HUAWEI

Huawei 5G Security White Paper

Partnering with the Industry for 5G Security Assurance

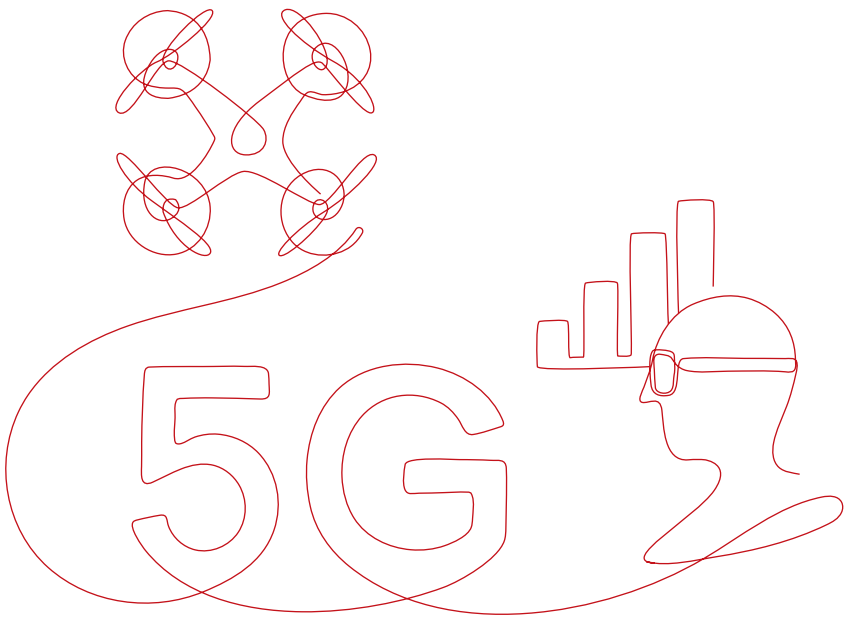
Contents

01 Executive Summary

This 5G security white paper focuses on the following:

- Why is 5G secure? How do experts from industry and standards organizations ensure that 5G security risks can be effectively managed in terms of security protocols and standards as well as security assurance mechanisms?
- Why are Huawei 5G products secure? What technical and management measures has Huawei adopted to ensure cyber security of Huawei equipment?
- How to ensure 5G cyber security, including Huawei's support for cyber resilience and recommendations on how to deploy and operate 5G networks in a secure manner.
- How to ensure 5G operations comply with national security regulations, including suggestions for regulators in developing laws and regulations and implementing regulatory policies.
- How to continuously improve the 5G security level from the perspectives of different stakeholders in order to address future challenges. It is recommended that stakeholders work together using their expertise to build a 5G security system, continuously improve 5G security, and ensure that 5G security risks are controllable.
- Unified, authoritative, and continuously evolving standards, such as the Network Equipment Security Assurance Scheme (NESAS) jointly defined by the GSMA and 3GPP, are required in the assessment of 5G cyber security to promote continuous improvement of 5G security in the mobile industry.

This document describes 5G security standards, Huawei's 5G security system, and the joint efforts of stakeholders.



02 5G Is On, Bringing Both Opportunities and Challenges

2.1 5G Will Change Our Lives with Diversified Applications

As mobile broadband begins to reach every corner of the world, people's desire to unfold the blueprint of the coming fully connected world is increasing. In the era where all things will be connected over mobile broadband, 5G networks need to meet the requirements of unprecedented connectivity in three scenarios:

- Enhanced Mobile Broadband (eMBB) focuses on services that require ultra-high bandwidth, such as high-definition video (4K/8K), virtual reality (VR), and augmented reality (AR), meeting user demands for a digital life.
- Massive Machine-Type Communications (mMTC) focuses on scenarios requiring high-density connections, such as intelligent transportation, smart grid, intelligent manufacturing (Industry 4.0), and smart logistics, meeting user demands for a digital society.
- Ultra-Reliable and Low-Latency Communications (URLLC) focuses on latency-sensitive services, such as autonomous driving/assisted driving, Internet of Vehicles (IoV), and remote control, meeting user demands for a digital industry.

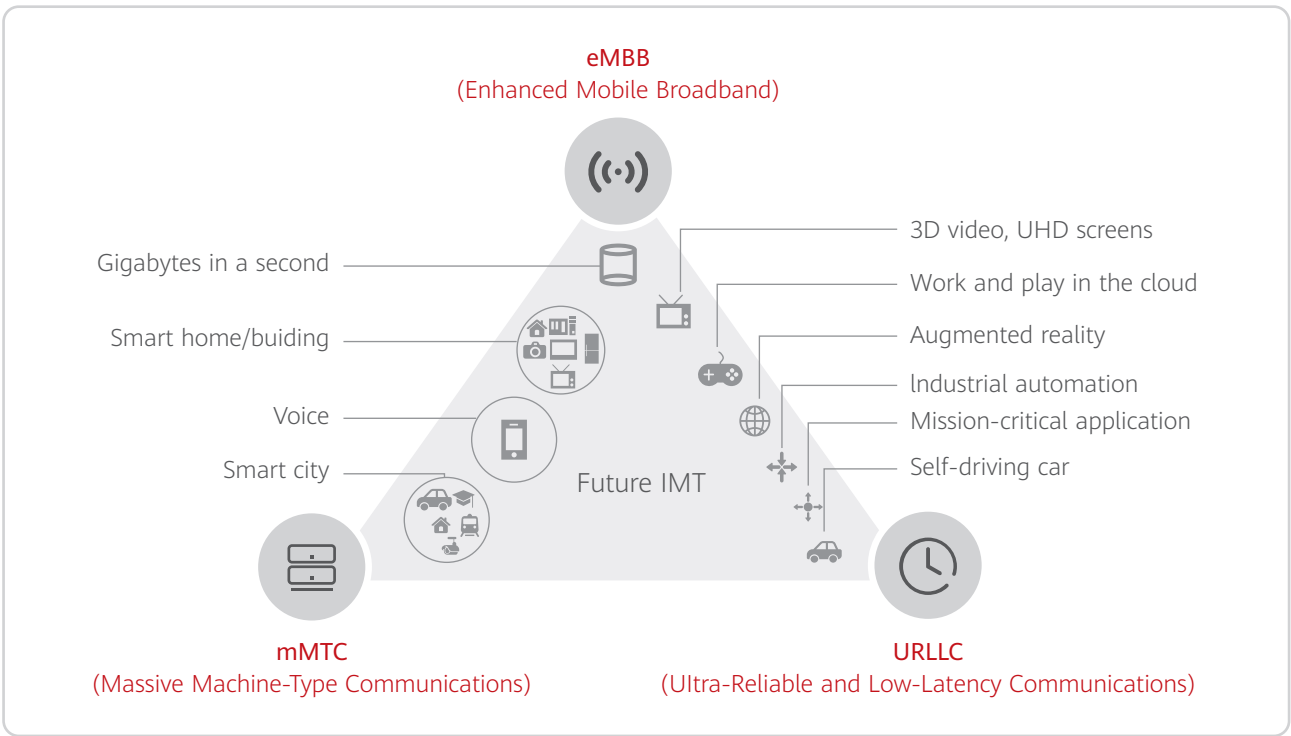


Figure 1: 5G scenario

To meet the increasing requirements for new experiences and applications, 5G scenarios need to be enhanced and expanded. Huawei proposes the 5.5G industry vision and defines three new scenarios that enhance the three standard 5G scenarios. This allows the evolution from supporting Internet of Everything (IoE) to realizing intelligent connection of everything, and creates new value for social development and industry upgrade. The three new scenarios are as follows:

- Uplink Centric Broadband Communication (UCBC) will enable a 10-fold increase in uplink bandwidth. This is perfect to support high-volume upload in production and manufacturing scenarios for machine vision and massive broadband Internet of Things (IoT), accelerating their evolution towards intelligence.
- Real-Time Broadband Communication (RTBC) supports high bandwidth and low latency. It will also enable a 10-fold increase in bandwidth at a given latency and reliability, offering an immersive experience for the interaction between the physical and digital worlds.

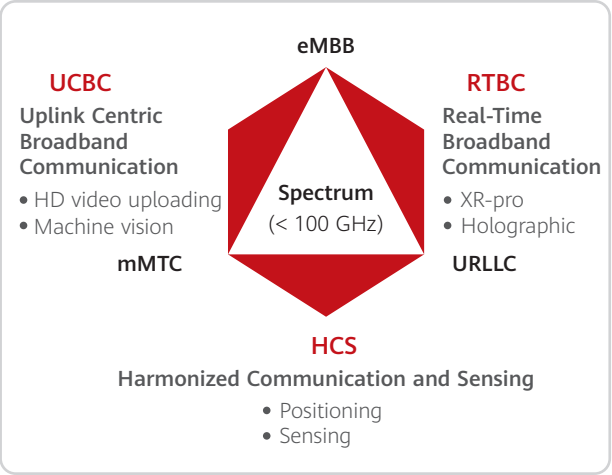


Figure 2: 5.5G scenario

- Harmonized Communication and Sensing (HCS) extends the capability boundaries of mobile networks and enables centimeter-level positioning and sensing. It applies to indoor digital management, intelligent transportation, and low-altitude drone scenarios.

So far in 5G evolution, visions have been proposed, technical directions have been defined, and the pace of standards formulation has been determined. Currently, the action plan is being implemented. As the communications industry has high expectations for the future development and evolution of 5G, Huawei will continue to innovate and work with the industry to create a golden decade for 5G.

2.2 5G New Architectures, Services and Technologies Will Bring Security Challenges

In general, most threats and challenges faced by 5G security are the same as those faced by 4G security. However, the additional security challenges brought by new architectures, services, and technologies to 5G networks must be considered[1].

New Architectures

In terms of new architectures, new 5G software and network deployment architectures introduce new interfaces and boundaries. The new Service Based Architecture (SBA) and slice architecture shall adapt to new security requirements, such as SBA-based identity authentication, slice security protection, and multi-slice risk management, to prevent attacks. In 5G network deployment, the User Plane Function on the core network is moved from the central equipment room to the Mobile Edge Computing (MEC), introducing new boundaries. The convergence of connection and computing also creates new security challenges.

New Services

As for new services, 5G networks empower vertical industries and shall provide better security capabilities for industry applications to meet these industries' security requirements.

New Technologies

In terms of new technologies, cloudification and virtualization technologies are widely used on 5G core networks, which creates security risks in the sharing and virtualization of infrastructure resources. In the future, the impact of quantum computing on traditional cryptographic algorithms shall also be considered to ensure network security.

The industry is working together to address new security risks faced by 5G architectures, technologies, and services, and address potential security challenges through unified 5G security standards, common 5G security concepts, and an agreed 5G security framework. In 2020, 111 companies (including their subsidiaries) from around the world sent technical experts to six SA3 meetings[2] to develop the latest 5G security standards. The 3GPP SA3 Working Group has established 42 projects to analyze security threats and risks in various 5G scenarios. Conclusions are gradually being drawn from these projects and implemented in security standards. The GSMA and 3GPP jointly define NESAS[3] to assess the security of mobile network equipment development and verification. The GSMA 5G Cybersecurity Knowledge Base proposes the security concept of shared responsibility and baseline security controls based on typical 5G network threats and key security solutions[4]. The top-down design principles of the 5G security architecture ensure a systematic, dynamic, and adaptive security framework. With these measures, we believe that 5G cyber security is manageable and verifiable.

03 5G Security Standards Improve on Their Predecessors

3.1 5G Security Architecture Inherits 4G Security Architecture

Currently, 3GPP SA3 has developed 5G R16 security standards and is developing 5G R17 security standards[5]. To ensure that 5G standards move ahead consistently at all technical levels, the 3GPP is developing security standards at the same pace as that of architecture and wireless standards. 5G R15 standards have defined security architectures and security standards for eMBB scenarios, covering Standalone (SA) and Non-Standalone (NSA) architectures. Based on the 5G R15 security architecture, 5G R16 and R17 standards will cover security optimization for mMTC and URLLC scenarios, and provide further enhancements to the security infrastructure.

The security architecture of mobile networks is hierarchical and classified by domain in design. The 5G security architecture contains the following security domains: network access security, network domain security, user domain security, application domain security, SBA security, and visibility and configurability of security, where SBA security is a new security domain in 5G. SBA security is the set of security features that enable network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. These features include network function registration, discovery, and authorization security aspects, as well as protection for service-based interfaces. An SBA forms the basis of the 5G core network. To ensure security between UEs in the SBA, security mechanisms such as Transport Layer Security (TLS) and Open Authorization (OAuth) are needed.

The 5G network inherits the 4G network security framework, but provides enhanced security features. The 5G access and core networks have clear boundaries. Even though some 5G core network functions (such as the User Plane Function [UPF]) are moving closer to applications, they are still part of the 5G core network and therefore comply with its traffic distribution policy. The access and core networks interconnect through standard protocols, support inter-vendor interoperability, and have standards-based security protection mechanisms[6].

3.2 Security Hardening of 5G Standards over 4G Standards

The 5G SA network supports more security features to tackle potential security challenges in the future 5G lifecycle. 5G NSA and 4G networks share the same security mechanisms and work in standard and practice consistently to keep improving their security levels.

R15 defined the following 5G security hardening features:

- **Stronger air interface security:** In addition to user data encryption on 2G, 3G, and 4G networks, the 5G SA architecture provides user data integrity protection to prevent user data from being tampered with.

- **Enhanced user privacy protection:** In 2G, 3G, and 4G networks, users' permanent IDs (international mobile subscriber identities — IMSIs), are transmitted in plain text over the air interface. Attackers can exploit this vulnerability using IMSI catcher attacks to track users. In 5G networks, users' permanent IDs (in this case, subscription permanent identifiers [SUPIs]) are transmitted in ciphertext to defend against such attacks.

- **Better roaming security:** Operators usually need to set up connections via third-party operators. Attackers can forge legitimate core network nodes to initiate Signaling System 7 and other attacks by manipulating third-party operators' devices. 5G SBA defines Security Edge Protection Proxy (SEPP) to implement security protection for inter-operator signaling at the transport and application strata. This prevents third- party operators' devices from tampering with sensitive data (e.g. key, user ID, and SMS) exchanged between core networks.

- **Enhanced cryptographic algorithms:** 5G R15 standards currently define security mechanisms such as 256-bit key transmission. Future 5G standards will support 256-bit cryptographic algorithms to ensure that such algorithms used on 5G networks are sufficiently resistant to attacks by quantum computers.

In R16 and R17, the existing security infrastructure was further optimized by enhancing SBA security, providing user-plane integrity protection for 5G NSA and 4G networks, and other means.

- **Enhanced SBA security:** The new SBA architecture of the 5G core network provides network functions as services. The relevant standard defines service security mechanisms for the architecture, including finer-grained authorization between network functions (NFs) and stronger protection for user-plane data transmission between operators, which ensures the security of data transmission on the signaling and user planes of the core network[7].

- **User-plane integrity protection for 5G NSA and 4G networks:** The user-plane integrity protection mechanism of 5G SA networks is introduced to 5G NSA and 4G networks to enhance air interface security[8].

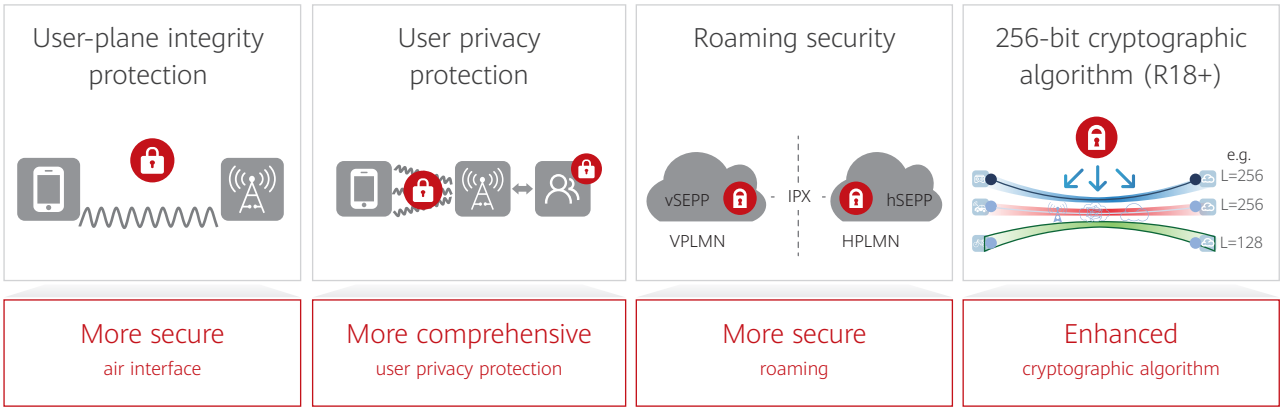


Figure 3: 5G security hardening features

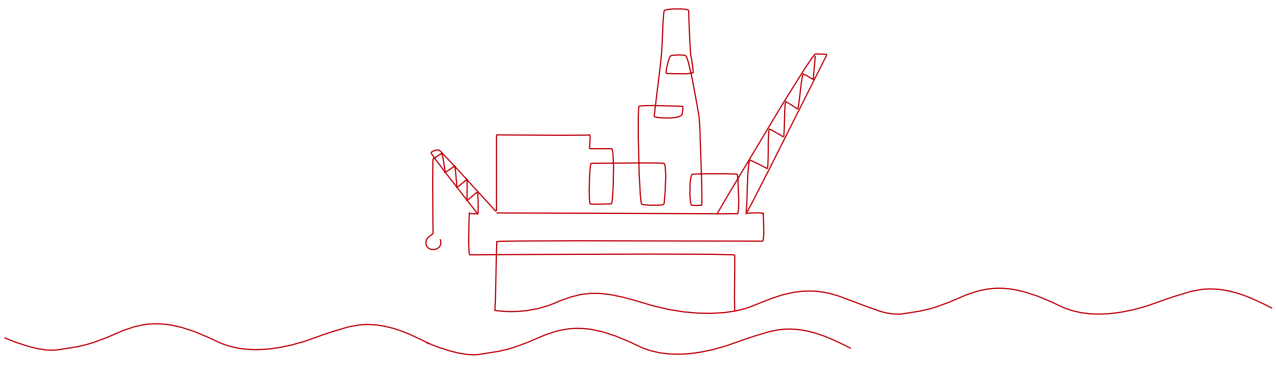
As standards evolve, 5G cyber security features continue to be expanded and enhanced to tackle potential security challenges and enhance security throughout the 5G lifecycle.

3.3 Vertical Industries Empowered by 5G Standards Security

Based on R15's basic security architecture, R16 and R17 provided diversified and customized security features for vertical industries, for example, security of small data transmission on IoT devices, security of redundant session transmission in URLLC, authentication and authorization for slices, and flexible authentication for multiple forms of private networks, to meet diversified security requirements of different industries and open up 3GPP security capabilities to third parties.

- **Cellular Internet of Things (CIoT) data transmission security:** Defined secure transmission and simplified mobility protection mechanisms for small data transmission to meet requirements for user data protection on IoT devices in unique small-scale data transmission scenarios [9].
- **Redundant session transmission security:** Defined equivalent user-plane security policies of the redundant session transmission mechanism to implement the same level of security protection for two user sessions during redundant transmission in high-reliability and low-latency scenarios[10].
- **Slice access security:** Defined the authentication and authorization process for slice access from UEs to meet vertical industries' requirements for controllable user access and authorization when using 5G networks[11].
- **Private network authentication security:** Defined authentication modes in different enterprise private network forms to flexibly meet different industries' authentication requirements. In the public network integrated non-public network (PNI-NPN), for example, in scenarios where a slice provided by the operator is used to access a private network, slice authentication can be used to authenticate and authorize access from vertical industry users. When the data network provided by the operator is used to access a private network, enterprises authenticate and authorize vertical industry users. For independent private networks, initial authentication modes (EAP framework) other than symmetric authentication are introduced for UEs[12].
- **Security capability openness:** Used the basic key provided on operators' networks to protect the data transmission of third-party applications, and provided a security capability openness framework for third-party services to use operators' networks[13].

5G networks provide mobile network services for more and more vertical industries. The security of 5G networks addresses potential security challenges to services.



3.4 5G Security Assessment Becoming Standardized

Cyber security assessment mechanisms shall follow globally accepted uniform standards to ensure that their operations are cost-effective and sustainable for the ecosystem. NESAS jointly defined by the GSMA and 3GPP has been used to assess the security of mobile network equipment. It provides an industry-wide security assurance framework to improve security across the mobile industry. **NESAS defines the security requirements and assessment framework for security product development and lifecycle processes, and uses security test cases in the Security Assurance Specifications (SCAS) defined by 3GPP to assess the security of network equipment.** Currently, 3GPP has initiated security evaluation of multiple 5G network equipment, and major equipment vendors and operators are actively participating in the NESAS standard formulation.

NESAS promotes security cooperation and mutual trust in the global mobile communications industry, and enables operators, equipment vendors, and other stakeholders to jointly promote 5G security construction. It provides customized, authoritative, efficient, unified, open, and constantly evolving cyber security assessment standards for the communications industry, and is a good reference for stakeholders such as operators, equipment vendors, and government regulators.

NESAS brings the following benefits to equipment vendors:

- Provides accreditation from the world's leading mobile industry representative body
- Delivers a world-class security review of security related processes
- Offers a uniform approach to security audits
- Avoids fragmentation and potentially conflicting security assurance requirements in different markets

NESAS brings the following benefits to mobile operators:

- Sets a rigorous security standard requiring a high level of vendor commitment
- Offers peace of mind that vendors have implemented appropriate security measures and practices
- No need to spend money and time conducting individual vendor audits

NESAS brings the following benefits to regulators:

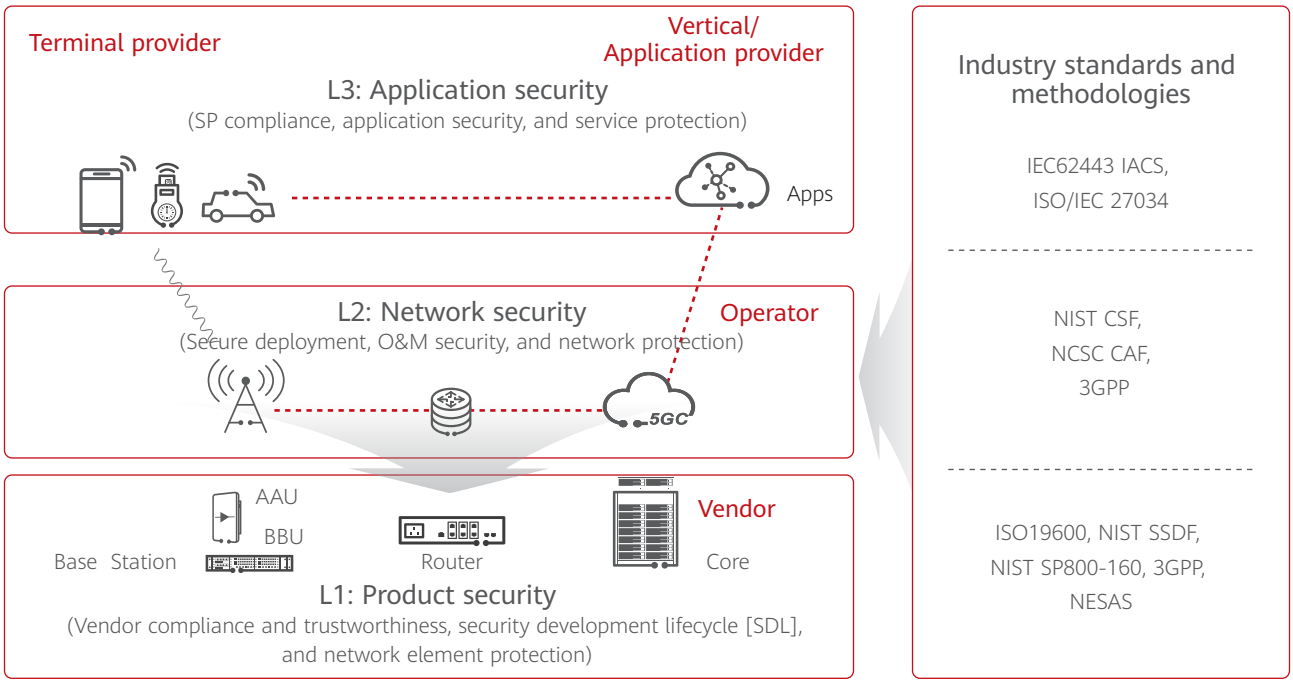
- Developed by the mobile communications industry to prevent standards fragmentation
- Open, maintained by the industry, and continuously evolving and enhanced
- Cost-effective, innovative, a low market entry barrier, and promoted security benefits

About NESAS[3]

The GSMA released NESAS 1.0 in October 2019, continued to drive the evolution of NESAS based on industry requirements, and released NESAS 2.0 in February 2021. Currently, the NESAS ecosystem has been established. Mainstream equipment vendors actively participate in NESAS evaluation, where Huawei's RAN and core network are the first to pass its audit and security function tests. The world's top audit bodies and well-known testing labs are qualified for evaluation. Multiple tier-1 operators require that NESAS compliance be included in 5G bidding documents.

04 Multi-Party Collaboration and Shared Responsibility for 5G Security

5G cyber security can be divided into three layers based on the security model in the communications industry: application security, network security, and product security (in descending order).



Inspired by 3GPP 33.501 security architecture

Figure 4: Three-layer cyber security model

- Application security is for both traditional mobile end users and vertical industries that provide or use a range of applications. This security layer requires collaboration among operators, device suppliers, and application providers to ensure the security of 5G networks and the users and services they support. Application security is not heavily dependent on the security of network pipes. Vertical industries must take responsibility for the security of their solutions, protect critical assets at the application layer from network attacks, promptly detect security threats, and quickly restore basic services. The Open Web Application Security Project (OWASP) provides an excellent set of best practices on the development assurance for application security, including the application security threat analysis methodology, Application Security Verification Standard (ASVS), and penetration test guide. In addition, ISO 27034 provides systematic suggestions for ensuring application security from an organizational perspective, including identifying risks from three dimensions, defining application security levels, and establishing application security controls (ASCs) along with mapping organization normative framework (ONF).

- Network security is usually managed and operated by operators. They consider network compliance and the security of network design, deployment, O&M, and operations, and continuously perform comprehensive risk assessment based on network components as well as the network equipment and architectures provided by vendors to ensure effective management of security threats. There are mature specifications and methodologies in the industry for reference. For example, the Identify, Protect, Detect, Respond and Recover (IPDRR) methodology defined by the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) can help operators systematically address cyber risks. The 3GPP also defines technical security specifications for network interworking.
- Product security must be provided by equipment vendors. It focuses on the compliance, secure development process, and security capabilities of products. Security assessment is critical for product security. It provides a basis for assessing whether network equipment and components are designed and implemented in compliance with security requirements. NESAS, established by the GSMA and 3GPP together with global operators, equipment vendors, and third parties, is a widely recognized NE security assurance standard in the industry.

5G cyber security is a shared responsibility of key stakeholders, including operators, interconnection providers, equipment vendors, application providers, standards organizations, governments, and regulators, each with their own clearly defined responsibilities. These responsibilities, when fulfilled, can enable the secure deployment and operations of 5G systems.

05 Huawei Is Committed to Ensuring 5G Equipment Security and Cyber Resilience

5.1 Incorporating Cyber Security Activities into the Product Lifecycle

Huawei R&D focuses heavily on security throughout product development, adhering to the principle of security by design and security in process. Cyber security activities built into the process are performed in strict compliance throughout the entire product lifecycle, so that security requirements can be implemented in each phase.

Huawei R&D provides the Integrated Product Development (IPD) process to guide end to end (E2E) product development. Since 2010, Huawei has started to build cyber security activities into the IPD process according to industry security practices and standards such as OWASP's Open Software Assurance Maturity Model (OpenSAMM), Building Security In Maturity Model (BSIMM), Microsoft Security Development Lifecycle (SDL), and NIST CSF as well as cyber security requirements of customers and governments. Such activities include security requirement analysis, security design, security development, security test, secure release, and vulnerability management. Check points are used in the process to ensure that security activities are effectively implemented in product and solution development. This practice improves the robustness of products and solutions, enhances privacy protection, and ensures Huawei provides customers with secure products and solutions.

- In the security requirement analysis phase, Huawei collects cyber security and privacy requirements through various channels such as customer feedback, industry standards, laws and regulations, and certifications. It also gains insights into the service scenarios of products and solutions; analyzes the network architecture, deployment environment, O&M management, and service characteristics to identify potential threats; assesses risks in terms of security, privacy, resilience, availability, reliability, and safety; and determines security requirements based on the threat assessment results. Huawei will analyze and manage these requirements.

- In the design phase, Huawei has extended the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) threat model to include the attack tree and privacy impact assessment (PIA) elements, calling this new model Advanced STRIDE (ASTRIDE). Huawei has also developed security design standards to guide engineers in security design, with reference to the best practices in the industry.

- In the development phase, Huawei has developed its own secure coding standards with reference to the best practices of the industry's secure coding standards of Computer Emergency Response Team (CERT), Common Weakness Enumeration (CWE), SysAdmin, Audit, Network, Security (SANS), and OWASP. Huawei implements a series of security development controls to ensure the quality of completed code, for example, local static code analysis using tools, the committer review mechanism, and enabling compiler security options.

- In the test phase, Huawei has designed test cases based on the threat modeling to verify the effectiveness of the threat mitigation measures designed. Huawei has adopted a "many eyes and many hands" security verification mechanism. In addition to security tests of product lines, Huawei established the Independent Cyber Security Lab (ICSL), which is independent of the R&D system, to be responsible for the final verification of products. Test results are directly reported to the Global Cyber Security & Privacy Officer (GSPO), who has veto power over product launch. Third-party testing and verification schemas are supported with the cooperation of customers and industry regulators.

- In the version release phase, Huawei scans software packages for viruses and releases signatures before version release. It then verifies the integrity of software packages during software transfer and delivery to ensure that they are not tampered with.

- In the lifecycle management phase, Huawei continuously focuses on security vulnerabilities to ensure customer service continuity. The vulnerability response process involves vulnerability awareness, vulnerability validation, remediation solution development, and post-remediation activities. The Product Security Incident Response Team (PSIRT) detects vulnerabilities through internal and external channels and identifies all products with vulnerabilities based on dependencies. It classifies, assesses, and grades detected vulnerabilities, and assigns them to relevant teams for remediation. All patches comply with Huawei's code quality requirements and undergo strict security tests. The PSIRT tracks vulnerability remediation to ensure the effectiveness of remediation solutions.

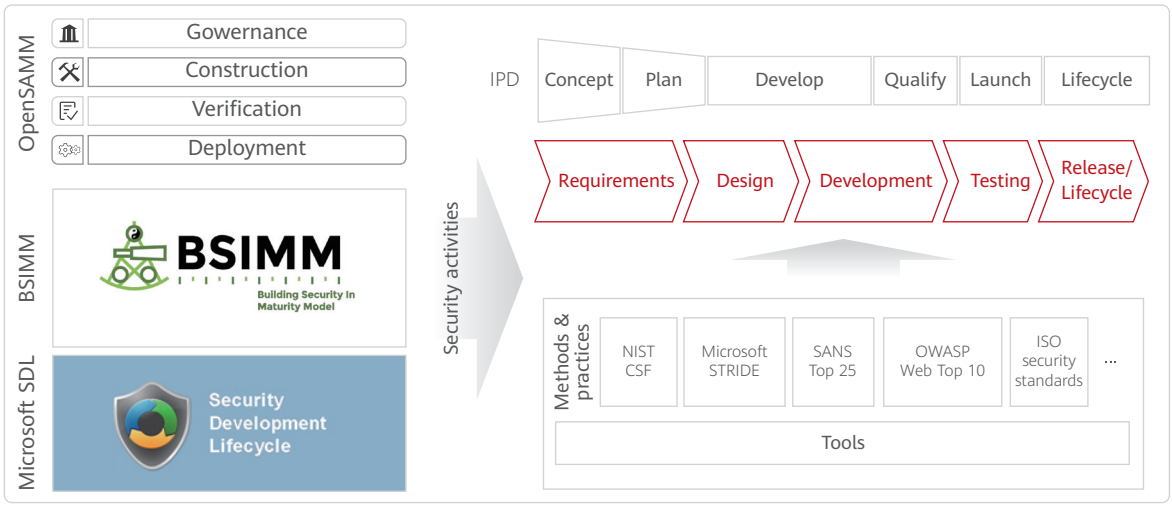


Figure 5: Incorporating cyber security activities into the IPD process

Huawei's R&D has made good progress in the operation of the live network. Huawei has built more than 1500 networks in over 170 countries and regions in the past 30 years, covering more than one third of the world's population, with no cyber security incidents. This shows the security of Huawei products.

Huawei is committed to not only building confidentiality, integrity, availability, traceability and user privacy protection in 5G equipment based on the 3GPP security standards, but also collaborating with operators to build high cyber resilience in networks from the O&M perspective. Looking to the future, as cloud, digitization, and software-defined everything become more and more prevalent and networks become more and more open, Huawei R&D will continuously build secure, trustworthy, and high-quality products and solutions.

5.2 Top-Down Design Principles for 5G Cyber Security

5G cyber security follows the design principles of defense in depth, Zero-trust@5G, and adaptive security, which collaboratively provide a systematic, dynamic, and adaptive security framework. Defense in depth provides multi-layer security measures to protect critical internal assets from external threats. Different security technologies are used at different layers to prevent the compromise of a single point affecting the entire system. Defense in depth prevents system breakdown caused by attacks and unauthorized access. In addition, information is encrypted, so even if it is stolen, no information leakage will occur. Moreover, malicious tampering can be identified so that mitigation measures can be taken accordingly. Zero trust is becoming a trend in cyber security. It assumes that the network is always vulnerable to risks and that no access is trusted before authentication. Therefore, access authentication, dynamic authorization, and continuous assessment are required to implement dynamic access control. Zero trust in the telecom field, that is, Zero-trust@5G, shall be adapted based on the service characteristics of mobile communications networks to improve 5G cyber security. Currently, Zero-trust@5G can focus on two important scenarios: O&M management and UE access. It implements dynamic and precise access control for O&M identity management and 5G UE access, to identify spoofing and prevent unauthorized access. Through the IPDRR methodology, adaptive security enables dynamic, continuous, closed-loop optimization of security measures to adapt to ever-changing security threats, supporting rapid system recovery.

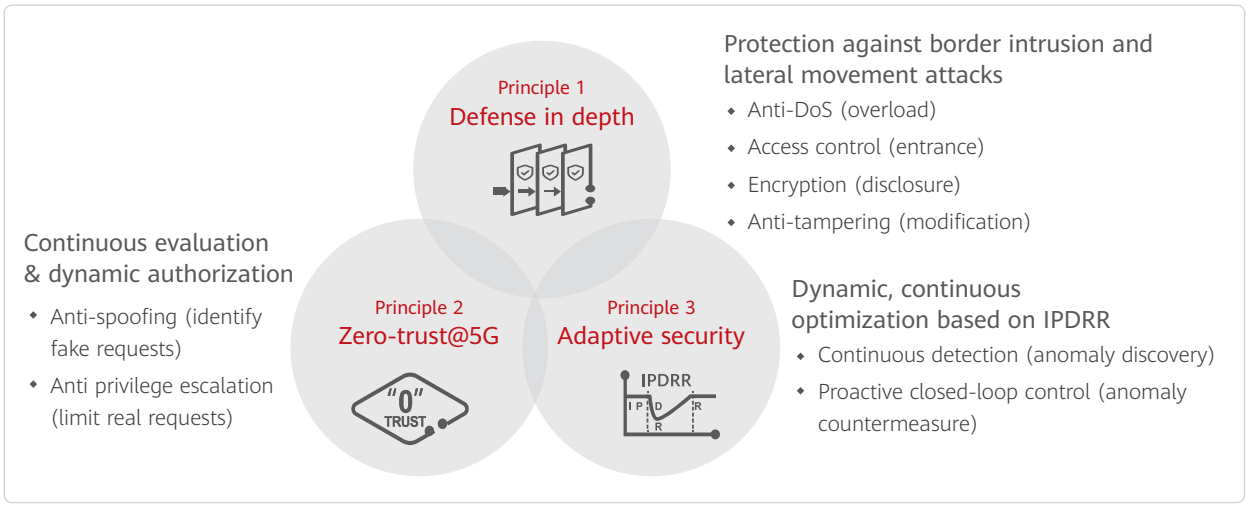


Figure 6: Top-down design principles for 5G cyber security

5.3 Industry-leading Security Measures for the Access Network

5G security standards bring enhancements to air interface and transport security mechanisms used in 4G.

- 5G inherits security protection mechanisms in 4G, and adds data integrity protection for the user plane to **prevent data tampering on the user plane.** In addition, the confidentiality and integrity protection of UE capability reporting information is added in R16 to **prevent UE privacy breaches or denial of service (DoS) attacks caused by UE capability eavesdropping or tampering.**
- In terms of transport security, the N2/N3 interfaces connecting the access and core networks and Xn interfaces connecting base stations use Internet Protocol Security (IPsec) in 4G for transport security. 5G additionally supports Datagram Transport Layer Security (DTLS) over Stream Control Transmission Protocol (SCTP) to secure signaling transmission on the control plane, ensuring transport security between RANs and core networks. Operators can select a transport security protection scheme based on security requirements to **prevent data breach and tampering on the transport network.**
- In terms of privacy protection, 5G security standards include encryption schemes for concealing the SUPI to tackle the risk of user information leakage through messages sent for the initial UE access, thereby **enhancing privacy protection.**

On the basis of 5G security standards for network equipment, Huawei further provides the following air interface and system security hardening measures:

Anti-DDoS

Base stations can identify distributed denial of service (DDoS) attacks launched at them through the air interface from malicious UEs and mitigate the attacks using specific control mechanisms, **ensuring the availability of base stations.**

Rogue Base Station Detection

To prevent rogue base stations from launching spoofing attacks on base stations and UEs over the air interface, base stations provide the rogue base station detection function based on the 5G NSA/SA network architecture, **helping operators identify and locate rogue base stations.**

Hardware Hardening

Hardware ports of base stations are hardened to prevent near-end attacks. Unused ports are disabled by default, and an alarm is generated upon any change in the port status, **reducing the risk of near-end attacks.**

OS Hardening

OSs are hardened to prevent attacks. By default, unnecessary services are disabled on the OSs of base stations. Login from an OS user is prohibited, **preventing attacks.**

Secure Boot

To prevent the system from being tampered with during boot and runtime, base stations support secure boot, detection of code segment tampering during runtime, and alarm reporting, **enhancing system integrity protection.**

Base Station Encryption

To prevent sensitive data, such as keys and passwords, from being stolen or tampered with, base stations store encrypted information in chips, **which cannot be obtained externally.**

5.4 Security Assurance Above Standards for the Core Network

Security Standards

5G core networks enhance the key hierarchy and roaming security mechanisms used in 4G:

- In terms of key hierarchy, the UE access authentication and key derivation framework and NAS signaling encryption and integrity protection for UE access are inherited in 5G. 5G enhances access authentication by defining a unified authentication framework for both 3GPP and non-3GPP access and supporting EAP Authentication and Key Agreement (EAP-AKA) and 5G AKA for **enhanced security flexibility.**
- Roaming networks may access to core networks. To address this risk, the SEPP can be deployed on 5G networks to provide the following security protection functions for signaling messages at the roaming boundaries: topology hiding, message filtering, TLS channels, and application-layer security protection for roaming messages through the Internet Packet Exchange (IPX) networks. This prevents data breach and unauthorized tampering at the transport and application strata, thereby **enhancing transport and data confidentiality and integrity.**
- 5G also provides security requirements and functions for user access authentication on the home operator networks to **address the threat of home network spoofing by roaming networks.**

Cloud Security

Compared with legacy architecture, the cloud architecture introduces universal hardware and runs network functions in a virtual environment, facilitating low-cost network deployment and quick service provisioning. Many core networks have adopted cloud-based deployment around the globe. Huawei has deployed cloud-based core network security solutions for multiple operators.

Huawei complies with security protocols and architectures defined by industry-recognized virtualization standards. The European Telecommunications Standards Institute (ETSI) is responsible for standards formulation for network functions virtualization (NFV) technologies used in the cloud architecture. Huawei adheres to NFV security standards, such as SEC009 (multi-tenant hosting management security) and SEC002 (security feature management of open source software), defined by the ETSI.

Huawei believes that NFV security isolation is an end-to-end solution. From the data center (DC) data interface to the virtual machine (VM) on the core server, NFV security requires a complete security solution that covers both the external and internal layers and everything in between. The NFV security isolation solution includes intra- DC security zone isolation, security isolation of different service domains in a zone, isolation of different host groups in a zone, isolation of VMs in a host, and a series of security hardening measures, implementing outside-in NFV security isolation.

Huawei has mature virtualization security applications in 4G. In terms of 5G network equipment security, Huawei provides the following standards-based security hardening measures:

- To improve the availability of DCs on the operator's network, resource pools can be deployed across DCs for data backup, ensuring service continuity in case of geographical disasters and other scenarios.

- In a DC, zones with different security levels can be designed based on services. Each zone is isolated by a firewall. Users cannot directly access zones with higher security levels. Instead, they can access only through specific servers.
- In a security zone, domains are used to further classify and isolate services. For example, operator network services are generally classified into O&M domain, gateway domain, control domain, and data domain. Different service types are aggregated into different domains. Domains are isolated from each other by firewalls and only authorized access is allowed.
- In a multi-vendor environment, intra-domain host isolation can be performed. In the same host, VM, virtualization layer, and even CPU, storage, and network security isolation is supported.

MEC Security

In the MEC architecture, the computing capabilities of cloud data centers are moved to the edge of the core network. Huawei provides cloud and virtualization security technologies and supports third-party application authentication and authorization management and user data protection to build security for edge networks. The MEC supports security domain division to isolate resources and networks between these domains. MEC security domains must be strictly defined between the UPF and Multi-access Edge Platform (MEP) and between the UPF and applications based on services and deployments. Security isolation for software, resources, systems, and application programming interfaces (APIs) is also supported for third-party applications deployed on the MEC.

For the security of MEC interfaces, Huawei provides the built-in IPsec solution for the N4 interface to protect the confidentiality and integrity of signaling data. The solution provides more comprehensive security protection than an external IPsec gateway. The management interface provides a TLS channel for secure transmission, enabling data security on the management plane. Moreover, the security deployment solution is **provided to comprehensively protect MEC interfaces**. For example, an IPsec gateway can be deployed on the N3/N6/N9 interface for encrypted transmission of user data, and a firewall can be deployed on the MEC to defend against DDoS and other traffic attacks.

Slice Access and Management Security

Network slicing is introduced in 5G networks so that a network can support multiple types of services. In addition to 5G security features, Huawei provides more security measures for slice access and management:

- Slice access security: On the basis of existing user authentication and authorization mechanisms on the 5G network, network slicing allows slice access authentication and authorization for users by operators and vertical industries collaborating together. This ensures authorized user access to slices and control over slice networks and end users by vertical industries.
- Slice management security: Slice-level rights- and domain-based management is provided. Tenants can view only their own slice's KPIs and configurations, preventing unauthorized O&M among multiple slices. The slice management service uses authentication and authorization mechanisms. Security protocols can be used for slice management and between slices to ensure communication integrity, confidentiality, and anti-replay. In the slice lifecycle management, the slice templates and configurations have a check and

verification mechanism to prevent slice access failures caused by incorrect configurations or security risks of data transmission and storage.

5.5 Helping Operators Deploy and Operate Networks with High Resilience

In terms of business operations, it is imperative to follow the security design principles of attack and defense. Specifically, enhanced cyber resilience based on confidentiality, integrity, and availability is critical in the design of cyber security. To speed up service recovery if a security incident occurs, the design must realize continuous monitoring and response to security incidents so that their impact scope and resulting service loss can be minimized. **As an equipment vendor, Huawei implements authoritative industry standards and best practices, and supports operators in building resilient networks, helping them better meet the service requirements for cyber resilience of their critical information infrastructure.**

- The equipment supports secure end-to-end transmission at the network layer to ensure data confidentiality and integrity, and **implements encryption, integrity protection, and anti-replay** on interfaces between UEs, base stations, and core networks.
- Slice isolation is supported, which requires collaboration among wireless, transmission, and core networks for E2E security isolation. Radio bearer (RB) reservation and spectrum isolation are used on the RAN to prevent air interface resource preemption; FlexE is used on the transport network to isolate slices; NFs, VMs, and zones are isolated on the core network. Measures are taken to implement precise and flexible slice isolation, **preventing resource preemption between slices.**
- The management, control, and signaling planes can be isolated to **prevent mutual access and horizontal attacks.**
- The equipment provides the flow control mechanism with load monitoring to prevent DDoS attacks. In cloud-based scenarios, elastic scaling and pool-based disaster recovery are also provided to **enhance cyber resilience.**
- The equipment supports system security monitoring and auditing, as well as **system traceability.**
- The equipment provides security management capabilities. The operations support system (OSS) implements security management for base stations and core networks based on alarms, logs, and configurations. In addition, it interconnects with a third-party service operations center (SOC) through a standard interface to report data, **implementing network-wide security management.** Zero-trust@5G is introduced to network management and control units, allowing evolution from "static authentication and authorization" to "user-identity-based authentication and authorization, continuous trust assessment, and dynamic access control", thereby **building a new security O&M system.**

5.6 Privacy Protection Measures

To comply with applicable privacy protection laws, such as the EU General Data Protection Regulation (GDPR), consider the following privacy protection measures:

- 3GPP 5G standards stipulate that user IDs are encrypted during transmission over the air interface, and encryption and integrity protection are performed on the end-to-end transmission channel to prevent personal data from being stolen or tampered with.
- User plane data protection: Both the air interface and transmission channel support encryption and integrity protection according to 3GPP specifications.
- Huawei 5G products protect personal data during the collection and processing of individuals' user identities for network O&M:

  a. System users can collect personnel data only with authorization, preventing unauthorized operations.

  b. Collected data can be encrypted during storage and processing to prevent data breach. The data can be automatically deleted upon expiry of the personal data storage period.

  c. For boards returned to the manufacturer, a secure deletion mechanism is provided to avoid data breach during repair.

- NEs' personal data descriptions are provided in product documentation to facilitate operators' privacy compliance.

06 Recommendations for Operators' Security Best Practices for 5G

For operators' 5G security, the security and resilience of their networks need to be enhanced, network data and basic user data need to be protected, and network security capabilities need to be open to meet vertical industries' security requirements.

Build and operate secure and resilient networks:

Operators can build secure and resilient networks by establishing a defense in depth system through security planning, design, deployment, and operations and identifying and controlling key risks in live network services through the IPDRR methodology, with the support of suppliers' product security capabilities and in accordance with industry standards and best practices, such as 3GPP specifications, NIST CSF, and GSMA 5G Cybersecurity Knowledge Base.

- Operators build a comprehensive 5G network protection system through security planning, design, and deployment.

Management plane protection:

Operators build an independent management plane network, isolate it from the Internet, perform security zone division, and deploy security protection measures such as firewalls, intrusion detection, and data leakage prevention. The bastion host, multi-factor authentication, and zero trust solutions are used for O&M access control, and all O&M activities are logged and audited.

Signaling plane protection:

To protect the signaling plane between networks, operators use devices such as the SEPP and signaling firewall to screen and monitor incoming and outgoing signaling. To protect intra-network signaling, they plan security zones on the signaling plane, provide inter-domain protection and slice signaling protection, and protect the APIs for network capability openness.

User plane protection:

Operators protect the security of 5G user-plane NFs, such as the MEC and UPF, and provide network-layer encryption and integrity protection to safeguard user data transmission.

Cloud infrastructure protection:

Operators protect the cloud platform, cloud-based virtual resources, virtual networks, and container environments, and leverage cloud capabilities, such as cloud services as well as rapid iteration and evolution, to improve security protection capabilities.

- Operators build the security operations platform and system for efficient and intelligent operations.

Build a security situational awareness and security operations center:

Operators build comprehensive security situational awareness for 5G networks; use cloud, big data, artificial intelligence (AI), and machine learning technologies to improve the automation and intelligence of security operations; and speed up risk discovery, identification, and closed-loop handling to improve the efficiency of security operations.

Build a security operations and O&M management system:

Operators build a comprehensive security O&M management process, involving triggers by service tickets, prior approval, minimum access permissions, operation monitoring, regular risk assessment, and audit by the operator or a third party. They enhance the standardization, automation, and intelligence of the security operations process. They also strengthen the exchange, sharing, and integration of threat intelligence and vulnerability information with external organizations such as industry organizations and suppliers.

Enhance data security protection:

Operators can provide communication channel encryption for users' application-layer data. They should protect network data and basic user data throughout the lifecycle to prevent data breaches. Application providers provide end-to-end encryption for application-layer data. When users' application-layer data, such as online payment/shopping data, is transmitted on operators' networks, network nodes cannot parse the data, and the data is invisible to operators and equipment vendors.

Open network security capabilities:

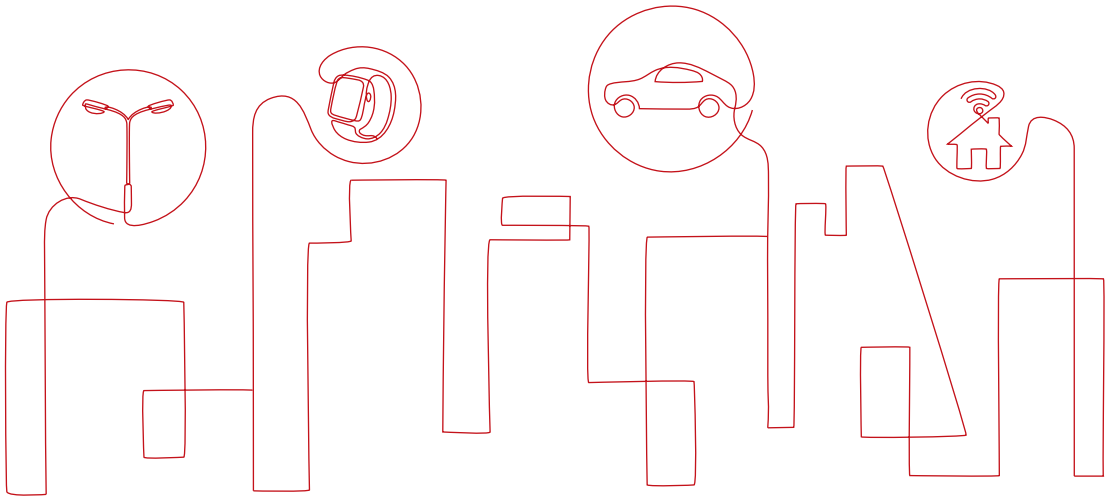
Operators build a network security capability openness platform to open up security capabilities, such as authentication, network encryption, and anti-DDoS, to meet vertical industries' security requirements.

Network security needs to continuously evolve in order to address new potential security risks coming from the open Internet and the development of new services. In-house or third-party security audit, or both, should be encouraged as a best practice for empowering mobile networks (not limited to 5G only). Operators need to be alert and always one step ahead of possible security threats.

About the GSMA 5G Cybersecurity Knowledge Base[4]

The 5G Cybersecurity Knowledge Base is led by the GSMA and a product of collaboration among industry stakeholders including operators, application providers, equipment vendors, and regulators. Based on typical 5G network threats and a series of key security solutions, it proposes baseline security controls to help stakeholders systematically understand and respond to the security threats posed by 5G networks at the technical level. The Knowledge Base mainly includes the following:

1. Threat landscape, mitigation policies and measures for different roles, standards, and best practices that are accepted in the industry. It describes the attack method and impact of each threat and the risk mitigation responsibilities of stakeholders, including application providers, mobile network operators (MNOs), and equipment vendors. It references the best practices of authoritative standards organizations and institutions in the industry, such as 3GPP, ENISA, and NIST.
2. Baseline security controls and a security maturity model for mobile networks. The model can be used to assess the maturity of information security and service control. Operators adopting the controls can compare their internally-deployed security controls with the ones listed by the GSMA to identify and assess potential gaps and address outstanding gaps.



07 Suggestions for Regulators on 5G Security

Security is part of cellular networks definition for 5G. **Compared to previous wireless technologies, 5G standards include more security features to tackle potential security challenges and lead to security enhancements in the future 5G lifecycle.** Governments can be part of these efforts in controlling risks to operate 5G services in line with country regulations. A recommended win-win strategy to address 5G security challenges is to deliver a plan described as follows:

- Formulation of laws and regulations, involving cross-discussion with all public and private partners, to guarantee a consistent security framework. Governments should take a key role here to define the requirements of their respective countries in terms of security, and their **regulators should encourage the development of new technologies with risk control mechanisms to address both their economic objectives and security needs.** This can be achieved through collaboration with all stakeholders, based on a common goal to define global standards. Governments play an important role in encouraging technological innovation (in 5G in the context of this document), allowing more suppliers that meet security specifications to participate in national 5G construction and development, and defining security standards, assurance mechanisms, and certification programs. These measures will improve national 5G network construction and operation efficiency, reduce costs, and stimulate positive social and economic development.

- Governments can implement specific policies to obtain oversight on the security level of each network operating in the country. Specifically, they supervise rogue base stations and radio interference that affect normal 5G communications and impose the necessary penalties for violations. Operators are responsible for the cyber security of the network infrastructure and manage risks in accordance with international standards and national security regulations. **Regulatory requirements for operators shall be transparent, fair, and consistent, and unified cyber security requirements shall be applied to all suppliers, to ensure security throughout the network.**

- **NESAS jointly defined by GSMA and 3GPP provides authoritative, unified, and open security assessment standards for the communications industry, helping governments, regulators, and operators monitor and manage local cyber security risks more efficiently.**

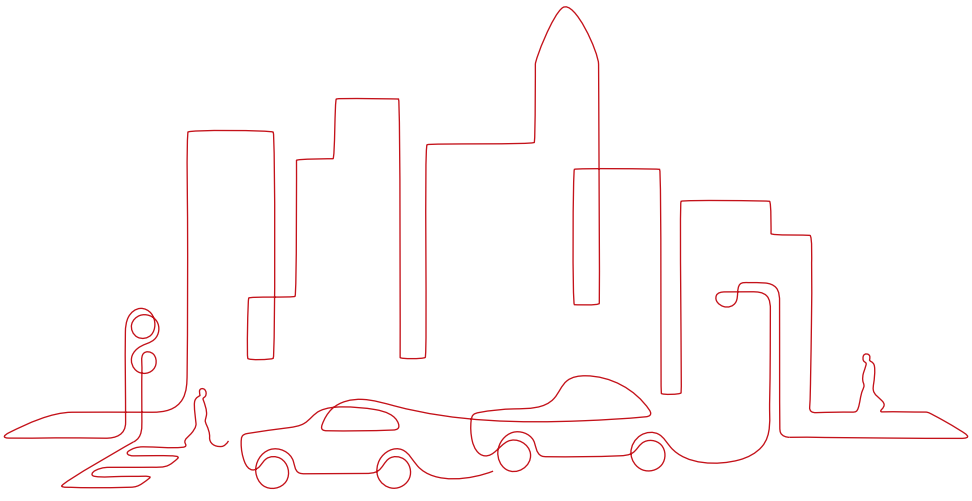
More and more governments and regulators are working closely with relevant industries and partners to develop a unified set of rules for 5G security. Operators can implement 5G security policies and mechanisms based on these rules. The support from equipment vendors and relevant vertical industries is also important.

08 Build Security Through Collaboration to Tackle Future Security Challenges

5G is becoming a reality and the lifecycle for 5G is going to be lasting for a while. Based on successful experience for 4G security, controlling 5G security risks is achieved through joint efforts of all industries. To control risks in the 5G lifecycle, we need to continuously enhance security solution capabilities through technological innovation and build secure systems and networks through standards and ecosystem cooperation.

- Equipment vendors: They integrate security technologies and manufacture secure products in compliance with standards and industry best practices, participate in the development of industry security standards, and work with customers and other stakeholders to help operators ensure security operations and cyber resilience.
- Operators: They are responsible for the networks' security operations and cyber resilience. Through security planning, design, and deployment, they build a comprehensive 5G network protection system with defense in depth. Operators can prevent external attacks with firewalls and security gateways. For internal threats, operators can manage, monitor, and audit all vendors and partners to verify security within and between their NEs.
- Industry and government regulators: As an industry, we all need to work together on unified standards. In terms of technologies, we need to continuously contextualize 5G security risks and enhance protocol-based security. In terms of security assurance, we need to standardize cyber security requirements and ensure that these standards are applicable to and verifiable for all vendors and operators.

Huawei calls on the industry to work together to share responsibilities, unify standards, formulate clear regulatory measures, and build a secure, reliable, open, and transparent 5G security ecosystem that benefits everyone and is widely recognized by stakeholders.



Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
3GPP	Third Generation Partnership Project
AI	artificial intelligence
API	application programming interface
AR	augmented reality
ASC	application security control
ASTRIDE	Advanced STRIDE
ASVS	Application Security Verification Standard
BSIMM	Building Security In Maturity Model
CERT	Computer Emergency Response Team
CIoT	Cellular Internet of Things
CWE	Common Weakness Enumeration
DC	data center
DDoS	distributed denial of service
DoS	denial of service
DTLS	Datagram Transport Layer Security
E2E	end to end
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Authentication and Key Agreement
eMBB	enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications Association
GSPO	Global Cyber Security & Privacy Officer
HCS	Harmonized Communication and Sensing
ICSL	Independent Cyber Security Lab
IMSI	international mobile subscriber identity
IoE	Internet of Everything
IoT	Internet of Things
IoV	Internet of Vehicles
IPD	Integrated Product Development
IPDRR	Identify, Protect, Detect, Respond and Recover
IPsec	Internet Protocol Security
IPX	Internet Packet Exchange
MEC	Mobile Edge Computing

Acronym and Abbreviation	Full Name
MEP	Multi-access Edge Platform
mMTC	Massive Machine-Type Communications
MNO	mobile network operator
NSA	Non-Standalone
NESAS	Network Equipment Security Assurance Scheme
NF	network function
NFV	network functions virtualization
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
OAuth	Open Authorization
ONF	organization normative framework
OpenSAMM	Open Software Assurance Maturity Model
OSS	operations support system
OWASP	Open Web Application Security Project
PIA	privacy impact assessment
PNI-NPN	public network integrated non-public network
PSIRT	Product Security Incident Response Team
RB	radio bearer
RTBC	Real-Time Broadband Communication
SA	Standalone
SANS	SysAdmin, Audit, Network, Security
SBA	Service Based Architecture
SCAS	Security Assurance Specifications
SCTP	Stream Control Transmission Protocol
SDL	Security Development Lifecycle
SEPP	Security Edge Protection Proxy
SOC	service operations center
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
UCBC	Uplink Centric Broadband Communication
UE	user equipment
UPF	User Plane Function
URLLC	Ultra-Reliable and Low-Latency Communications
VM	virtual machine
VR	virtual reality

References

[1] 3GPP TR 33.899: "Study on the security aspects of the next generation system"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045

[2] 3GPP meetings for group S3

https://www.3gpp.org/dynareport/Meetings-S3.htm?Itemid=451

[3] GSMA Network Equipment Security Assurance Scheme (NESAS)

https://www.gsma.com/security/network-equipment-security-assurance-scheme/

[4] GSMA 5G Cybersecurity Knowledge Base

https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

[5] 3GPP TS 33.501: "Security architecture and procedures for 5G System"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[6] 3GPP 5G Security

http://www.3gpp.org/news-events/3gpp-news/1975-sec_5g?from=timeline

[7] 3GPP TR 33.875: "Study on enhanced security aspects of the 5G Service Based Architecture (eSBA)"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3845

[8] 3GPP TR 33.853: "Study on key issues and potential solutions for integrity protection of the User Plane (UP)"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3571

[9] 3GPP TR 33.861: "Study on evolution of Cellular Internet of Things (CIoT) security for the 5G System"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3480

[10] 3GPP TR 33.825: "Study on the security of Ultra-Reliable Low-Latency Communication (URLLC) for the 5G System (5GS)"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3548

[11] 3GPP TR 33.813: "Study on security aspects of network slicing enhancement"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3541

[12] 3GPP TR 33.857: "Study on enhanced security support for Non-Public Networks (NPN)"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3764

[13] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)"

https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3690