Private 5G Security Assessment Framework: Development and Validation from Testbed to Operational Network *

Jieon Oh, Yeongjae Kim, Bonam Kim, and Ilsun You†

Kookmin University, Seoul, Republic of Korea
[jieon1006, zeroash, kimbona, isyou]@kookmin.ac.kr

Abstract

Private 5G(5th generation mobile network) are increasingly deployed across industries such as manufacturing, logistics, and public safety. However, their diverse configurations and security settings make it difficult to evaluate 5G-specific security assurance using conventional IT certification schemes. This study proposes a security assessment framework for private 5G networks, extending the 3rd Generation Partnership Project (3GPP) Security Assurance Specification (SCAS) by integrating 3GPP standards, recent research, and field security issues. The framework defines 72 assessment items addressing design, implementation, and operational security aspects. Its feasibility was validated through a testbed built with Open5GS and UERANSIM, and later applied to an R&D private 5G network. Results demonstrate that the framework can systematically and reproducibly evaluate the security of private 5G environments, offering practical guidance for both operators and evaluators in achieving reliable 5G security assurance.

Keywords: Private 5G, Private 5G Security Assesement Framework, Testbed Validation, Application to a Commercial Private 5G Network

1 Introduction

Private 5G networks are rapidly expanding across various industries including smart factories, energy, logistics, and public safety[1]. Unlike public networks operated by mobile network operators, private networks are deployed and managed by individual enterprises or institutions[2], resulting in varying configurations and security settings[3]. This diversity necessitates a dedicated security assessment framework.

To address network equipment security, 3rd Generation Partnership Project (3GPP) and GSM Association (GSMA) established the Network Equipment Security Assurance Scheme (NESAS), with the Security Assurance Specification (SCAS) defining security requirements and test procedures for 5G network functions[4]. However, SCAS focuses primarily on manufacturer-centric test environments and does not fully reflect the operational diversity of actual private networks.

This study proposes a private 5G security assessment framework extending SCAS by integrating 3GPP standards, recent security research, and field security issues. The framework defines 72 assessment items covering design flaws, implementation defects, and operational misconfigurations.

The framework's effectiveness was validated through a testbed based on Open5GS and UERANSIM, and subsequently applied to an R&D private 5G network. Results demonstrate that the proposed framework is applicable to both testbed and operational environments as a practical security verification system.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 54, December 16-18, 2025, Sapporo , Japan.

†Corresponding author

Section 2 analyzes the limitations of existing IT security certification and evaluation schemes, and derives the needs and requirements for a security assessment framework tailored to private 5G networks. Section 3 presents the proposed SCAS-based security assessment framework, describing the derivation and classification of 72 assessment items. Section 4 details the implementation and validation process of the framework using a testbed built with Open5GS[5] and UERANSIM[6]. Section 5 applies the proposed framework to a commercial private 5G network to evaluate its effectiveness and applicability in real operational environments. Finally, Section 6 concludes the study by summarizing the results and discussing future research directions.

2 Gaps and Requirements

2.1 Gaps in 5G Security under Existing Frameworks

The information security evaluation and certification systems are designed to enhance security by assessing the security level of an organization or product. Major systems include Common Criteria (CC), ISO/IEC 27001, and ISMS-P. CC certification evaluates whether an IT product's security meets ISO/IEC 15408 [7]. ISO/IEC 27001 [8] ensures that an organization establishes, operates, and continuously improves its information security management system. ISMS-P verifies that measures for information protection and personal data protection comply with established standards [9]. However, these systems were designed for general IT environments and fail to fully capture the structural and operational characteristics of 5G networks.

A 5G network consists of User Equipment (UE), next-generation Node B (gNB), and the 5G core network (5GC), which includes several network functions (NFs). These functions are interconnected through various interfaces. As user devices move between cells, they frequently establish new connections with different base stations, and during roaming, network authentication and session processes are repeatedly renewed. Throughout these processes, new security vulnerabilities can arise across the wireless and mobility domains. However, existing certification systems do not include procedures to verify interface-level communication security or inter-NF communication security. In the case of private 5G networks, the integration with public 5G networks, the complexity of multiple management domains, and the adoption of new technologies introduce various security challenges[10].

Consequently, existing general-purpose certification schemes are insufficient to assess the complex architecture and operational environments of private 5G networks. Therefore, a new security assessment framework is required—one that reflects operational environments and enables interface-level verification of network behavior.

2.2 Requirements for Private 5G Security Assessment Framework

Security assessment for private 5G networks should go beyond simple configuration checks. It must verify that the network can effectively detect, prevent, and respond to potential security threats. To achieve this, a practical and comprehensive assessment framework should meet the following requirements:

(1) Coverage of Private 5G Components The assessment should include all key components of the private 5G architecture— gNodeB (gNB), and 5GC. Each component performs distinct functions and enforces specific security responsibilities, requiring dedicated assessment items and criteria.

In addition, the Subscriber Identity Module (SIM), which stores authentication credentials and cryptographic keys, should also be evaluated to ensure that subscriber authentication and key protection mechanisms are securely implemented and managed.

(2) Assessment of Key Interfaces Core interfaces such as N1, N2, N3, and the Service-Based Interface (SBI) represent critical communication paths across the network. Encryption, authentication, and integrity protection mechanisms should be validated at the message level to ensure proper implementa-

tion.

(3) Evaluation of Inter-Node Interactions Security must be verified not only at the configuration level but also during real-time interactions between network nodes. This process helps detect vulnerabilities in authentication, key management, and session control procedures that may emerge during inter-NF communication.

(4) Verification of Mobility Scenarios During handover or roaming, when a UE transitions between gNBs, session continuity and key validity must be maintained. Because these transitions can introduce weaknesses in key derivation or re-authentication processes, corresponding procedures must be assessed. A secure design should ensure consistent protection across mobility boundaries.

(5) Assessment of Realistic Attack Scenarios The framework should evaluate resilience against real-world attack scenarios such as Denial of Service (DoS), replay, session hijacking, and unauthorized access. This allows verification of the network's defensive capabilities beyond what is explicitly defined in standards.

The next section introduces the proposed Private 5G Security Assessment Framework designed to fulfill these requirements.

3 Proposed Private 5G Security Assessment Framework

3.1 Overview

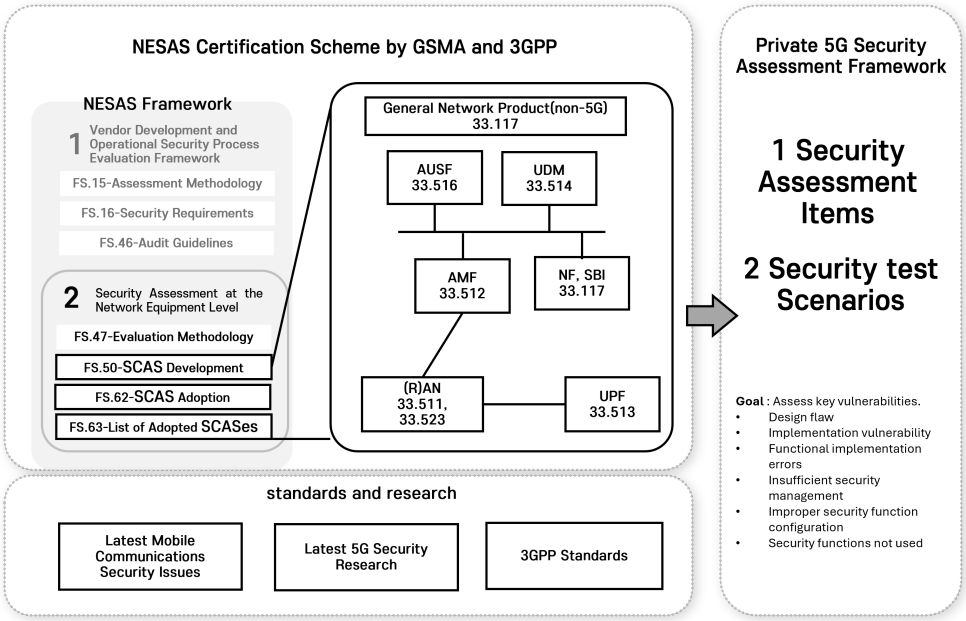

Figure 1: Proposed framework and reference

GSMA and 3GPP have established the NESAS to systematically verify the security of network equipment[11]. NESAS consists of two stages. The first stage evaluates the security of vendor development and operational processes, and the second verifies the security of the network equipment itself. The SCAS defines security assessment items and test methods for each 5G network function.

This study introduces a security assessment framework tailored to private 5G environments, devel-

oped with reference to SCAS, 3GPP standards, and recently reported security issues, and incorporating the security requirements described in Section 2.2. The framework consists of two main components. The first defines assessment items that reflect both the structural characteristics of 5G and the operational characteristics of private networks. The second defines test procedures to verify each item. Figure 1 illustrates the overall structure and its relationship with the 3GPP NESAS SCAS scheme.

It comprehensively evaluates design level flaws, implementation vulnerabilities, and operational configuration weaknesses. The framework examines both 5G specific vulnerabilities originating from the 5GC and gNB components and general security weaknesses that may lead to conventional network attacks. All assessment items are organized into four groups—5GC, gNB, SIM and Gnr—according to their functional domains within the network architecture. To more clearly highlight items requiring elevated criticality, an additional category named CRT(CRITICAL) was introduced. A total of 72 items were derived and classified by security domain and functional layer. Figure 2 presents the overall composition. Appendix Table 6, Table 7, Table 8, Table 9 and Table 10 provide a structured presentation of these assessment items, detailing the corresponding requirements and evaluation criteria. The following section describes the detailed items and assessment content for each security requirement.

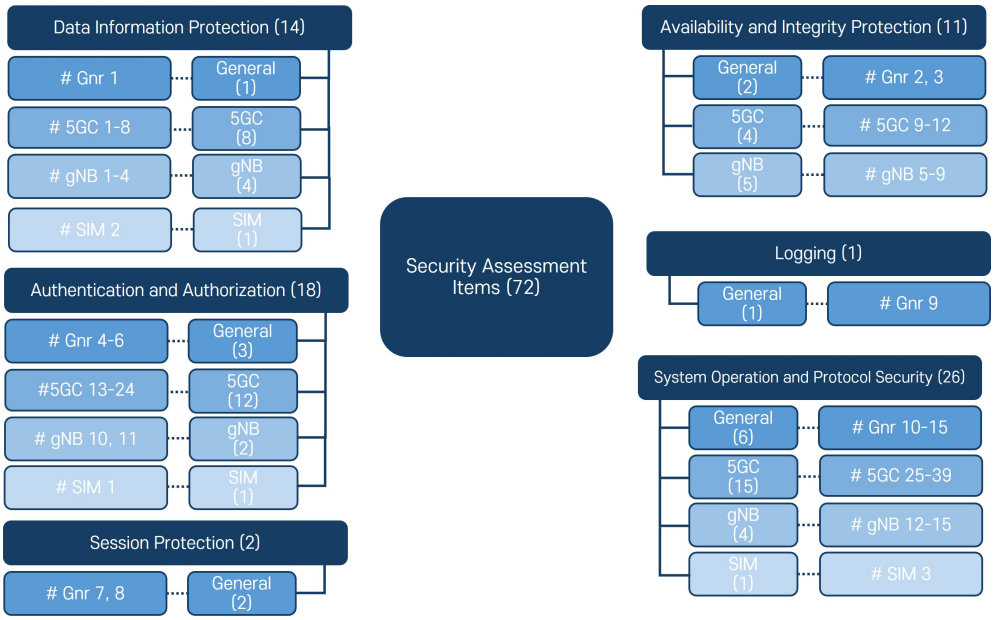

Figure 2: Proposed assessment items

3.2 Security Requirement-Based Assessment Framework

3.2.1 Data and Information Protection

Data and information protection assessment items are listed in Table 1.

 # 5GC 1, 2, 4, 5, # CRT 1 focus on encryption algorithm management. If the Access and Mobility Management Function (AMF) fails to apply the NAS encryption algorithm, Control Plane (CP) messages may be exposed. Furthermore, if the algorithm is not selected according to the UE's security algorithm priority and AMF policy, a man-in-the-middle attacker can exploit this to downgrade the encryption level, leading to CP message leakage.

 # 5GC 3, # CRT 2, 3 and # Gnr 1 address user identification and credential protection. User identifiers such as IMEI may be exposed during communication, and improper credential management of UEs can result in privacy breaches and credential leakage.

 # gNB 1, 2, 3, 4 focus on radio interface security. If RRC signaling data is not properly encrypted within the radio section, UE identifiers, Control Plane data, and User Plane data may be exposed.

 # SIM 2 focuses on SIM information security. SIM data such as KEY and OPC must be provisioned in encrypted form and stored encrypted within the core. An attacker who obtains SIM information could impersonate the UE and use its services.

Assessment Target	Case No.	Assessment Point	Threat Model	Ref.
Gnr	# Gnr 1	Are passwords securely stored using hashing?	• Sensitive asset leakage	[12]
5GC	# 5GC 1	When the AMF changes, is the NAS protection algorithm re-selected according to priority?	• Sensitive asset leakage	[13]
	# 5GC 2	During the initial NAS registration procedure, are UE 5G security capabilities correctly conveyed?	• Credential tampering • Mobility data leakage	[13]
	# 5GC 3	Is the IMEI identification procedure transmitted in encrypted form?	• Identifier exposure	[14]
	# 5GC 4	Is an appropriate encryption algorithm used to protect user data?	• User data leakage	[13]
	# 5GC 5	Is Non-clear Text transmitted only after encryption is applied?	• Sensitive data exposure	[15]
	# CRT 1	Are NAS messages protected with integrity and encryption?	• NAS interception • Tampering	[13]
	# CRT 2	Are authentication/identification-related UE data securely managed?	• Identity exposure • Credential compromise	[16], [12]
	# CRT 3	Are session keys securely managed according to their lifecycle?	• Key compromise	[14]
gNB	# gNB 1	Is RRC signaling data protected for confidentiality?	• Signaling interception	[17]
	# gNB 2	Is UP data encrypted according to the SMF-provided security policy?	• UP data leakage	[17], [18]
	# gNB 3	Is an appropriate AS protection algorithm selected?	• Algorithm downgrade attack	[17]
	# gNB 4	When the gNB changes, is the AS protection algorithm re-selected according to priority?	• Unauthorized downgrade • Signaling manipulation	[17]
SIM	# SIM 2	During USIM provisioning to the 5G Core, are mechanisms in place to prevent exposure in cleartext?	• Credential leakage • UE impersonation	[14]

Table 1: Data and Information Protection Assessment Items (14 cases)

3.2.2 Availability and Integrity Protection

Availability and integrity protection assessment items are listed in Table 2.

As private 5G expands across various industrial sectors, ensuring availability has become a critical requirement for environments that demand stable service operations. In addition, integrity is essential to ensure that data remains unaltered and trustworthy during transmission and storage.

#5GC 6, 8, 9 and #gNB 5, 6 address message integrity protection. Without proper NAS or AS integrity verification, a man-in-the-middle attacker can modify signaling or user plane messages, leading to tampering of mobility management and UP data.

#5GC 7 and #gNB 7, 8, 9 address retransmission control. If retransmitted NAS signaling, RRC signaling, or UP data are not properly handled, the network may enter a denial-of-service state.

#Gnr 2, 3 address protection against IP spoofing and SYN flooding attacks. These attacks can consume excessive network resources or generate forged requests repeatedly, disrupting normal service processing.

Assessment Target	Case No.	Assessment Point	Threat Model	Ref.
Gnr	# Gnr 6	Is IP spoofing prevention implemented?	• Identity spoofing	[12]
	# Gnr 7	Does the system support SYN flooding prevention mechanisms?	• Denial of service	[12]
5GC	# 5GC 6	When NAS integrity verification fails, are NAS messages properly discarded?	• NAS message tampering	[14]
	# 5GC 7	Are NAS signaling messages over the N1 interface protected against retransmission?	• Replay attack	[13]
	# 5GC 8	Is NIA0 excluded from the NAS integrity protection algorithms?	• Unauthorized downgrade	[13]
	# 5GC 9	Are NAS integrity algorithms correctly selected and applied?	• Signaling tampering • Unauthorized downgrade	[13]
gNB	# gNB 5	Is RRC signaling data protected for integrity?	• Signaling tampering • Mobility manipulation	[17]
	# gNB 6	Is UP data properly integrity-protected according to the security policy delivered by the SMF?	• UP data tampering	[17, 18]
	# gNB 7	When RRC/UP integrity verification fails, are messages properly discarded?	• Tampering attempt • Denial of service	[17]
	# gNB 8	Is UP data between UE and gNB protected against retransmission?	• Replay attack • UP tampering	[17]
	# gNB 9	Is RRC signaling data protected against retransmission?	• Replay attack • Signaling manipulation	[17]

Table 2: Assessment Items for Integrity and Availability Protection (11 cases)

3.2.3 Authentication and Authorization

In private 5G networks, authentication and authorization mechanisms are essential for maintaining secure access control, protecting subscriber information, and ensuring service continuity across network functions. The assessment focuses on verifying whether password management, NF-to-NF communication, authentication synchronization, and key handling procedures are securely implemented in accordance with 3GPP specifications. The assessment items for authentication and authorization are listed in Table 3.

#Gnr 2, 3, 11 address password policies, login, and remote access. If password rules are weak or login settings are poorly configured, attackers may compromise administrator accounts, alter system configurations, or escalate privileges, leading to unauthorized access to critical network assets.

#5GC 10, 11 address security of inter-NF communication. If TLS settings are insecure or access-token verification is missing, sensitive data exchanged between network functions may be exposed, and attackers could impersonate legitimate NFs or gain unauthorized control of signaling flows.

#5GC 12, 13, 16, 17 address authentication synchronization and verification. If SQN synchronization or RES verification failures are not properly handled, repeated re-synchronization attempts may consume system resources and cause denial of service for legitimate users. Such failures can also be exploited by attackers to trigger abnormal authentication loops or exhaust authentication servers.

#5GC 14, 15, #CRT 4 address key and identifier management. Errors in SUPI/SUCI handling, encryption or decryption failures, and poor identifier management can lead to subscriber-data exposure and privacy breaches. If the Unified Data Management (UDM) decrypts SUCI without validating an invalid ECC public key, it may be exploited as an oracle to infer the HN's private key, posing a serious threat to the confidentiality of subscriber identities.

#5GC 18, 19, #CRT 5 address the reliability of authentication procedures. If vulnerabilities exist in the authentication process or emergency access is improperly handled, unauthorized devices may connect to the network or use services without authentication, undermining the trust model of the core network.

#gNB 10, # CRT 7 address base-station authentication and interface security. If gNB certificate verification is insufficient or the gNB–5GC interface lacks proper encryption and integrity protection,

man-in-the-middle attacks and identity spoofing may occur, allowing attackers to impersonate legitimate network nodes.

#SIM 1 address UE impersonation. An attacker who obtains SIM information must not be able to impersonate a registered UE to access services.

Assessment Target	Case No.	Assessment Point	Threat Model	Ref.
Gnr	# Gnr 2	Is the password policy properly configured?	• Weak authentication • Unauthorized access	[12]
	# Gnr 3	Is the login policy properly configured?	• Account compromise • Denial of service	[12]
	# Gnr 11	Are system commands prevented from execution through SSI directives?	• Command injection • Privilege escalation	[12]
5GC	# 5GC 10	Are all NF communications within the same PLMN protected according to the TLS profile?	• NF impersonation • API data leakage	[12]
	# 5GC 11	When access-token verification fails within the same PLMN, is the request rejected?	• Unauthorized NF access • API misuse	[12]
	# 5GC 12	Does the AMF/SEAF properly handle synchronization-failure messages?	• Service disruption • Authentication failure looping	[13]
	# 5GC 13	Does the AMF/SEAF properly handle RES* verification failures?	• Unauthorized UE access • False acceptance risk	[13]
	# 5GC 14	Is the SUPI correctly decrypted?	• UE identity mismatch • Authentication failure	[19]
	# 5GC 15	Are invalid SUCIs rejected?	• Subscription data exposure • HN private-key exploitation	[19]
	# 5GC 16	Does the UDM properly handle synchronization-failure messages?	• Subscription data corruption • Service disruption	[19]
	# 5GC 17	Does the UDM accurately store the UE authentication state?	• Mis-binding of UE state • Authentication bypass	[19]
	# 5GC 18	Can unauthorized UEs perform abnormal emergency-access procedures?	• Unauthorized UE access	[14]
	# 5GC 19	Are UE connections allowed without completing authentication procedures?	• Identity spoofing • Unauthorized network access	[14]
	# CRT 4	Is the 5G-GUTI properly updated?	• UE traceability • Privacy leakage	[15]
	# CRT 5	Is the 5G-AKA authentication procedure correctly performed?	• Authentication failure • UE impersonation	[14]
gNB	# gNB 10	When certificates are invalid, does the system reject the connection?	• MITM attack • Spoofing	[17]
	# CRT 7	Are the N2/N3 interfaces securely protected by security protocols?	• Core-edge interception • Signaling manipulation	[17]
SIM	# SIM 1	Does the system prevent unauthorized access through SIM-swap attacks?	• UE impersonation	[14]

Table 3: Authentication and cases Authorization Assessment Items (18 cases)

3.2.4 Session Protection and Logging

Session protection and logging assessment items are listed in Table 4.

#Gnr 4, 12 address session management security. If inactivity timeout or session ID and cookie lifetime are not properly configured, attackers may hijack or reuse sessions to gain unauthorized access to critical assets.

#Gnr 5 address log integrity and event recording. If log files are not securely stored or logging functions are disabled, attackers may alter or delete logs to conceal malicious activities or evade detection. Logging also plays a critical role in post-incident investigation and accountability, ensuring that security events can be traced and verified.

Assessment Target	Case No.	Assessment Point	Threat Model	Ref.
Gnr	# Gnr 4	Are inactive interactive sessions automatically terminated after timeout?	• Exposure of critical assets	[12]
	# Gnr 12	Are session IDs, cookies, and lifetimes properly configured?	• Session tampering	[12]
	# Gnr 5	Does the system properly log security events?	• Log file tampering • Repudiation	[12]

Table 4: Session Protection and Logging Assessment Items (3 cases)

3.2.5 System Operation and Protocol Security

System operation and protocol security assessment items are listed in Table 5.

#Gnr 8, 9, 10 address system accounts and device access control. If user accounts do not have unique UIDs or removable media auto-run is enabled, attackers may impersonate legitimate users or modify the system.

#Gnr 13, 14, 15 address web and network service protection. If internal information is exposed in HTTP headers or error pages, or if IP filtering is insufficient, system structure may be revealed or DoS attacks may occur. In particular, if administrator credentials or configurations are leaked from the private 5G management web page, it may critically affect the entire service.

#5GC 20, 24, 28 address message validation in the core network. If abnormal messages are not properly rejected, attackers may send forged data to disrupt NF APIs or cause service failures.

#5GC 21, 22, 23 address protection against bidding-down attacks. If security level verification is insufficient, attackers may redirect UEs to lower security domains (e.g., EPC) and perform eavesdropping or session hijacking.

#5GC 25, 26 address user anonymity and session uniqueness. If the AMF does not assign a new 5G-GUTI or TEIDs are duplicated, users may be tracked, and traffic integrity may be compromised.

#5GC 27, 29 address consistency of user plane (UP) security policy. If policies between the UDM and SMF are inconsistent or not properly verified, UP data may be tampered with or leaked.

#5GC 30, 31 address key update and verification procedures. If security keys are reused or invalid values are not verified, attackers may eavesdrop, bypass authentication, or cause denial-of-service attacks.

#5GC 32, 33, # CRT 6 address network stability and data protection. If connections are abnormally terminated or encryption settings are insufficient, mobility or location data may be exposed.

#gNB 11, 12, 13, 14 address key renewal and UP security activation in the base station. If security keys are not properly updated during handover or dual connectivity transitions, UP data leakage or service interruption may occur.

#SIM 3 address SIM information protection and USIM lifecycle management. SIMs or USIMs that fall outside proper lifecycle management may lead to security risks, particularly when legacy equipment remains in use.

Assessment Target	Case No.	Assessment Point	Threat Model	Ref.
Gnr	# Gnr 8	Does each LINUX account have a unique UID?	• Identity spoofing • Privilege escalation	[12]
	# Gnr 9	Is special packet-processing functionality disabled?	• Information disclosure • Exposure of critical assets	[12]
	# Gnr 10	Are removable media devices prevented from auto-run or auto-mount?	• Hardware/OS modification	[12]
	# Gnr 13	Are critical web server details excluded from HTTP headers?	• Information disclosure	[12]
	# Gnr 14	Are web server details excluded from error pages?	• Information disclosure	[12]
	# Gnr 15	Does IP packet filtering operate properly?	• Service denial	[12]
5GC	# 5GC 20	Are messages containing invalid IEs rejected?	• Protocol violation • Service denial	[12]
	# 5GC 21	Does the AMF properly perform UE EPS redirection?	• Service disruption • Mobility data leakage	[13]
	# 5GC 22	Does the Xn handover prevent Bidding-Down attacks?	• Unauthorized downgrade • Mobility data tampering	[13]
	# 5GC 23	Does the AMF assign unpredictable new 5G-GUTIs?	• UE traceability • Privacy leakage	[13]
	# 5GC 24	Are messages containing invalid UE 5G security capabilities rejected?	• Security capability tampering • Unauthorized access	[13]
	# 5GC 25	In N4 session setup, are TEIDs uniquely generated?	• Session tampering • Charging manipulation	[20]
	# 5GC 26	Does the UP security policy from the UDM take precedence?	• UP data tampering • Policy bypass	[13]
	# 5GC 27	When UE UP policies mismatch, does the SMF handle them correctly?	• UP data leakage • UP tampering	[13]
	# 5GC 28	Are abnormal Security Header Types handled properly?	• Protocol violation • Service denial	[15]
	# 5GC 29	Are UEs disconnected due to network implementation issues?	• Service denial • Network misconfiguration	[15]
	# 5GC 30	Is the ABBA value properly used across the network?	• Bidding-down attack • Protocol mismatch	[15]
	# 5GC 31	Is a new security key used for every access procedure?	• Key theft • Eavesdropping	[14]
	# 5GC 32	Are invalid security values properly handled?	• Unauthorized access • Service disruption	[15]
	# 5GC 33	Are messages containing location information encrypted before transmission?	• Location privacy leakage	[15]
CRT	# CRT 6	Is the 5G Core securely protected?	• Exposure of critical assets • Physical tampering	[12]
gNB	# gNB 11	Is KgNB updated correctly?	• Mobility data leakage • UP data leakage	[17]
	# gNB 12	Does Xn handover prevent Bidding-Down attacks?	• Mobility manipulation	[17]
	# gNB 13	Are keys properly refreshed in dual-connectivity environments?	• UP data leakage	[17]
	# gNB 14	Does the gNB activate UP security during the RRC_INACTIVE state?	• Service denial	[17]
SIM	# SIM 3	Is an integrated USIM security management system implemented to manage the lifecycle securely?	• Sensitive information leakage	[14]

Table 5: System Operation and Protocol Security Assessment Items (26 cases)

3.3 Fulfillment of Private 5G Security Assessment Requirements

The proposed framework is designed to comprehensively assess all elements of a private 5G network by categorizing the items in the table into four domains: 5GC, gNB, SIM, and general items (Gnr) that apply to the overall system. The following summarizes how the framework satisfies the requirements defined in Section 2.2.

(1) **Comprehensive Verification by Component**

The framework divides assessment items into 5GC, gNB, SIM, and Gnr domains, evaluating the distinct security responsibilities of each component. SIM items verify the secure storage and transmission of credentials and subscriber information; gNB items examine RRC and UP data protection, algorithm selection, key renewal, and security continuity during handover; 5GC items evaluate NAS protection, authentication, key management, and inter-NF communication; and Gnr items assess general system and network security controls. This structure enables a layered and exhaustive evaluation of the entire private 5G architecture.

(2) **Verification of Key Interfaces**

The framework assesses the major interfaces N1, N2, N3, and SBI to ensure secure data and signaling exchange. At N1, it verifies encryption, integrity, and replay protection of NAS messages; at N2 and N3, it examines RRC and UP data protection and mutual authentication between gNB and 5GC; and at SBI, it checks TLS communication and token validation to guarantee secure control-plane operations in the SBA environment.

(3) **Evaluation of Inter-Node Interactions**

Beyond static configuration checks, the framework evaluates inter-node behavior under both normal and exceptional conditions. It examines the handling of authentication synchronization failures, RES*/SUCI verification errors, and abnormal requests, confirming that the control-plane procedures operate securely and consistently.

(4) **Verification of Mobility and Session Continuity**

Handover and reconnection procedures are included to verify that key regeneration and session maintenance remain secure. The framework evaluates Xn handover between gNBs, RRC_INACTIVE transitions, and GUTI reallocation and key updates in the 5GC, ensuring that cryptographic contexts and session data are properly maintained during mobility.

(5) **Assessment of Realistic Attack Scenarios**

The framework includes items that represent real-world threats such as bidding-down, denial of service, session hijacking, unauthorized access, and protocol violations. It evaluates the network's ability to detect, block, and recover from such attacks, while Gnr items extend the assessment to general system and network vulnerabilities, providing a broader view of operational security risks.

In summary, the framework integrates five key dimensions—components, interfaces, inter-node operations, mobility, and attack scenarios—to comprehensively and practically evaluate the structural and operational security of private 5G networks, thereby fulfilling all requirements defined in Section 2.2.

4 Application of the Framework

4.1 Experimental Application

To verify the feasibility and effectiveness of the proposed security assessment framework, experiments were conducted on a testbed built with UERANSIM and Open5GS. UERANSIM emulated the RAN segment, configuring both the UE and gNB, while Open5GS simulated the 5G Core network. We adopted the Standalone Non-Public Network (SNPN) model for the testbed because it provides full control over all nodes and interfaces, enabling complete security verification.

The experiments followed the 3GPP SCAS methodology for network equipment security evaluation. Each test verified that security configurations were properly activated and that runtime behaviors operated as intended. The goal was to assess the practical effectiveness of the proposed framework under realistic operational conditions.

Assessment scenarios were categorized into white-box and black-box methods. The white-box method examined whether security functions operated correctly by analyzing configuration parameters and packet logs within observable system internals. The black-box method focused on how the

system responded to abnormal or exceptional conditions through controlled external interactions. Each approach was applied according to the characteristics of the test items.

To support the behavior-focused tests, We developed a simulator. While UERANSIM is originally a 5G UE and RAN simulator for normal operations, it was extended to reproduce abnormal message injection, retransmission control, and policy inconsistency scenarios. The simulator was integrated with Open5GS, enabling dynamic and reproducible testing of all target items.

Figure 3 illustrates the testbed architecture and data flow between the modified UERANSIM and Open5GS components. The next section presents representative test cases and results, showing how the framework operates under both configuration-based and behavior-based validation.

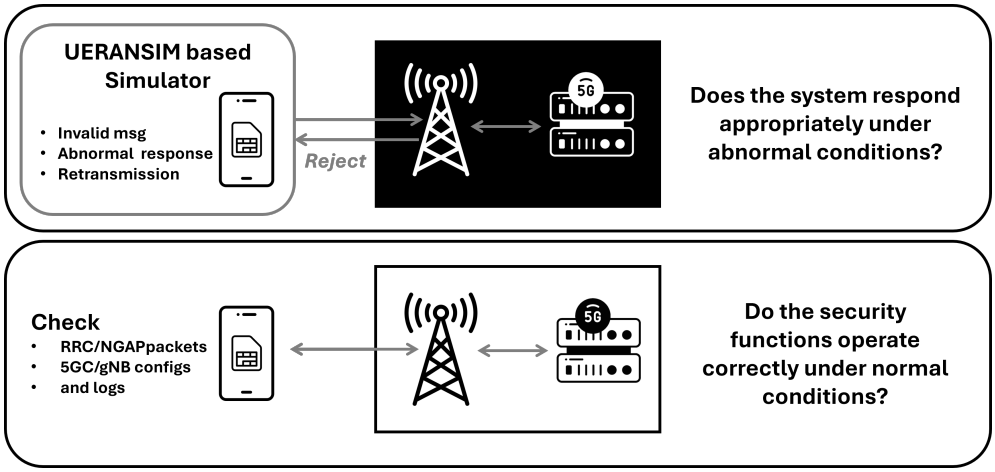

Figure 3: Testbed and Simulator

4.2 Results of Framework Application

4.2.1 Verification from Outside: Configuration and Behavior Observation

#5GC 2 verifies whether the AMF correctly forwards the UE's security capabilities during the initial registration procedure. The UE must be able to confirm that the selected encryption algorithm reflects both its own preferences and the core network's priority; otherwise, a man-in-the-middle attacker could downgrade the negotiated algorithm to a weaker one, leading to a bidding-down attack.

In this test, the UE sends a NAS Registration Request containing its supported security algorithms, and the AMF forwards this information to the gNB through an NGAP Context Setup Request. At this stage, the UE's RRC uplink message is inspected on the N1 interface, and the AMF's NGAP downlink message is inspected on the N2 interface.

The experiment confirmed that the security-capability values observed on both interfaces were identical, indicating that the AMF correctly relayed the UE's security information without modification. Figure 4 presents the verification result of the UE security capability transfer procedure.

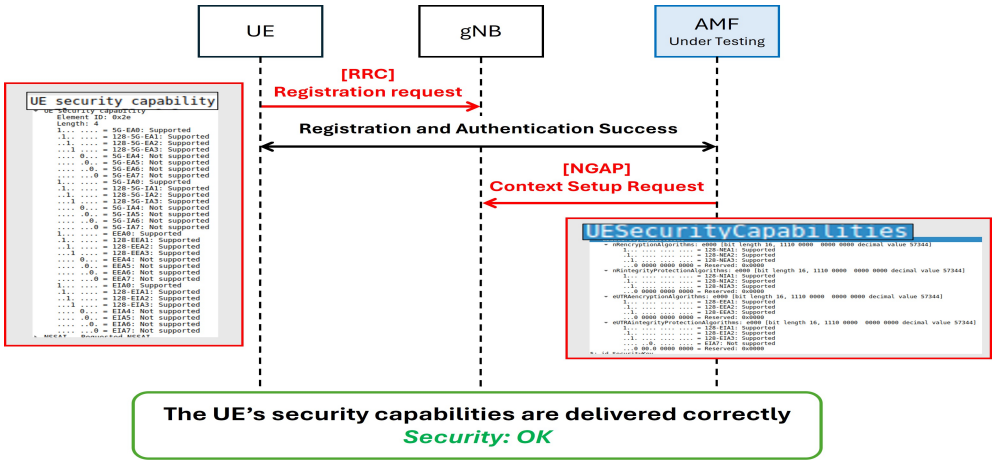

Figure 4: : Experiment Result of #5GC 2

4.2.2 Verification from Outside to Inside: Using a UE Simulator

#5GC 26 tests whether the AMF rejects invalid UE 5G security capabilities.

If the AMF does not properly reject NIA0 or NEA0, an attacker could manipulate signaling messages in transit to force the selection of a weaker algorithm, leading to a bidding-down scenario.

In this test, the UE-type simulator was configured to disable all mandatory 5GS encryption algorithms by setting the corresponding capability bits to zero and sent a Registration Request message. The AMF is expected to reject this request.

However, the experimental results showed that the Open5GS AMF accepted the registration and responded with an SMC message selecting NEA0. Although 3GPP TS 33.501[14] does not explicitly mandate NAS encryption, the absence of encryption can expose control-plane data and identifiers. This finding indicates that additional safeguards are needed to ensure stronger protection in private 5G environments.

Figure 5 shows the signaling where the UE sent an all-zero security capability, and the AMF responded with Null Ciphering.

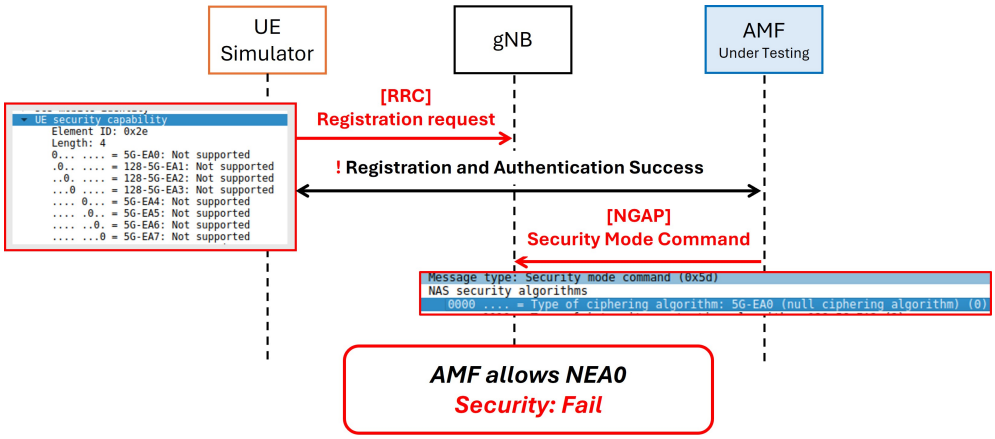

Figure 5: Experiment Result of #5GC 26

4.2.3 Verification from Inside to Inside: Using a NF Simulator

#5GC 17 tested whether the UDM correctly handled synchronization failure messages, which is essential to maintain reliable authentication between the UE and the network. Without this mechanism, outdated Sequence Number(SQN) values could lead to repeated authentication failures, resulting in potential denial-of-service conditions.

In this test, the simulator acting as the AUSF was configured to send a tampered indication containing invalid RAND and AUTS values to the UDM. The condition could be triggered by sending an HTTP message to the NF or by making the UE return a synchronization-failure in its authentication response. Upon receiving the message, the UDM initiated a resynchronization procedure with the ARPF and returned a new authentication vector to the AUSF. As shown in Figure 6, the UDM successfully processed the failure and completed the resynchronization procedure. The figure illustrates the end-to-end message flow between the AUSF, UDM, and ARPF during resynchronization.

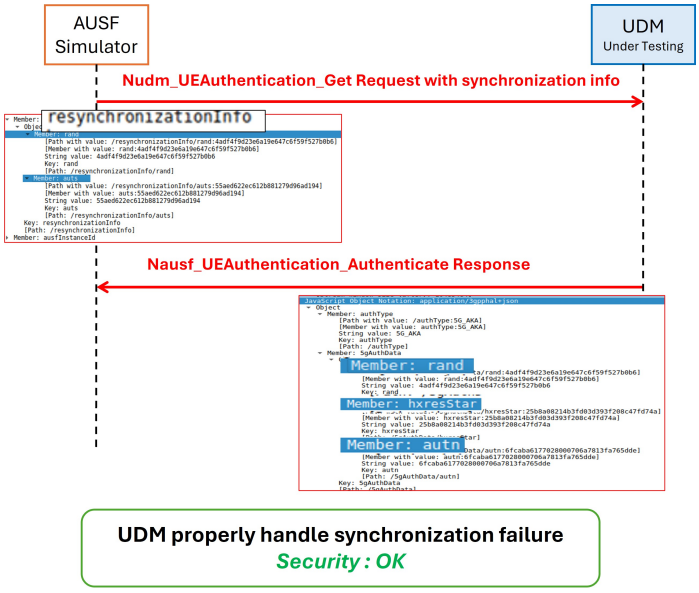

Figure 6: Experiment Result of #5GC 17

5 Application to a Commercial Private 5G Network

5.1 Environment and Inspection Scope

To verify the practical effectiveness of the proposed security assessment framework beyond testbed conditions, it was applied to E-Company's operational R&D private 5G network. Among the 72 assessment items, the inspection focused on features supported by the network and accessible nodes. Core network inspection was conducted by analyzing NGAP packets exchanged between the AMF and gNB, and Service-Based Interface (SBI) communication logs within the core. Base station inspection focused on RRC messages, while additional analysis of system logs, configuration files, and management interfaces available in the operational environment supplemented the inspection scope.

For the inspection, our research team provided E-Company with the derived security assessment items and test scenarios. E-Company conducted self-testing for certain items to verify its security posture, while tests requiring a UE simulator or real-time evidence collection were carried out directly by our research team on-site. Through this process, the operation of authentication and session procedures as well as the behavior of major security functions were verified in the live network.

The overall inspection process is illustrated in Figure 7.

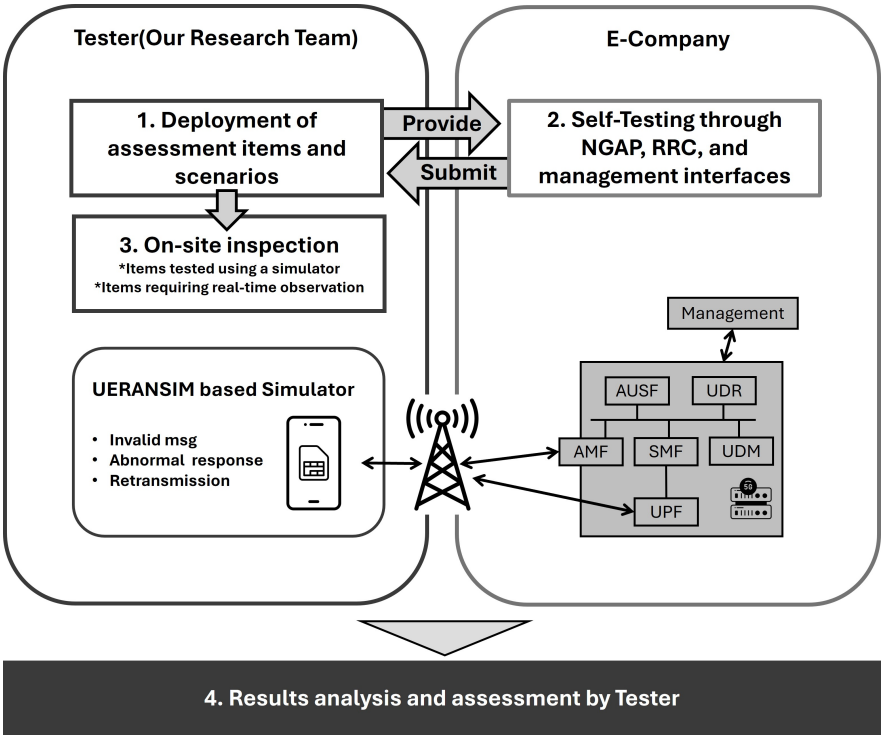

Figure 7: Overall Inspection Process in Commercial Private 5G Network (E-Company)

5.2 Assessment Results and Analysis

Most assessment items satisfied the security requirements defined in the proposed private 5G security assessment framework. As discussed in Section 4.2.2, item #5GC 26, which had failed in the testbed, operated correctly in the commercial environment.

Some configurations in the operational network differed from those defined in the framework; however, these variations were not security flaws, but adaptations made to ensure interoperability and operational efficiency.

Even when certain functions were not implemented or were outside the direct assessment scope, equivalent security controls were verified to be in place. For example, when token-based authorization was unavailable due to the absence of NRF implementation, we confirmed that alternative access-control mechanisms were applied.

Using the test scenarios and simulator developed in this study, we were able to assess not only external components such as the AMF, which connects to the UE through the N1 interface, and the UPF, which connects to external data networks through the N6 interface, but also internal control-plane entities such as the UDM.

While the detailed inspection results from E-Company cannot be disclosed for security reasons, the overall security level was found to be satisfactory. These findings demonstrate that the proposed framework can effectively evaluate both external and internal components within real private 5G operational environments.

6 Conclusion

This study proposed a security assessment framework to systematically evaluate the security of private 5G networks. Based on 3GPP standards, recent research, and field security issues, 72 assessment items were defined, and corresponding test procedures and validation tools were implemented. The framework was validated in a testbed built with Open5GS and UERANSIM, confirming its feasibility and reproducibility. When applied to an R&D private 5G network, most assessment items satisfied the defined security requirements. The results demonstrated that the proposed framework can serve as a practical verification system applicable to real operational environments, beyond the boundaries of controlled testbeds. Furthermore, by using unified test scenarios and simulators, the framework successfully verified not only externally exposed components but also core internal functions, proving its scalability and effectiveness for comprehensive security evaluation.

For future work, we plan to extend the framework by incorporating deployment models and service-specific security requirements of private 5G networks, and to develop automated tools that enable broader application across diverse industrial environments.

Acknowledgments

Following are results of a study on the 'Policy Research on Strengthening Cybersecurity in Companies Adopting New 5G Technologies' project, supported by Korea Internet & Security Agency (No.A2025-0455)

References

[1] Miaowen Wen, Qiang Li, Kyeong Jin Kim, David López-Pérez, Octavia A. Dobre, H. Vincent Poor, Petar Popovski, and Theodoros A. Tsiftsis. Private 5g networks: Concepts, architectures, and research landscape. *IEEE Journal of Selected Topics in Signal Processing*, 16(1):7–25, 2022.

[2] Yiming Guo and Yong Zhang. Study on core network security enhancement strategies in 5g private networks. In *2021 IEEE 21st International Conference on Communication Technology (ICCT)*, pages 887–891, 2021.

[3] Shida Xia, Dejian Li, Xu Zhao, Jie Zhou, Jiadong Du, Qi Wang, Weibin Hou, and Risheng Lv. Research on the physical layer security for industrial 5g private networks. In *2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, volume 11, pages 816–819, 2023.

[4] Francesco Mancini and Giuseppe Bianchi. Scasdk - a development kit for security assurance test in multi-network-function 5g. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, New York, NY, USA, 2023. Association for Computing Machinery.

[5] Open5GS Project. Open5gs website. `https://open5gs.org`, 2024. Retrieved November 2025.

[6] UERANSIM Project. Ueransim resources: Ueransim github repository. `https://github.com/aligungr/UERANSIM`, 2024. Retrieved November 2025.

[7] Iso/iec 15408-1:2022 information security, cybersecurity and privacy protection — evaluation criteria for it security — part 1: Introduction and general model, 2022. Ref. No. 72891. Available at: `https://www.iso.org/standard/72891.html`.

[8] Iso/iec 27001:2022 information security, cybersecurity and privacy protection — information security management systems — requirements, 2022. Available at: `https://www.iso.org/standard/82875.html`.

[9] Korea Internet Security Agency (KISA). Isms-p (2024.07). Online; https://isms.kisa.or.kr/main/ispims/notice/?boardId=bbs_0000000000000014&mode=view&cntId=24, 2024. Accessed: 2025-11-05.

[10] GV Pavan, V Sangeetha, et al. Survey on security risks in 5g private industrial networks. In *2022 4th International Conference on Circuits, Control, Communication and Computing (I4C)*, pages 147–152. IEEE, 2022.

[11] Silvana Qose and Esmeralda Kadena. Enhancing trust in 5g. In *2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES)*, pages 000131–000136, 2022.

[12] 3GPP. Catalogue of general security assurance requirements . Technical Specification (TS) 33.117, 3rd Generation Partnership Project (3GPP).

[13] 3GPP. 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF). Technical Specification (TS) 33.512, 3rd Generation Partnership Project (3GPP).

[14] 3GPP. Security architecture and procedures for 5G System. Technical Specification (TS) 33.501, 3rd Generation Partnership Project (3GPP).

[15] 3GPP. Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3. Technical Specification (TS) 24.501, 3rd Generation Partnership Project (3GPP).

[16] 3GPP. 5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3. Technical Specification (TS) 29.505, 3rd Generation Partnership Project (3GPP).

[17] 3GPP. Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class. Technical Specification (TS) 33.511, 3rd Generation Partnership Project (3GPP).

[18] 3GPP. 5G Security Assurance Specification (SCAS); Split gNB product classes. Technical Specification (TS) 33.523, 3rd Generation Partnership Project (3GPP).

[19] 3GPP. 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class. Technical Specification (TS) 33.514, 3rd Generation Partnership Project (3GPP).

[20] 3GPP. 5G Security Assurance Specification (SCAS); User Plane Function (UPF). Technical Specification (TS) 33.513, 3rd Generation Partnership Project (3GPP).

A 5G Security Assessment Framework Tables

The following tables summarize the detailed assessment items used in the proposed Private 5G Security Assessment Framework.

Category	Case No.	Assessment Point	Threat Model	Ref.
Data and Information Protection	# Gnr 1	Are passwords securely stored using hashing?	Sensitive asset leakage	33.117
Authentication and Authorization	# Gnr 2	Is the password policy properly configured?	Identity spoofing	33.117
	# Gnr 3	Is the login policy properly configured?	Denial of Service	33.117
Session Protection	# Gnr 4	Are inactive interactive sessions automatically terminated after timeout?	Exposure of critical assets	33.117
Logging	# Gnr 5	Does the system properly log security events?	Log file tampering, Repudiation	33.117
Availability and Integrity Protection	# Gnr 6	Is IP spoofing prevention implemented?	Identity spoofing	33.117
	# Gnr 7	Does the system support SYN flooding prevention mechanisms?	Denial of Service	33.117
System Operation and Protocol Security	# Gnr 8	Does each LINUX account have a unique UID?	Privilege escalation, Identity spoofing	33.117
	# Gnr 9	Is special packet-processing functionality disabled?	Information disclosure, Exposure of critical assets	33.117
	# Gnr 10	Are removable media devices prevented from auto-run or auto-mount?	Hardware/OS modification	33.117
Authentication and Authorization	# Gnr 11	Are system commands prevented from execution through SSI directives?	Privilege escalation	33.117
Session Protection	# Gnr 12	Are session IDs, cookies, and lifetimes properly configured?	Session tampering	33.117
System Operation and Protocol Security	# Gnr 13	Are critical web server details excluded from HTTP headers?	Information disclosure	33.117
	# Gnr 14	Are web server details excluded from error pages?	Information disclosure	33.117
	# Gnr 15	Does IP packet filtering operate properly?	Denial of Service	33.117

Table 6: General Security Configuration Assessment Items (Gnr 1–15)

Category	Case No.	Assessment Point	Threat Model	Ref.
Data and Information Protection	# 5GC 1	When the AMF changes, is the NAS protection algorithm re-selected according to priority?	Sensitive asset leakage	33.512
	# 5GC 2	During the initial NAS registration procedure, are UE 5G security capabilities correctly conveyed?	Credential tampering, Mobility data leakage	33.512
	# 5GC 3	Is the IMEI identification procedure transmitted in encrypted form?	Identifier exposure	33.501
	# 5GC 4	Is an appropriate encryption algorithm used to protect user data?	User data leakage	33.512
	# 5GC 5	Is Non-clear Text transmitted only after encryption is applied?	Sensitive data exposure	24.501
Availability and Integrity Protection	# 5GC 6	When NAS integrity verification fails, are NAS messages properly discarded?	NAS message tampering	33.512
	# 5GC 7	Are NAS signaling messages over the N1 interface protected against retransmission?	Replay attack	33.512
	# 5GC 8	Is NIA0 excluded from the NAS integrity protection algorithms?	Unauthorized downgrade	33.512
	# 5GC 9	Are NAS integrity algorithms correctly selected and applied?	Signaling tampering, Unauthorized downgrade	33.512
Authentication and Authorization	# 5GC 10	Are all NF communications within the same PLMN protected according to the TLS profile?	NF impersonation, API data leakage	33.117
	# 5GC 11	When access-token verification fails within the same PLMN, is the request rejected?	Unauthorized NF access, API misuse	33.117
	# 5GC 12	Does the AMF/SEAF properly handle synchronization-failure messages?	Service disruption, Authentication failure looping	33.512
	# 5GC 13	Does the AMF/SEAF properly handle RES* verification failures?	Unauthorized UE access, False acceptance risk	33.512
	# 5GC 14	Is the SUPI correctly decrypted?	UE identity mismatch, Authentication failure	33.514
	# 5GC 15	Are invalid SUCIs rejected?	Subscription data exposure, HN private-key exploitation	33.514
	# 5GC 16	Does the UDM properly handle synchronization-failure messages?	Subscription data corruption	33.514
	# 5GC 17	Does the UDM accurately store the UE authentication state?	Mis-binding of UE state, Authentication bypass	33.514
	# 5GC 18	Can unauthorized UEs perform abnormal emergency-access procedures?	Unauthorized UE access	33.501
	# 5GC 19	Are UE connections allowed without completing authentication procedures?	Identity spoofing, Unauthorized network access	33.501
System Operation and Protocol Security	# 5GC 20	Are messages containing invalid IEs rejected?	Protocol violation, Denial of Service	33.117
	# 5GC 21	Does the AMF properly perform UE EPS redirection?	Service disruption, Mobility data leakage	33.512
	# 5GC 22	Does the Xn handover prevent Bidding-Down attacks?	Unauthorized downgrade, Mobility data tampering	33.512
	# 5GC 23	Does the AMF assign unpredictable new 5G-GUTIs?	UE traceability, Privacy leakage	33.512
	# 5GC 24	Are messages containing invalid UE 5G security capabilities rejected?	Security capability tampering, Unauthorized access	33.512
	# 5GC 25	In N4 session setup, are TEIDs uniquely generated?	Session tampering, Charging manipulation	33.513
	# 5GC 26	Does the UP security policy from the UDM take precedence?	UP data tampering, Policy bypass	33.515
	# 5GC 27	When UE UP policies mismatch, does the SMF handle them correctly?	UP data leakage, UP tampering	33.515
	# 5GC 28	Are abnormal Security Header Types handled properly?	Protocol violation, Denial of Service	24.501
	# 5GC 29	Are UEs disconnected due to network implementation issues?	Denial of Service, Network misconfiguration	24.501
	# 5GC 30	Is the ABBA value properly used across the network?	Bidding-down attack, Protocol mismatch	24.501
	# 5GC 31	Is a new security key used for every access procedure?	Key theft, Eavesdropping	33.501
	# 5GC 32	Are invalid security values handled appropriately?	Unauthorized access, Service disruption	24.501
	# 5GC 33	Are messages containing location information encrypted before transmission?	Location privacy leakage	24.501

Table 7: 5GC Security Assessment Items (5GC 1–33)

Category	Case No.	Assessment Point	Threat Model	Ref.
Data and Information Protection	# gNB 1	Is RRC signaling data protected for confidentiality?	Signalling interception	33.511
	# gNB 2	Is UP data encrypted according to the SMF-provided security policy?	UP data leakage	33.511, 33.523
	# gNB 3	Is an appropriate AS protection algorithm selected?	Algorithm downgrade attack	33.511
	# gNB 4	When the gNB changes, is the AS protection algorithm re-selected according to priority?	Unauthorized downgrade, Signalling manipulation	33.511
Availability and Integrity Protection	# gNB 5	Is RRC signaling data protected for integrity?	Signalling tampering, Mobility manipulation	33.511
	# gNB 6	Is UP data properly integrity-protected according to the security policy delivered by the SMF?	UP data tampering	33.511, 33.523
	# gNB 7	When RRC/UP integrity verification fails, are messages properly discarded?	Tampering attempt, Denial of Service	33.511
	# gNB 8	Is UP data between UE and gNB protected against retransmission?	Replay attack, UP tampering	33.511
	# gNB 9	Is RRC signaling data protected against retransmission?	Replay attack, Signalling manipulation	33.511
	# gNB 10	When certificates are invalid, does the system reject the connection?	MITM attack, Spoofing	33.511
System Operation and Protocol Security	# gNB 11	Is KgNB updated correctly?	Mobility data leakage, UP data leakage	33.511
	# gNB 12	Does Xn handover prevent Bidding-Down attacks?	Mobility manipulation	33.511
	# gNB 13	Are keys properly refreshed in dual-connectivity environments?	UP data leakage	33.511
	# gNB 14	Does the gNB activate UP security during the RRC_INACTIVE state?	Denial of Service	33.511

Table 8: gNB Security Assessment Items (gNB 1–14)

Category	Case No.	Assessment Point	Threat Model	Ref.
Data & Information Protection	# CRT 1	Are NAS messages protected with integrity and encryption?	NAS interception, Tampering	33.512
	# CRT 2	Are authentication/identification-related UE data securely managed?	Identity exposure, Credential compromise	29.505, 33.117
	# CRT 3	Are session keys securely managed according to their lifecycle?	Key compromise	33.501
Authentication & Authorization	# CRT 4	Is the 5G-GUTI properly updated?	UE traceability, Privacy leakage	24.501
	# CRT 5	Is the 5G-AKA authentication procedure correctly performed?	Authentication failure, UE impersonation	33.501
System Operation and Protocol Security	# CRT 6	Is the 5G Core securely protected?	Exposure of critical assets, Physical tampering	33.117
Authentication & Authorization	# CRT 7	Are the N2/N3 interfaces securely protected by security protocols?	Core-edge interception, Signalling manipulation	33.210, 33.501, 33.511, 33.523

Table 9: CRT Security Assessment Items (CRT 1-7)

Assessment Target	Case No.	Assessment Point	Threat Model	Ref.
Authentication & Authorization	# SIM 1	Does the system prevent unauthorized access through SIM-swap attacks?	UE impersonation	33.501
Data & Information Protection	# SIM 2	During USIM provisioning to the 5G Core, are mechanisms in place to prevent exposure in cleartext?	Credential leakage, UE impersonation	33.501
System Operation and Protocol Security	# SIM 3	Is an integrated USIM security management system implemented to manage the lifecycle securely?	Sensitive information leakage	33.501

Table 10: SIM Security Assessment Items (SIM 1–3)