorized parties.

Slicing lifecycle security ensures security in slice design, configuration, activation, operation, and termination phases. It also protects the released security resources from exploitation of software vulnerabilities when a slice is decommissioned.

Intelligent slicing security O&M includes automated slicing security function orchestration, slicing security policy control, and the alarm generation for slices through vulnerability scanning and anomaly detection technologies etc.

Proactive and Intelligent Security Defense Mechanism

The network Security Events Control & Security Intelligence Sharing center schedules and coordinates security components to implement intelligence sharing and security policy control between carriers' networks and vertical industries based on security events. By achieving distributed deployment of security components and automatic configuration of security policies, the security defense approach of 5G networks change from manual and passive response to intelligent and proactive defense, forming a unified collaborative security defense mechanism.

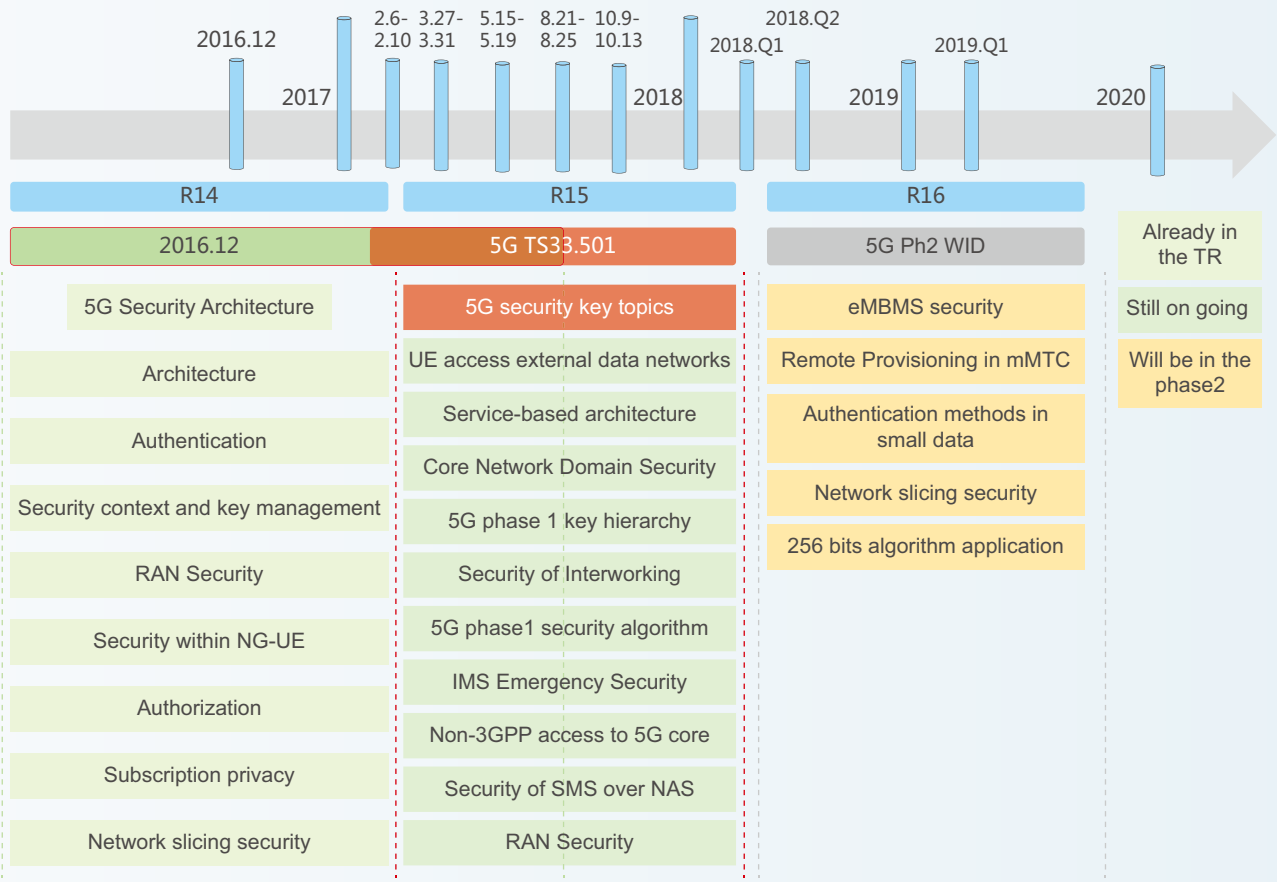
2.4 Overview of Global 5G Security Standardization

The global unified 5G security technology in the standard organizations such as ITU□3GPP and IMT-2020(5G) has been made great progress. In detail, most of the security features of 5G phase1□such as security architecture, access security, user data confidentiality and integrity protection, mobility and session management security, the privacy of the users identity and so on are already done. At present, 3GPP SA3 has a study item on 256 bits key length algorithm in 5G network. For 256 bit key length algorithm, 3GPP SA3 decide that the protocol shall support the new algorithm until March, 2018, but the specified algorithm will not be limited. The specific cryptographic algorithm standardization shall be started in 5G phase2.

The 3GPP SA3 has been in 5G safety standardization work, including Study Items (such as the study of the next generation of system security technology) and Work Items (e.g. the security architecture and process of 5G system), R15 is planned to be completed in March 2018. 5G network security features and solutions has close relationship with the radio access network and core network architecture, so except 3GPP SA3, 3GPP SA1, SA2, RAN2, RAN3 are all closely related to 5G security standardization work.

The new technology (such as NFV/SDN etc.) will influence the 5G network security, the study scope of ETSI NFV security group including NFV security architecture, privacy protection, lawful interception, MANO (management and scheduling) security, certificate management, security management and etc. The research of the ONF (Open Network Foundation) and ITU-T involves the standardization of SDN security.

The 3GPP 5G security standardization progress is as follows, other standardization progress can refer to this figure.



03

Promote 5G Security Standardization and Building a 5G Security Ecosystem

In the future, more diversified service scenarios and new network architectures will drive the 5G security architecture to transform and will promote industry partners to build a new security ecosystem that ensures the digital transformation requirements of various 5G network industries are met.

- Legislation organizations are expected to strengthen security regulations and policies, and strengthen the foundations of the cyber security ecosystem.
- Traditional telecom standard organizations and vertical industry organizations are expected to proactively cooperate and exchange needed products with each other for their mutual benefit, build a healthy security standard ecosystem, and make joint efforts to improve the security defense capabilities of products and solutions.
- The industry is expected to facilitate active communication of different technologies in different fields, share technology innovations, accelerate the speed of 5G security technology upgrading, and jointly provide the best security solutions for 5G networks.

3.1 End-to-End Security Assessment System

Standards-based security evaluation is an effective way to ensure 5G network security. Global security assessment standards can integrate the best security practices in the industry and improve the security level of the entire industry. In addition, global security assessment standards help reduce certification costs of the entire industry.

5G security evaluation criteria should cover cloud-pipe-device to support the construction of a 5G end-to-end security assessment system.

Devices and the cloud: 5G networks will bear more services, and a wide variety of device types will access 5G networks. In addition, 5G networks will also provide interfaces with third-party applications. Unsecure terminal devices and third-party applications may bring risks to 5G networks, which can be resolved through the introduction of security assessment standards for terminal devices and third-party applications..

Pipe: Virtualization technologies will be widely applied on 5G network devices. Security evaluation standards for 5G network devices must be able to evaluate the security of 5G network devices achieved by virtualization cloud technologies.

Conclusion

We have now presented all key concepts of 5G security. In addition, we have seen the big extension potential of those concepts in protection of many different services. Scalable identity management, distributed authentication, network slice security are examples of 5G security cornerstones. The great legacy of network access security in 4G and even earlier mobile generations is fully utilized in 5G security.

It can be concluded that 5G is a big step forward, not only in enabling new digitalized industries but also in cybersecurity. The providers of 5G networks have a golden opportunity to contribute for advances in protection of people in modern society.

References

[1]3GPP TS 23.501: "System Architecture for the 5G System".

[2]3GPP TS 23.502: "Procedures for the 5G System".

[3]3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[4]3GPP TS 38.470: “NG-RAN; F1 General aspects and principles“.

[5]3GPP TS 38.472: “NG-RAN; F1 interface control plane protocol”.

[6]3GPP TS 38.474: “NG-RAN; F1 data transport”

Trademark Notice


, HUAWEI , and 
are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
Other trademarks, product, service and company names mentioned are the property of their respective owners.

NO WARRANTY

THE CONTENTS OF THIS MANUAL ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE LAWS, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE,ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS MANUAL.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO CASE SHALL HUAWEI TECHNOLOGIES CO., LTD BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOST PROFITS, BUSINESS, REVENUE, DATA, GOODWILL OR ANTICIPATED SAVINGS ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS MANUAL.

HUAWEI TECHNOLOGIES CO., LTD.
Bantian, Longgang District
Shenzhen518129, P. R. China
Tel:+86-755-28780808

www.huawei.com