ISSN 2616-5775 Vol. 8, Issue 11: 99-106, DOI: 10.25236/AJCIS.2025.081111

Research on the Progress and Trends of Mobile Communication Network Equipment Security Standardization

Dan Lu[1,a,*], Zelong Ma[1,b], Yizhou He[1,c]

[1]*Security Research Department, China Academy of Information and Communications Technology, Beijing, China*
[a] *ludan@caict.ac.cn,* [b] *mazelong@caict.ac.cn,* [c] *heyizhou@caict.ac.cn*
**Corresponding author*

Abstract: *In October 2025, the Security Working Group (SA3) of the 3rd Generation Partnership Project (3GPP) officially initiated the study on security use cases and requirements for 6G within Release 20 (R20). Against this backdrop, this paper begins by systematically reviewing the experience gained in building device security capabilities during the 5G era. It then provides an in-depth analysis of the new device security risks emerging from the evolution towards 6G networks, which stem from challenges such as massive heterogeneous terminals, the authentication of new network elements, and cross-domain trust mechanisms. Furthermore, the paper proposes a development framework and specific countermeasures for the 6G device security standards system. These proposals encompass the construction of an endogenous security baseline, the classification and grading of terminal security, and the design of cross-domain mutual trust mechanisms. The insights presented aim to provide valuable references for establishing a globally unified security assurance system for mobile communication equipment.*

Keywords: *6G security, 5G security, equipment security, standardization*

1. Introduction

The global mobile communications industry is currently at a critical stage of generational transition. In October 2025, the 3GPP SA3 124th meeting was held in Wuhan, officially launching the 6G security research for Release 20, with all related work for this release scheduled for completion by May 2027[1]. At this pivotal juncture, proactively advancing research on 6G device security is particularly crucial.

Mobile communication network equipment security serves as the cornerstone for ensuring the secure and reliable operation of the entire communication system. In recent years, the deep integration of 5G networks with vertical industries has increasingly highlighted the importance of equipment security standardization. The Network Equipment Security Assurance Scheme (NESAS)[2], jointly launched by the Global System for Mobile Communications Association (GSMA) and 3GPP in 2019, established a globally recognized equipment security evaluation framework. However, with the accelerated advancement of 6G research and development, security challenges posed by massive heterogeneous terminals and novel network elements present entirely new requirements for existing standardization systems.

This paper focuses on the progress and trends of mobile communication network equipment security standardization, aiming to provide references for the initial phase of 6G standardization. Compared with existing research, the innovations of this paper are mainly reflected in proposing recommendations for the critical window period of equipment security standardization based on the launch of 3GPP Release 20.

2. International Progress And Implementation Of 5G Equipment Security Standardization

2.1. Global Equipment Security Standard Framework Construction

NESAS has been established as the globally recognized security assessment framework for 5G equipment. As illustrated in Figure 1, the system comprises two complementary components: the product lifecycle process evaluation framework developed by GSMA, and the Security Assurance Specifications

ISSN 2616-5775 Vol. 8, Issue 11: 99-106, DOI: 10.25236/AJCIS.2025.081111

(SCAS) formulated by 3GPP. The GSMA framework establishes a comprehensive lifecycle audit mechanism spanning R&D, production, and operations through its FS.13 specification document and supporting FS.14-FS.16 series. Concurrently, 3GPP provides standardized security assurance specifications for 17 categories of 5G network elements (including base stations, core network components, and Release 19 additions such as SMSF) via the TS 33.117 standard series[2].

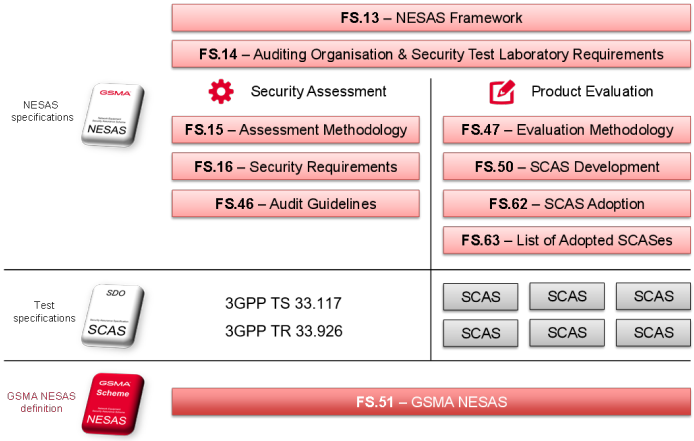

Figure 1: NESAS documentation architecture (Source: GSMA PRD FS.13 v3.0, 2025)

Since its introduction, NESAS has been continuously improved and rapidly developed:

In terms of standard development, GSMA has consistently updated and refined the NESAS management specifications, releasing NESAS 3.0 in February 2025 with a more formal standard system, clearer role responsibilities, more defined testing laboratory qualifications, and improved management norms. Currently, GSMA is actively advancing the internationalization and standardization of its framework: On one hand, it is aligning the NESAS specifications with ETSI document drafting rules through editorial revisions, promoting their transformation into draft European standards, and ultimately establishing them as ETSI technical standards. On the other hand, it has implemented a dynamic maintenance mechanism to ensure the standards evolve alongside industry developments. Simultaneously, to build a globally unified certification ecosystem, GSMA has adopted multi-dimensional initiatives: encouraging countries to develop localized certification schemes based on the NESAS framework, supporting more testing laboratories in obtaining ISO 17025 accreditation and joining the evaluation system, and continuously integrating advanced security specifications from organizations like ETSI and O-RAN. These efforts aim to create a complete closed loop from international consensus to practical implementation of NESAS standards, providing systematic safeguards for the security of 5G and even future 6G equipment.

3GPP has actively promoted SCAS standard research and development, completing the SCAS standards for Release 19 by the end of 2024, which added security assurance specifications for network elements such as SMSF (Short Message Service Function). In June 2025, the 3GPP Security Working Group (SA3) successfully approved the SCAS standard project for Release 20, focusing on the following three key directions:

1) Foundational Security Enhancements: Research on general security requirements such as protocol robustness improvement, virtualization security, and containerization security, aiming to update and refine relevant SCAS standards for universal security .

2) 5G-Advanced Architecture and Features: Addressing new architectures and capabilities like network intelligence, public-private network interworking, and integrated sensing-communication, the project will advance security enhancement studies for network functions (e.g., NWDAF, AANF, SMSF, UDR) and update corresponding SCAS technical specifications .

3) Threat Analysis for New Network Functions: Conduct in-depth security threat analysis for newly added 5G-Advanced functionalities, developing associated requirements and testing methodologies to ensure comprehensive coverage of network security assurance needs .

2.2. Standard Implementation Effectiveness

NESAS has gained widespread global acceptance and support by establishing a security benchmark

ISSN 2616-5775 Vol. 8, Issue 11: 99-106, DOI: 10.25236/AJCIS.2025.081111

framework recognized across the industry.

In industrial implementation, global leading communication equipment manufacturers including Huawei, Ericsson, and Nokia, as well as renowned companies like Microsoft, Oracle, and Samsung, have joined the NESAS program. Meanwhile, multiple institutions from China, the UK, Singapore, and other countries have become NESAS audit organizations or testing laboratories. Currently, GSMA is actively promoting mutual recognition of test results among different laboratories.

Regarding regulatory adoption, countries have developed localized security technical specifications covering core networks and base stations based on the 3GPP SCAS and GSMA NESAS international standards, tailored to local network requirements. Regional certification schemes such as "NESAS-German Implementation" (NESAS CCS-GI) exemplify such practices. According to publicly available policy documents, as of November 2025, nearly 30 countries or regions (e.g., Germany, Spain) have explicitly recognized NESAS/SCAS standards through government regulatory bodies, with approximately half incorporating them into legislation as mandatory security testing criteria for 5G equipment.

While 5G security frameworks have achieved maturity through these global implementations, 6G's ICDT (Integrated Communication, Detection, and Computing Technologies) capabilities and space-terrestrial coverage introduce new security dimensions: 6G features deep integration of communication, sensing, computing, and intelligence, as well as global coverage integrating space and terrestrial networks.

2.3. 5G Device Security Evaluation Practices

2.3.1. Evaluation System Architecture Design

To comprehensively assess the security performance of 5G network equipment, this study established a complete evaluation system encompassing four dimensions: test environment setup, test case design, test toolchain configuration, and evaluation execution with result analysis. This system, based on the 3GPP TS 33.501 security architecture specification and combined with the actual deployment situation of 5G networks in China, forms a device security evaluation methodology with Chinese characteristics.

The test environment adopts an end-to-end architectural design, built within the China Academy of Information and Communications Technology (CAICT) 5G security laboratory. Participating vendors, according to unified requirements, separately constructed complete 5G network test environments including terminals, base stations, core networks, and applications. Security testing tools mainly include two categories: first, general security detection tools, comprising open-source software (e.g., port scanning tools, data packet capture/injection tools) and commercial tools (e.g., vulnerability scanners, fuzz testing tools, simulated attack tools); second, 5G protocol-specific testing tools, including programmable 5G terminals, 5G signaling traffic simulators, 5G authentication protocol analyzers, 5G encryption/decryption conformance analyzers, etc. These tools are integrated into the test environment for systematic security testing of base station and core network equipment.

2.3.2. Test Case System Construction

This study designed a comprehensive test case system covering 137 test items. As shown in Table 1, the test cases are divided into four levels: General Security Tests (78 items), Base Station (gNB) Security Tests (21 items), Core Network Security Tests (38 items), and Newly Added Characteristic Test Items (9 items). The first three categories are based on the 3GPP SCAS series standards (TS 33.511 to TS 33.522), with mandatory items accounting for over 85%, ensuring the comprehensiveness and authority of the evaluation. Simultaneously, by investigating the actual needs of China's 5G networks, the research team added 9 characteristic test items, including DTLS protection testing, service-based network element (SBA-NE) authentication testing, and user plane data integrity protection testing. These added items primarily address the following security threats: first, when 5G networks use the UDP protocol for data transmission, DTLS protection can effectively prevent UDP data eavesdropping and tampering; second, as the 5G core network adopts a Service-Based Architecture (SBA) where network elements communicate via service-based interfaces, the SBA-NE authentication test can prevent network element impersonation attacks; third, the user plane data integrity protection test can verify whether data has been tampered with during transmission, preventing data integrity destruction attacks.

ISSN 2616-5775 Vol. 8, Issue 11: 99-106, DOI: 10.25236/AJCIS.2025.081111

Table 1: Test Scope of This Study

Test Category	Coverage Scope
General Security	Primarily covers general security requirements for Service-Based Architecture (SBA), such as data and information protection, availability and integrity protection, OS and web service security, vulnerabilities, robustness/fuzziness, software package security, and other fundamental requirements.
Base Station (gNB) Security	Comprehensively covers security functions of gNB equipment, including confidentiality/integrity/anti-replay protection for air interface RRC and user plane data, algorithm negotiation and selection, handover security, key update, interface protection, and device physical security.
Core Network Security	Comprehensively covers security functions of various Core Network Functions (NFs), including specific security features of NFs like AMF, UDM, SMF, PCF, SCP, NWDAF, N3IWF, SEPP, as well as security requirements in virtualized environments.
Newly Added Characteristic Test Items	DTLS Protection, Service-Based Network Element Authentication, User Plane Data Integrity Protection, etc.

2.3.3. Evaluation Execution Process

The evaluation execution adopted a phased, multi-round testing strategy to ensure comprehensive coverage of security requirements across different standard versions. The testing covered 5G network equipment from mainstream vendors including Huawei, ZTE, Datang, Ericsson, and Shanghai Nokia Bell.

Four core testing methodologies were employed during the process:

1) Scanning Tests: Using techniques like port scanning, vulnerability scanning, and source code scanning to identify insecure services/ports and known vulnerabilities. Professional vulnerability scanning tools were used for comprehensive scans of operating systems, applications, and security mechanisms.

2) Simulated Attack Tests: Constructing attack packets to detect device defense capabilities. Test scenarios included DoS attacks, null cipher algorithm attacks, and man-in-the-middle (MitM) attacks. By simulating real attack scenarios, the device's defensive capabilities under actual threats were validated.

3) Fuzz Testing: Automatically generating malicious/random data to probe for unknown security issues. A fuzz testing framework was used, cumulatively generating a large number of test cases to discover unknown vulnerabilities.

4) Protocol Analysis Tests: Capturing and analyzing interface packets to verify protocol function conformance. Protocol analysis tools were used for in-depth analysis of air interface signaling and core network signaling, ensuring protocol implementation complied with 3GPP standards.

2.3.4. Analysis of Evaluation Results

After testing, we found that the participating devices performed excellently overall in the implementation of security functions, with generally high pass rates, comprehensively covering the 3GPP SCAS standard requirements. Specifically: in General Security Tests, participating devices achieved full scores in core security functions like data encryption, identity authentication, and access control; in Base Station Security Tests, key indicators such as air interface signaling encryption, air interface data transmission protection, and network handover security all met expected requirements; in Core Network Security Tests, functions like service-based architecture security, signaling encryption, and user plane data protection were fully implemented. However, the evaluation also revealed that some devices still had shortcomings in enhanced security functions such as DTLS protection and user plane data integrity protection, with related mechanisms not yet perfected. This indicates that while various vendors already possess good capabilities in meeting the basic security requirements of the 3GPP SCAS standards, there is still uneven progress in implementation and incomplete functional coverage regarding additional security features required for high-security-demand scenarios. In the future, it is necessary to further promote the research, development, and deployment of these enhanced security functions to improve the overall security level of devices in complex application scenarios.

ISSN 2616-5775 Vol. 8, Issue 11: 99-106, DOI: 10.25236/AJCIS.2025.081111

3. Equipment Security Challenges And Capability Requirements In The 6G Era

Compared with 5G, 6G will undergo significant adjustments in network architecture and application scenarios, bringing entirely new security challenges and upgraded capability requirements[3].

3.1. Elevated Security Requirements Due to 6G's Native Security Architecture

6G networks will deeply integrate security functions with network functions, requiring devices to possess native security protection capabilities at the hardware level[4]. Traditional add-on security solutions suffer from high latency and excessive resource consumption, making them unsuitable for 6G's millisecond-level real-time protection demands. Particularly for edge computing nodes and integrated communication-sensing devices, hardware-level trusted execution environments (TEE) and secure boot mechanisms must be implemented to ensure full-stack trust from chip to system[5].

This architectural shift imposes three major new requirements on device security:

1) Dynamic security policy loading and runtime verification to enable elastic scaling of security capabilities.

2) Cross-layer security coordination to facilitate real-time interaction with network-side security orchestration systems.

3) Built-in AI security acceleration engines to support localized execution of lightweight threat detection algorithms.

These requirements will significantly increase design complexity and security verification challenges for devices.

3.2. The "Low-Computation, High-Threat" Dilemma for Massive Heterogeneous 6G Terminals

6G networks will connect tens of billions of heterogeneous devices, including satellite-based terminals, micro-sensors, and AR/VR devices, which vary greatly in computing power, energy supply, and security needs. Due to limited computing and storage resources (e.g., in satellite-based devices), some terminals cannot support traditional encryption algorithms and authentication mechanisms.

Besides, the open deployment environment of 6G terminals vastly expands the attack surface. Emerging radio-frequency devices such as reconfigurable intelligent surfaces (RIS) and terahertz transceivers may become entry points for physical-layer attacks. Poorly protected digital twin terminals could serve as gateways for network infiltration.

Additionally, the heterogeneity of 6G terminals complicates the establishment of unified security baselines. Consumer-grade and industrial-grade terminals have vastly different security requirements, yet current standardization frameworks lack effective classification mechanisms, making terminals vulnerable weak points in network defenses.

3.3. Lack of Cross-Domain Trust Mechanisms in 6G's Distributed Architecture

6G's space-air-ground integrated networks will deeply interconnect devices from different administrative domains, such as satellite communications, terrestrial base stations, and maritime nodes, breaking traditional network trust boundaries. Currently, certificate systems across domains are incompatible, and there is no unified identity management framework among satellite operators, terrestrial service providers, and other stakeholders. In communication-sensing data exchange scenarios, temporary trust relationships between devices lack verifiable traceability mechanisms, leaving them vulnerable to man-in-the-middle attacks.

Public-private network hybrid scenarios further complicate trust management. Industrial control devices must interact with both operator networks and local private networks, yet existing security protocols lack dynamic cross-domain access control mechanisms. Insufficient isolation between network slices may lead to critical services being compromised, necessitating fine-grained device resource access control policies and cross-slice security auditing mechanisms.

ISSN 2616-5775 Vol. 8, Issue 11: 99-106, DOI: 10.25236/AJCIS.2025.081111

3.4. Security Testing and Certification System for 6G Network Element Equipment Needs Continuous Evolution

While the current NESAS-based security testing and certification framework covers 17 types of network elements (e.g., base stations and core network components), future 6G network elements—such as satellite communication gateways and non-terrestrial network (NTN) base stations—are not yet included. For example, satellite gateways require specialized security evaluation standards due to their unique inter-satellite link protocols.

Furthermore, security testing technologies must evolve. Emerging techniques such as digital twins and AI-based offensive/defensive testing lack standardized evaluation frameworks. Additionally, the threat posed by quantum computing to cryptographic algorithms demands that certification systems dynamically adapt to new security requirements.

4. Latest Progress And Trend Analysis In International Standardization

4.1. 3GPP Standardization Developments

Building upon the foundational framework established by ITU-T Y.3601[6] for 6G security standardization, the 3GPP Security Working Group (SA3) officially initiated Release 20 work items in May 2025, involving final improvements to 5G security standards and research on 6G security use cases and requirements:

Regarding 5G equipment security, 3GPP successfully established Release 20 SCAS standard work items, focusing on three main directions: First, conducting research on basic general security enhancement requirements such as protocol robustness enhancement, virtualization security, and containerization security, promoting updates and improvements to relevant SCAS general security standards. Second, promoting research on security enhancement requirements for new 5G-Advanced architectures and features including network intelligence, public-private network interconnection, and communication-sensing integration, driving updates to technical specifications for network elements like NWDAF, AANF, SMSF, and UDR. Third, conducting in-depth security threat analysis for newly added 5G-Advanced network functions and developing relevant requirements and supporting testing methods to ensure comprehensive coverage of network security assurance needs.

For 6G equipment security, Release 20 proposals focus on dynamic identity management, AI-driven anomaly detection, enhanced underlying (L1/L2) protection, efficient encryption algorithms (such as AEAD), and decentralized trust mechanisms. The overall trend shows a shift from passive defense to active, full-stack, lightweight security architectures to proactively address new 6G security risks and diverse service scenarios requirements.

4.2. GSMA Standardization Developments

After releasing NESAS 3.0, GSMA is actively promoting the internationalization and standardization of the standard system: On one hand, through editorial revisions to make NESAS specifications comply with ETSI document drafting rules, promoting their conversion into European standard drafts, and ultimately forming ETSI technical standards. On the other hand, establishing dynamic maintenance mechanisms to ensure synchronization between standards and industry development.

To build a globally unified certification ecosystem, GSMA has adopted multidimensional measures: encouraging countries to develop localized certification schemes based on the NESAS framework, supporting more testing laboratories to obtain ISO 17025 certification and join the evaluation system, while continuously incorporating advanced security specifications developed by organizations like ETSI and O-RAN. This series of actions aims to achieve a complete closed loop from international consensus to implementation for NESAS standards, providing systematic assurance for 5G/6G equipment security.

5. Considerations For Building 6G Network Equipment Security Capabilities

At this critical window period when 5G security standards are becoming mature and 6G security research is about to fully commence, it is imperative to seize the strategic opportunity of generational transition, initiate forward-looking planning for 6G equipment security standards, and conduct pre-research on new requirements such as native security and cross-domain mutual trust. Standardization

ISSN 2616-5775 Vol. 8, Issue 11: 99-106, DOI: 10.25236/AJCIS.2025.081111

work during this transition period will lay a solid foundation for 6G equipment security.

5.1. Constructing a Native Security Standard System for 6G Equipment

It is recommended to commence equipment native security architecture design during the initial phase of 6G standardization, focusing on advancing the following work: First, develop overall technical requirements for 6G equipment native security, clarifying security function modules and protection mechanisms that need to be built into network element equipment. Second, establish equipment security baseline standards covering hardware, protocols, data and other aspects, such as technical requirements for hardware security modules and specifications for user plane security protocols. Third, develop supporting testing and evaluation standards, constructing a multi-level evaluation system from simulation verification to live network testing. By prioritizing standards, we can ensure that 6G equipment possesses native security protection capabilities at the design stage.

5.2. Establishing a Graded and Classified Equipment Security Standard Framework

To address the diversification characteristics of 6G terminal equipment, we recommend: First, develop graded and classified security standards for 6G terminal equipment, establishing differentiated indicator systems based on equipment types (core/edge/terminal) and application scenarios (industrial/vehicle networking/consumer-grade). Second, formulate security technical requirements for various types of equipment, focusing on core indicators such as anti-attack capabilities, encryption algorithms, and firmware security. Finally, promote the formation of a 6G terminal security evaluation and certification mechanism covering hardware, protocols, applications and other aspects in accordance with the standards, ensuring terminal security in open environments.

5.3. Developing Cross-Domain Equipment Mutual Trust Standards

For 6G space-terrestrial integrated scenarios, we recommend focusing on: Researching blockchain-based distributed equipment authentication standards, formulating technical specifications for lightweight identity identification and certificate management; developing equipment authentication protocol standards supporting post-quantum cryptographic algorithms to ensure future-oriented security protection capabilities; creating cross-domain security information interaction standards to achieve secure interoperability between equipment in different network domains. Through standard innovation, we can build a trusted interconnection system for equipment adapted to 6G network characteristics.

5.4. Promoting the Improvement of a Globally Unified Mobile Network Equipment Security Standard System

Actively participate in equipment security technology research and standard development within international standardization organizations such as GSMA and 3GPP, promote the formation of a 6G security testing and evaluation system with international consensus, and simultaneously update domestic equipment security standards and specifications. Promote international mutual recognition of evaluation results based on unified technical standards, building a global foundation for 6G security mutual trust.

6. Conclusion And Outlook

The standardization of 6G equipment security is at a critical juncture that builds upon past achievements and paves the way for future progress. A systematic solution must be developed across three dimensions:

At the technical architecture level, efforts should focus on the 3GPP Release 20 framework, prioritizing breakthroughs in core technologies such as native security architectures, lightweight authentication protocols, and heterogeneous terminal management. For instance, end-to-end security protection can be achieved through hardware-level TEE.

At the standards framework level, a comprehensive set of standards must be established, covering security baselines for equipment, tiered classification requirements, and cross-domain mutual recognition mechanisms. Particular emphasis should be placed on refining security assessment specifications for emerging network elements, such as satellite communication gateways.

At the industrial ecosystem level, global harmonization of security certification systems should be

ISSN 2616-5775 Vol. 8, Issue 11: 99-106, DOI: 10.25236/AJCIS.2025.081111

promoted through international organizations like GSMA and 3GPP. This includes fostering mutual recognition of testing capabilities and encouraging collaborative innovation among industry, academia, and research institutions, thereby laying a solid foundation for the secure and reliable deployment of 6G networks.

References

[1] P. Jain, "Rel-20 planning and progress in TSG SA," 3GPP Highlights, no. 9, Dec. 2024. [Online]. Available: https://www.3gpp.org
[2] GSMA, Network Equipment Security Assurance Scheme (NESAS), GSMA FS.13, Feb. 2025. [Online]. Available: https://www.gsma.com/nesas
[3] L. Dan et al., "6G security requirements and key technologies discussion," Information and Communications Technology and Policy, vol. 51, no. 1, pp. 52-55, Jan. 2025. DOI: 10.12267/j.issn.2096-5931.2025.01.008
[4] X. Ji, J. Wu, L. Jin et al., "Discussion on a New Paradigm of Endogenous Security Towards 6G Networks," Frontiers of Information Technology & Electronic Engineering, 2022. DOI: https://doi.org/10.1631/FITEE.2200060.
[5] W. Zijun, Z. Haijun, M. Xu, and R. Yuzheng, "System architecture and key technologies of 6G integrated sensing, communication, and computing," J. Univ. Sci. Technol. Beijing, vol. 48, no. 3, pp. 26-39, 2024, doi: 10.3969/j.issn.1006-1010.20240125-0004.
[6] ITU-T Y.3601, "Framework for 6G Security Standardization," Jan. 2025.