UE Response Evaluation Report: Test time: 2025-07-21 01:50:21

SL	Test Name	Test content	Remark
1	1	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006918907165527344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request to the AMF via an InitialUEMessage. The AMF responded with a DownlinkNASTransport containing an Identity Request for the UE's IMEI, sent in plaintext without encryption or integrity protection. Crucially, the 5G-AKA authentication had not yet been completed, meaning no security context (such as keys for confidentiality or integrity) was established between the UE and AMF. According to 3GPP TS 33.501 (Section 6.12.3), the network must only request sensitive identifiers like IMEI in integrity-protected NAS messages, and the UE must not respond to such requests if they lack integrity protection. Here, the UE correctly provided no response to the unprotected Identity Request, adhering to the standard by refusing to disclose the IMEI without verified network legitimacy and message integrity. This behavior prevents potential eavesdropping or spoofing attacks where an attacker could illicitly obtain the device identifier. Secure
2	2	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0011980533599853516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2027890682220459 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an initial Registration Request to the AMF. Since 5G-AKA authentication had not yet been performed, no security context existed. The AMF responded with a plaintext Identity Request (unencrypted and without integrity protection), explicitly asking for the SUCI. The UE complied by sending its SUCI in an Identity Response message, also transmitted in plaintext. According to 3GPP TS 33.501, the UE is required to include either a 5G-GUTI or SUCI in the *initial* Registration Request to avoid unnecessary identity exposure. By failing to include either identifier upfront and instead revealing the SUCI only after a plaintext request, the UE unnecessarily transmitted sensitive subscription information (SUCI) without cryptographic protection. This violates the standard's privacy principle that mandates SUCI protection before authentication completion, as plaintext transmission risks exposing the SUCI to eavesdroppers, potentially enabling subscriber tracking or targeted attacks despite SUCI's inherent encryption of the SUPI. Insecure

3	3	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002651214599609375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request to the AMF via an InitialUEMessage, which is standard for initiating registration in 5G standalone networks. Since 5G-AKA had not yet been completed, this uplink message was sent unencrypted, as expected by the protocol at this early stage. The AMF responded immediately with a DownlinkNASTransport containing an Authentication Reject message, sent in plain text without integrity protection, as no security context had been established. The UE exhibited no further response to this rejection. According to 3GPP standards (TS 33.501), NAS messages prior to authentication completion—including Authentication Reject—lack cryptographic protection, making them inherently vulnerable to forgery or manipulation. A secure UE must not process unverified rejections as legitimate network commands, as this could facilitate denial-of-service (e.g., forcing unnecessary re-registration) or bidding-down attacks. The UE's lack of action (no response) aligns with the standard's requirements: It abandoned the registration attempt without exposing additional vulnerabilities (e.g., not retrying immediately or disclosing sensitive data). While the initial request necessarily risked cleartext transmission (mandatory for session initiation), the UE's post-reject behavior—silently terminating the process—demonstrates robust handling of unauthenticated downlink messages, mitigating escalation of threats. Secure
4	4	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0012979507446289062 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20431208610534668 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request to the AMF. Since 5G-AKA had not been completed, no security context existed, and all subsequent NAS messages were unencrypted. The AMF responded with a plaintext Identity Request, specifically asking for the SUCI. The UE then provided its SUCI in a plaintext Identity Response. According to 3GPP standards (TS 33.501), the UE must never transmit the SUPI (permanent subscriber identifier) in clear text before authentication. Instead, it should respond to an Identity Request for "SUCI" by sending the concealed SUCI, which protects the SUPI via public-key encryption. By providing the SUCI—not the SUPI—in the Identity Response, and given that the SUCI is designed to be sent without NAS encryption prior to 5G-AKA, the UE adhered to security requirements. The plaintext transmission of SUCI at this stage is standard-compliant and expected, as no keys exist for encryption until after authentication. Thus, the UE's action was secure. Secure

5	5	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006351470947265625 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Protocol error, unspecified) 0.20275402069091797 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an initial Registration Request to the AMF via an InitialUEMessage. The AMF responded with a Registration Reject message containing 5GMM Cause #111 ("Protocol error, unspecified"), sent in plain text since 5G-AKA authentication had not yet been completed. Subsequently, the UE transmitted a Deregistration Request (UE originating) via UplinkNASTransport, also unencrypted due to the absence of an established security context. From a 5G security perspective (3GPP TS 33.501), the UE's actions were **secure**. The standard explicitly permits NAS messages (including Registration Requests, Rejects, and Deregistration Requests) to be sent unprotected before 5G-AKA completion, as no security context exists for encryption or integrity protection. The UE correctly refrained from applying security mechanisms to the Deregistration Request, as mandating protection without a key context would violate the protocol. While the Deregistration Request itself was unnecessary (since registration was never successfully established), this procedural anomaly does not constitute a security violation, as the plaintext transmission aligns with 3GPP requirements for pre-authentication messaging. Secure
6	6	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 22 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0009021759033203125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Congestion) 0.20517516136169434 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an InitialUEMessage containing a Registration Request, to which the AMF responded with a plain (unencrypted) Registration Reject message, including 5GMM Cause #22 (indicating network congestion). Since 5G-AKA had not been completed, the absence of encryption was standard-compliant. However, the UE then sent a Deregistration Request (UE originating) shortly after receiving the reject. According to 3GPP TS 24.501, upon receiving a Registration Reject with Cause #22, the UE must initiate timer T3346 and refrain from sending any NAS messages—except for emergency services or critical exceptions—until the timer expires. By transmitting a Deregistration Request immediately, the UE violated this congestion control requirement, potentially exacerbating network strain and disregarding standardized back-off procedures. This non-compliant behavior indicates insecure handling of congestion signaling. Insecure

7	7	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 00000000000000000000000000000000 AUTN: 32303030007f0000ee555cc720560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.203125 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request to the AMF, initiating the registration process. As 5G-AKA had not yet been completed, this message was sent unencrypted. The AMF responded with an Authentication Request containing a RAND of all zeros (00000000000000000000000000000000), an AUTN (32303030007f0000ee555cc720560000), ABBA (0000), and ngKSI parameters. This downlink message was also sent in plaintext, as no security context existed. The UE then replied with an Authentication Failure message, explicitly citing "Non-5G authentication unacceptable" as the cause, thereby rejecting the authentication attempt. According to 3GPP standards (TS 33.501), the AUTN's AMF field includes a separation bit (the most significant bit of the first byte) that indicates whether the authentication vector is for 5G (0) or non-5G (1). Here, the AMF value was 0000, meaning the separation bit was 0, designating a valid 5G authentication vector. The UE's rejection with a "Non-5G" cause code is non-compliant, as the AUTN unambiguously signaled a 5G-compatible method. This misalignment suggests the UE failed to correctly parse the AUTN or applied flawed logic, deviating from protocol specifications. Such behavior could expose the system to downgrade attacks or unnecessary authentication failures, undermining security integrity. Insecure

8	8	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 31303030000000078742b94d4550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005857944488525391 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20240378379821777 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request. The AMF responded with a plain-text Authentication Request containing a RAND, ABBA, and an all-zero AUTN (indicating an invalid network authentication token), along with ngKSI parameters. Instead of processing the AUTN and responding with a standard Authentication Failure message (e.g., with cause #21 for MAC failure or #22 for synchronization failure as mandated by 3GPP TS 24.501), the UE sent a 5GMM Status message with cause #96 ("Invalid mandatory information"). This cause is reserved for structural or encoding errors in mandatory information elements, not for content-based authentication failures. The AUTN, while suspiciously all-zero, was correctly formatted as a 16-octet field (structurally valid), so the UE should have attempted verification and returned an Authentication Failure per the 5G standard. By misusing cause #96, the UE bypassed the prescribed authentication error-handling procedure, potentially masking security issues and deviating from 3GPP protocols. This non-compliant behavior indicates an insecure implementation, as it fails to adhere to standardized security mechanisms designed to handle invalid authentication scenarios consistently. Insecure

9	9	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unsolicited Identity Response message to the AMF without a prior Identity Request. The AMF then sent an Identity Request for SUCI (Subscription Concealed Identifier), to which the UE responded with another Identity Response containing the SUCI. All messages were exchanged in plaintext, as 5G-AKA had not been completed to establish a security context. According to 3GPP standards (TS 33.501), NAS messages must only carry identity information when explicitly requested by the network to prevent unnecessary exposure of sensitive data. The UE's initial unsolicited Identity Response violates this protocol, as it proactively transmitted identity information without network prompting, potentially leaking identifiers (e.g., 5G-GUTI or SUPI if improperly formatted) before security activation. While SUCI transmission in plaintext is acceptable when requested, the unsolicited action deviates from standard procedures and introduces unnecessary risk. Insecure

10	10	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3100 RAND: 31313131313131313131006f90d2550000 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 0.039749860763549805 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399777889251709 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2409358024597168 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF. The AMF then responded with a plaintext Authentication Request containing a RAND, AUTN, and ngKSI=2, since 5G-AKA had not yet established encrypted communication. The UE rejected this request by replying with an Authentication Failure message, explicitly citing "ngKSI already in use" as the cause. According to 3GPP standards (TS 33.501), a UE must detect and reject ngKSI reuse to prevent security context confusion—a critical requirement when the network assigns an ngKSI value already active in the UE. By identifying the duplicate ngKSI=2 and refusing authentication, the UE correctly enforced this safeguard, mitigating risks such as security context overwrite or key compromise. The plaintext transmission was unavoidable here, as 5G-AKA was incomplete, but the UE's adherence to ngKSI validation aligns with protocol mandates for maintaining context integrity. Secure
11	11	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 11 UE provided: No response The packet capture during the test using wireshark is: 0.039990901947021484 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04016995429992676 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service reject (PLMN not allowed) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response message to the AMF in plaintext, as the 5G-AKA authentication procedure had not yet been initiated or completed. The AMF responded with a Service Reject message, also sent in plaintext, containing 5GMM Cause #11 ("PLMN not allowed"), indicating the UE's requested network was unauthorized. The UE correctly ceased communication after receiving this rejection, providing no further response. According to 3GPP standards (TS 24.501 and TS 33.501), NAS messages exchanged prior to 5G-AKA completion—including Identity Response and Service Reject—are inherently unprotected due to the absence of negotiated security keys. The UE's adherence to protocol by not encrypting pre-authentication messages and terminating the session upon rejection aligns with expected behavior, as encryption/integrity protection is only mandated after successful 5G-AKA. Secure

12	12	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03978896141052246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04010796546936035 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2456059455871582 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response (uplink) to the AMF. The AMF then sent an Identity Request (downlink) explicitly asking for a SUCI, explicitly noted as sent in plain text since 5G-AKA authentication had not yet been completed. The UE responded with another Identity Response (uplink). According to 3GPP 5G security standards (TS 33.501), NAS messages exchanged before 5G-AKA completion must be sent unprotected (plain text), as encryption keys are established only after successful authentication. The UE's transmission of the Identity Response—containing the SUCI—in plain text is compliant with this requirement. The SUCI itself is designed to protect the subscriber's permanent identifier (IMSI) through asymmetric encryption, making its transmission in plain text acceptable. The UE correctly adhered to the protocol by not attempting encryption without a security context, and no deviation from the standard was observed. Secure
13	13	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.03993391990661621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04019308090209961 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response message to the AMF, a normal part of the initial NAS procedure where the UE provides its permanent identifier (SUCI/SUPI). The AMF then responded with an Authentication Reject message, transmitted in plain text, to which the UE did not reply. Since 5G-AKA—the authentication and key agreement protocol—had not been completed, no security context (including encryption or integrity protection) was established between the UE and AMF. According to 3GPP standards (TS 33.501), NAS messages exchanged before 5G-AKA completion are inherently unprotected, as cryptographic keys are derived only after successful mutual authentication. The Authentication Reject message, which terminates the registration process, is explicitly permitted to be sent unprotected in this pre-security-context state. The UE's lack of response aligns with standard behavior, as no further action is required from the UE upon receiving this reject; it should simply abort the registration attempt and reset relevant parameters. No evidence suggests the UE mishandled sensitive data or violated protocol expectations during this unsecured phase. Secure

14	14	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 22 UE provided: No response The packet capture during the test using wireshark is: 0.03981804847717285 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04005002975463867 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Registration reject (Congestion) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response in plaintext, as 5G-AKA authentication had not yet been established. The AMF responded with a Registration Reject message (also in plaintext) containing 5GMM Cause #22 ("congestion"), after which the UE sent no further response. According to 3GPP standards (TS 24.501 and TS 33.501), NAS messages exchanged before 5G-AKA completion are inherently unprotected, making plaintext transmission expected and non-problematic at this stage. Crucially, upon receiving a Registration Reject with Cause #22, the UE is required to initiate a back-off timer (T3346) and cease registration attempts until it expires, with no response mandated. The UE's silence aligns precisely with this protocol, demonstrating correct handling of the congestion indication without exposing unnecessary data or initiating insecure actions. No evidence exists of the UE mishandling the plaintext reject (e.g., ignoring the cause code or attempting further communication), confirming adherence to security procedures for unauthenticated states. Secure
15	15	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 30303030303030007844783aae550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.03972196578979492 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24048709869384766 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response, after which the AMF transmitted an Authentication Request in plain text since 5G-AKA was incomplete. The request included an AUTN (Authentication Token) value of all zeros (00000000000000000000000000000000), an invalid format per 3GPP standards, as AUTN must contain a valid MAC (Message Authentication Code) and sequence number components to authenticate the network. The UE responded with an Authentication Failure message, explicitly citing "Non-5G authentication unacceptable" (cause value #22 from TS 24.501). This rejection aligns with 3GPP security requirements (TS 33.501), which mandate that UEs must validate AUTN to prevent connection to untrusted networks. By detecting the invalid AUTN and terminating the procedure—rather than proceeding with key derivation or encryption setup—the UE correctly enforced network authentication, mitigating risks like fake base station (IMSI catcher) attacks. Its compliance with the standard ensures no sensitive data (e.g., SUPI) was exposed before network legitimacy was verified. Secure

16	16	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3200 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 5G-IA7 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.11983895301818848 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12023711204528809 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response after completing 5G-AKA authentication. The AMF then responded with a Security Mode Command (SMC) to activate ciphering and integrity protection for subsequent NAS messages. Critically, the AMF transmitted this SMC as a **plain/unprotected NAS message** (security header type 0), with no integrity protection or encryption applied, despite specifying security algorithms (128-5G-EA1 for ciphering, 5G-IA7 for integrity). The UE provided no response to this SMC. According to 3GPP 5G security standards (TS 33.501, Section 6.7), the Security Mode Command **must always be integrity-protected** to prevent tampering, as it establishes the security algorithms and keys for the session. Transmitting it unprotected violates a core security requirement, as an attacker could modify the message (e.g., downgrade algorithms or inject malicious parameters). The UE's lack of response—failing to reject the unprotected SMC with a *Security Mode Reject* message (e.g., with cause #98, "Message not compatible with protocol state")—indicates it accepted an insecure command that bypassed mandatory integrity validation. This non-compliance exposes the UE to man-in-the-middle attacks where security settings could be compromised. Insecure
17	17	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.35177087783813477 UE to AMF UplinkNASTransport, Authentication response 0.35199785232543945 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response message to the AMF as part of the 5G-AKA procedure, which had not yet completed. Since 5G-AKA was unfinished, no security context (including encryption/integrity keys) was established, leaving NAS messages unprotected. The AMF responded with a Service Reject message (5GMM Cause 111: "Protocol error, unspecified"), sent in plain text, and the UE provided no further response. According to 3GPP TS 24.501 and TS 33.501, NAS messages exchanged before security activation—including Service Reject—may be sent unprotected if the AMF encounters an error during authentication setup. The UE's lack of response aligns with standard behavior, as Service Reject terminates the NAS signaling connection, requiring no acknowledgment or action from the UE. While this scenario exposes a protocol-level vulnerability to spoofed rejections (a known DoS risk in pre-security phases), the UE's adherence to standard procedures—accepting the unprotected reject and terminating silently—is itself compliant and does not constitute an insecure deviation. The insecurity arises from the protocol's inherent limitations, not the UE's implementation. Secure

18	18	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 4.243709087371826 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 4.243997097015381 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Identity request 4.445895195007324 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response, followed by the AMF requesting the SUCI via an Identity Request sent in plaintext. The UE complied by providing an Identity Response containing the SUCI, also in plaintext. According to 3GPP standards (TS 33.501), NAS messages exchanged before the completion of 5G-AKA lack encryption and integrity protection, as a security context has not yet been established. The SUCI is explicitly designed to protect the user's permanent identifier (SUPI) when transmitted without security, as it uses elliptic curve encryption to conceal the SUPI. Thus, the UE's transmission of the SUCI in plaintext at this stage aligns with the protocol's security design, which anticipates unprotected initial identity transfers. The action is permissible because the UE responded to a valid network request with the appropriate concealed identity, avoiding SUPI exposure, and no security context existed to enforce encryption. Secure
19	19	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11986708641052246 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12012410163879395 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3239710330963135 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA authentication, after which the UE sent an Authentication Response. The AMF then sent a Security Mode Command (SMC) protected with integrity (using 128-5G-IA2) but proposing null ciphering (5G-EA0). The UE responded with a Security Mode Reject (unspecified cause), rejecting the security configuration. According to 3GPP standards (TS 33.501), while null ciphering (5G-EA0) is permitted in limited scenarios (e.g., emergency services), its use for general NAS signaling is discouraged due to the lack of confidentiality. The UE's rejection of this proposal demonstrates adherence to security best practices by refusing to disable encryption, thereby preventing potential eavesdropping or data exposure. Although the rejection cause was unspecified, the decision aligns with the standard's emphasis on robust protection, indicating the UE enforced a secure policy by mandating encryption. Secure

20	20	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 2f4b62abf69d8352398c608fb3a89563 AUTN: 062d8ab6b7549000811f4ee8b8da8440 ngKSI_TSC: Native security context ngKSI_KSI: 6 UE provided: Authentication response The packet capture during the test using wireshark is: 1.9198977947235107 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Authentication response 1.9201328754425049 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.120612859725952 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an initial Authentication Response to the AMF. The AMF then responded with a Downlink Authentication Request containing RAND (2f4b62abf69d8352398c608fb3a89563), AUTN (062d8ab6b7549000811f4ee8b8da8440), and ABBA (3030), explicitly marked as sent in plain text. The UE subsequently sent another Authentication Response. Crucially, 5G-AKA authentication had not been completed at any point during this exchange, as confirmed by the test summary. According to 3GPP standards (TS 33.501), NAS messages—including Authentication Request/Response—must remain unencrypted until 5G-AKA successfully establishes a security context. Since no keys were derived (due to incomplete authentication), encryption was neither required nor expected. The UE correctly processed the plaintext Authentication Request and responded in plaintext, adhering to protocol mandates. No deviation or premature encryption attempt was observed. Secure

21	21	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 303030303030300078d431f251560000 AUTN: 4953cc15a85a90008f0a1f4e8f0a3310 ngKSI_TSC: Native security context ngKSI_KSI: 4 UE provided: Authentication failure (MAC failure) The packet capture during the test using wireshark is: 1.8795151710510254 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, Authentication response 1.8797390460968018 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.0836050510406494 UE to AMF UplinkNASTransport, Authentication failure (MAC failure) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF. The AMF then responded with a Downlink NAS Transport containing an Authentication Request, which included RAND and AUTN values for 5G-AKA authentication. This message was sent in plaintext, as no security context had been established yet. Upon receiving the request, the UE detected a MAC (Message Authentication Code) failure during AUTN verification, indicating the authentication parameters were invalid or tampered with. The UE then correctly sent an Authentication Failure message (with explicit "MAC failure" cause) to abort the procedure instead of proceeding. This aligns with 3GPP TS 33.501 security standards, which mandate that UEs must reject authentication if AUTN validation fails—a critical safeguard against spoofed network attacks. The UE's refusal to process the flawed AUTN and its explicit error reporting demonstrate compliant security behavior. Secure

22	22	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3200 RAND: 303030303030300078b457a1d8550000 AUTN: 313131313131313310057a1d8550000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.11977601051330566 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999082565307617 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.3230268955230713 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF. The AMF then responded with a plaintext Downlink NAS Transport message containing an Authentication Request, which included the parameters RAND, AUTN, ABBA, and ngKSI. Since 5G-AKA authentication had not yet been completed, encryption was not applied to this message as per the 5G standard. Upon receiving the request, the UE analyzed the AUTN (Authentication Token) and determined it was incompatible with 5G authentication requirements—likely because the AUTN structure or AMF field indicated a legacy (non-5G) authentication method like EPS-AKA. The UE correctly rejected this by sending an Authentication Failure message with the standardized cause value "Non-5G authentication unacceptable" (cause #26 per 3GPP TS 24.501), refusing to proceed with non-compliant authentication. This behavior aligns with 3GPP security standards (TS 33.501), which mandate that UEs must only accept 5G-compatible AUTN to prevent downgrade attacks and ensure robust authentication. The UE's adherence to protocol by validating the AUTN and explicitly rejecting non-5G methods demonstrates secure implementation. Secure

23	23	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11994004249572754 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12018203735351562 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.32151198387145996 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Authentication Response after completing 5G-AKA authentication. The AMF then sent a Security Mode Command (SMC) protected with integrity (security header type 3) using the 128-5G-IA2 algorithm but specified null ciphering (5G-EA0), meaning no encryption would be applied to subsequent communications. The UE rejected this configuration with a Security Mode Reject message, citing an unspecified cause. According to 3GPP standards (TS 33.501), while 5G-EA0 is a mandatory-supported algorithm, its use is explicitly discouraged for non-emergency services due to the absence of confidentiality. By rejecting the SMC, the UE refused to operate without encryption, thereby enforcing a higher security posture that prevents potential eavesdropping on sensitive NAS messages. This aligns with security best practices and demonstrates the UE's adherence to confidentiality requirements beyond minimal compliance. Secure

24	24	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 5781adc4c6cd42baaf6e4fe6cef2e17f AUTN: 67373384aeb990006bc203d2c023b868 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication response The packet capture during the test using wireshark is: 0.11973094940185547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12026000022888184 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.32166409492492676 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unsolicited Authentication Response uplink message (0.11973094940185547) without having received an initial Authentication Request from the AMF. Subsequently, the AMF sent a Downlink Authentication Request (0.12026000022888184) containing RAND, AUTN, and other parameters in plaintext, as 5G-AKA was incomplete and no security context existed. The UE then responded with another Authentication Response uplink (0.32166409492492676). According to 3GPP standards (TS 33.501), the 5G-AKA procedure mandates that the network (AMF) must initiate authentication by sending the first Authentication Request; the UE should never transmit an Authentication Response without first receiving and validating this request. The UE's premature Authentication Response violates this sequence, indicating non-compliant behavior that could expose the system to replay attacks or unauthorized state manipulation, as the unsolicited message might reflect mishandled authentication state or residual data from prior sessions. Insecure
25	25	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 1.3825318813323975 UE to AMF UplinkNASTransport, Authentication response 1.3827719688415527 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication reject 1.3827838897705078 UE to AMF SACK (Ack=2, Arwnd=106469) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, expecting to continue the 5G-AKA procedure. However, the AMF responded with an Authentication Reject message sent in plaintext, as 5G-AKA was incomplete and no security context existed for encryption. Instead of halting further NAS communication as mandated by 3GPP TS 33.501 upon receiving Authentication Reject, the UE immediately sent a Deregistration Request. This action violates the 5G security standard, which requires the UE to treat the authentication failure as terminal for the current session, invalidate stored security parameters (e.g., 5G-GUTI, TAI list), and refrain from initiating new NAS signaling until USIM removal or device restart. By proceeding with deregistration, the UE ignored the rejection's finality, potentially exposing itself to malicious AMF impersonation or state manipulation attacks, as subsequent messages lacked cryptographic protection. Insecure

26	26	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15973997116088867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15994787216186523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.3668229579925537 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure context between the UE and the AMF. The UE sent a Security Mode Complete message, confirming activation of negotiated security algorithms for integrity protection and ciphering. Subsequently, the AMF transmitted a protected Deregistration Request (security header type 2: integrity-protected and ciphered), which the UE acknowledged with a Deregistration Accept. According to 3GPP TS 33.501, after Security Mode Complete, all subsequent NAS messages—including Deregistration Accept—must be protected using the established security context to ensure integrity and confidentiality. However, the test summary explicitly notes the AMF's Deregistration Request as protected but omits any mention of protection for the UE's Deregistration Accept. This omission, coupled with the absence of security header details for the Deregistration Accept in the packet capture description, indicates the UE failed to apply mandatory protection to its response. This violates 3GPP standards, as unprotected NAS messages post-security activation expose the system to forgery or manipulation attacks. Insecure
27	27	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.1597728729248047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16001200675964355 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.36782288551330566 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication and NAS security mode procedures, the UE sent a Security Mode Complete message to the AMF, confirming the activation of NAS security. The AMF then sent a protected Deregistration Request (UE-terminated), which was integrity-protected and ciphered (security header type 2) in accordance with 5G standards. The UE responded with a Deregistration Accept message. However, the UE failed to protect this Deregistration Accept message with integrity protection or ciphering, despite the established security context. According to 3GPP TS 24.501 and TS 33.501, after security activation (post–Security Mode Complete), all subsequent NAS messages—including Deregistration Accept—must be both integrity-protected and ciphered to prevent tampering and eavesdropping. The UE's omission of these protections violates 5G security requirements, exposing the message to potential manipulation or interception. Insecure

28	28	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16000795364379883 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602778434753418 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36232805252075195 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message after 5G-AKA authentication, indicating readiness for secured communication. The AMF then sent a Security Mode Command protected with the new security context (header type 3), specifying ciphering algorithm 128-5G-EA2 but selecting null integrity protection (5G-IA0). The UE rejected this configuration with a Security Mode Reject (unspecified reason). According to 3GPP TS 33.501, null integrity (5G-IA0) is explicitly prohibited for NAS signaling after successful authentication (5G-AKA completion), as it leaves messages vulnerable to tampering. The UE correctly identified this violation of the 5G security standard, which mandates integrity protection for all NAS messages post-authentication to ensure message authenticity and integrity. By rejecting the insecure null integrity algorithm, the UE adhered to 3GPP security requirements and prevented potential downgrade attacks. Secure

29	29	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.15992307662963867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016101837158203 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36194396018981934 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA authentication, establishing a security context. The UE then sent an unprotected Security Mode Complete message, followed by the AMF transmitting a Security Mode Command marked as "Integrity protected with new security context" but proposing null algorithms for both ciphering (5G-EA0) and integrity (5G-IA0). The UE rejected this command with a Security Mode Reject (cause: "unspecified"). According to 3GPP standards (TS 33.501), UEs must reject null algorithm configurations (5G-EA0 + 5G-IA0) for NAS security because they provide no encryption or integrity protection, violating mandatory security requirements. The UE's rejection aligns with this directive, as accepting such a proposal would have left subsequent communications entirely unprotected. By enforcing the standard's security policies, the UE demonstrated correct behavior. Secure

30	30	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF began with the completion of 5G-AKA authentication, establishing a security context. However, the UE prematurely sent a **Security Mode Complete** message (at 0.160s) *before* receiving the AMF's **Security Mode Command** (sent at 0.160s but processed afterward). The AMF's command, protected with integrity using 128-5G-IA2, specified ciphering via 5G-EA7 and included ABBA parameters. The UE later sent another **Security Mode Complete** (at 0.365s) after processing the command. This sequence violates the 5G security protocol (3GPP TS 33.501), which mandates that the UE must *always* wait for the AMF's **Security Mode Command** to activate security (integrity and ciphering) before sending **Security Mode Complete**. By transmitting the first **Security Mode Complete** unprotected and out-of-order, the UE exposed sensitive data (e.g., the embedded Registration Request) and disregarded the standardized handshake. This could allow attackers to intercept or manipulate unprotected NAS messages, bypassing security activation. **Insecure**

31	31	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.1600170135498047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16026687622070312 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36418795585632324 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the completion of 5G-AKA, establishing a security context. The UE then unexpectedly sent a Security Mode Complete message without having first received a Security Mode Command from the AMF. Subsequently, the AMF transmitted a Security Mode Command, which was marked as "protected" (security header type 3, indicating integrity protection with a new context) but specified a null integrity algorithm (5G-IA0) and the 5G-EA4 ciphering algorithm. The UE did not reject this command and proceeded to send a Deregistration Request. According to 3GPP TS 33.501, the initial Security Mode Command must activate both integrity and ciphering protection, and null integrity (5G-IA0) is explicitly prohibited for non-emergency sessions after 5G-AKA, as it leaves messages vulnerable to tampering. By accepting this invalid configuration and continuing communication, the UE violated the standard's security requirements. Insecure

32	32	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.1595141887664795 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15984320640563965 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF deviates from the 3GPP 5G security protocol. After 5G-AKA completion, the UE initiated an uplink message containing both a Security Mode Complete and a Registration Request. Subsequently, the AMF sent a protected Security Mode Command (integrity-protected and ciphered using header type 2), which the UE did not acknowledge or process. This sequence violates the 3GPP standard (TS 33.501), where the Security Mode Command must be sent by the network *before* the UE responds with Security Mode Complete to activate NAS security. The UE's premature Security Mode Complete—sent without having received the Security Mode Command—bypasses critical security activation steps. Furthermore, the UE's failure to respond to the AMF's valid Security Mode Command indicates non-compliance with protocol requirements, leaving subsequent communications without established cryptographic protection. This behavior exposes the UE to security risks, such as accepting unprotected or maliciously injected NAS messages, and fails to enforce mutual security activation. Insecure
33	33	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 6 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.16021108627319336 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1606900691986084 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Illegal ME) 0.36391305923461914 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message, confirming successful completion of 5G-AKA and activation of NAS security. The AMF responded with a protected GMM Status message containing cause value 6 (Illegal ME), indicating a permanent error condition (e.g., ME blacklisting). Upon receiving this status, the UE initiated a UE-originating deregistration by sending a Deregistration Request. According to 3GPP TS 24.501, a GMM Status with cause #6 mandates the UE to abort ongoing procedures and trigger local deregistration, which aligns with the UE's response. Crucially, the AMF's GMM Status was sent as "Protected" (encrypted and integrity-protected), leveraging the established 5G-AKA security context, and the UE's subsequent Deregistration Request—while not explicitly marked as protected in the trace—must be secured per 5G standards after Security Mode Complete, as non-protected NAS messages are prohibited post-security activation unless initiating recovery. The UE correctly processed the protected error indication and responded with a standard-compliant deregistration action, demonstrating adherence to 3GPP security protocols. Secure

34	34	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15963101387023926 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15987801551818848 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.360584020614624 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing mutual authentication and security keys. The UE then sent an unprotected Security Mode Complete message, confirming activation of the security context. Subsequently, the AMF sent a protected Deregistration Request (integrity-protected and ciphered), initiating UE-terminated deregistration. The UE responded with a Deregistration Accept message. Critically, while the AMF's Deregistration Request was correctly protected (as mandated by 3GPP TS 33.501 after security context activation), the UE's Deregistration Accept was transmitted without security protection, as evidenced by the absence of security header notation (e.g., "Integrity protected and ciphered") in the packet capture and test summary. This violates the 5G standard, which requires all NAS messages post-security activation—including deregistration responses—to be both integrity-protected and encrypted to prevent forgery and eavesdropping. The UE's failure to protect this message exposes it to tampering or replay attacks, undermining session security. Insecure
35	35	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.15990018844604492 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16015410423278809 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an uplink message containing a Security Mode Complete, indicating successful activation of security algorithms after 5G-AKA authentication. This message was accompanied by a Registration Request, suggesting bundled NAS signaling. The AMF then responded with a protected Service Accept message, confirming service establishment with active security protection (integrity and encryption). The UE correctly refrained from responding to the Service Accept, as it is a terminating message in the NAS procedure per 3GPP TS 24.501. Crucially, the UE's Security Mode Complete message—sent after 5G-AKA completion—must be the first integrity-protected and encrypted NAS message under 3GPP TS 33.501. The absence of errors or fallback to plaintext, coupled with the UE's seamless transition to processing the AMF's protected Service Accept, confirms adherence to security protocols. No vulnerabilities (e.g., missing protection or improper validation) were observed in the UE's behavior. Secure

36	36	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5051651000976562 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5054340362548828 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7091829776763916 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message after successfully completing 5G-AKA authentication, establishing a NAS security context. The AMF then sent a protected Deregistration Request (security header type 2: integrity-protected and ciphered), indicating an active security context. The UE responded with a Deregistration Accept. According to 3GPP standards (TS 33.501), once a NAS security context is established, all subsequent NAS messages—including the Deregistration Accept—must be integrity-protected to prevent tampering and ensure authenticity. The test summary and packet capture explicitly noted the AMF's Deregistration Request as protected but did not indicate any security measures (integrity protection or ciphering) for the UE's Deregistration Accept message. This omission suggests the UE sent the Deregistration Accept without applying mandatory integrity protection, violating 3GPP security requirements and exposing the system to potential manipulation or spoofing attacks. Insecure
37	37	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5078079700469971 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080060958862305 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Service accept 0.7117960453033447 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure context between the UE and AMF. The UE sent a protected Registration Complete, and the AMF responded with a protected Service Accept, adhering to 5G security protocols. However, the UE then initiated a Deregistration Request (UE originating) immediately after receiving the Service Accept. According to 3GPP standards (TS 33.501), after 5G-AKA completion, all subsequent NAS messages—including Deregistration Request—must be protected (encrypted and integrity-protected) to prevent eavesdropping, spoofing, or tampering. The test summary explicitly noted the AMF's Service Accept as "Protected" but omitted this status for the UE's Deregistration Request, and the packet capture showed no indication of protection for this message. Since the UE sent this sensitive request without leveraging the established security context, it violated the 5G security mandate, exposing the message to potential attacks. Insecure

38	38	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.5716309547424316 UE to AMF UplinkNASTransport, Registration complete 0.5718338489532471 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message to the AMF, indicating the conclusion of initial NAS procedures. The AMF then responded with a Security Mode Command (SMC) message, which was integrity-protected using the new security context (as indicated by security header type 3) and specified the integrity algorithm 128-5G-IA2 and null ciphering (5G-EA0). This SMC message was sent shortly after the UE's Registration Complete, as confirmed by the packet capture. Critically, the UE did not generate any response to the SMC—neither a Security Mode Complete nor a Security Mode Reject—despite the completion of 5G-AKA, which established the necessary keys for security processing. According to 3GPP standards (TS 24.501, Section 5.4.1), upon receiving an SMC, the UE must always respond to confirm or reject the security configuration. A valid UE must verify the integrity of the SMC using the derived keys and, if accepted, activate the new security context and reply with Security Mode Complete. If integrity verification fails or parameters are unsupported, it must send Security Mode Reject. The absence of any UE response violates this protocol, leaving the security context unconfirmed and the connection in an ambiguous state. This deviation suggests the UE failed to process the SMC correctly, potentially due to implementation flaws in handling integrity verification or state transitions, undermining the security assurance mandated by 5G standards. Insecure
39	39	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.2683730125427246 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2686209678649902 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.476357936859131 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF began with the completion of 5G-AKA, establishing a secure NAS context. The UE sent a Registration Complete message, after which the AMF transmitted a Configuration Update Command protected with both integrity and ciphering (security header type 2), as required by 3GPP standards (TS 33.501) for post-authentication NAS messages. The UE responded with a Configuration Update Complete message. However, the test summary explicitly noted the AMF's downlink message as protected but omitted any mention of security protection for the UE's Configuration Update Complete. Given that 3GPP mandates all NAS messages after security context establishment to be integrity-protected and ciphered (to prevent tampering and eavesdropping), the absence of documented protection for the UE's response suggests a deviation from the standard. If the UE sent this message unprotected, it would expose the system to potential attacks like replay or manipulation, indicating a security lapse in the UE's implementation. Insecure

40	40	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.427475929260254 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.427738904953003 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.6314868927001953 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure context between the UE and AMF. The UE sent a Registration Complete message, followed by the AMF transmitting a protected Configuration Update Command (security header type 2, indicating integrity protection and ciphering as mandated by 3GPP standards after security context setup). The UE responded with a Configuration Update Complete message. However, the test summary and packet capture lack explicit confirmation that this uplink Configuration Update Complete message was protected (i.e., no security header type 2 is noted for it). According to 3GPP TS 33.501, after 5G-AKA, all subsequent NAS messages—including Configuration Update Complete—must be integrity-protected and ciphered to prevent tampering and eavesdropping. The absence of documented protection for the UE's response suggests non-compliance, as the UE failed to apply required security measures despite having an active security context. This omission exposes the message to potential manipulation or interception, violating 5G security protocols. Insecure

41	41	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0272 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 6.938914060592651 UE to AMF UplinkNASTransport, Registration complete 6.939129114151001 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Security mode command 7.142905950546265 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 7.143115997314453 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message after completing 5G-AKA authentication. The AMF then sent a Security Mode Command (SMC), protected with integrity using the new security context (security header type 3), specifying ciphering (128-5G-EA2) and integrity (128-5G-IA2) algorithms along with ABBA parameter 0272. Instead of responding with a Security Mode Complete or Reject message as mandated by 3GPP TS 24.501, the UE ignored the SMC and initiated a new Service Request via an InitialUEMessage. This premature Service Request was sent without completing the SMC procedure, leaving it unprotected (as InitialUEMessage occurs prior to NAS security activation). Consequently, the AMF rejected the request, indicating it could not derive the UE identity due to the unresolved security context. This action was **insecure** because the UE violated 5G NAS protocol requirements by failing to respond to the SMC before initiating new service requests. Per 3GPP standards, the SMC exchange must be conclusively completed (either accepted or rejected) to activate negotiated security algorithms and synchronize the security context between UE and AMF. Skipping this step exposes subsequent communications to potential integrity and confidentiality risks, undermines key hierarchy establishment, and causes protocol errors (e.g., the AMF's inability to identify the UE). The UE's deviation compromises the security activation sequence defined in 3GPP TS 33.501 and TS 24.501. Insecure
42	42	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.513239860534668 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5140058994293213 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5144908428192139 AMF to UE DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure NAS context. The UE then sent an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a protected Downlink NAS Transport message carrying a Configuration Update Command, followed by another protected Downlink NAS Transport message containing a Deregistration Accept (UE terminated). The UE provided no response to the Deregistration Accept message. According to 3GPP standards (TS 24.501), after 5G-AKA, all NAS messages must be integrity-protected and encrypted. The Deregistration Accept (UE terminated) is only valid if preceded by a Deregistration Request from the network, which is absent in this sequence. The UE should reject such an unsolicited Deregistration Accept as it is incompatible with the protocol state (UE is mid-session and expecting session-related responses). A secure UE must either ignore the message or respond with a 5GMM Status message indicating a protocol error (e.g., cause #98: "Message type not compatible with protocol state"). The UE's lack of reaction—no error indication, no state change, and no follow-up—suggests it insecurely accepted or ignored an invalid, unexpected protected message, violating standard handling procedures for anomalous network commands. Insecure

43	43	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5069518089294434 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5071558952331543 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5073068141937256 AMF to UE DownlinkNASTransport 0.7109389305114746 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE sent a protected Uplink NAS Transport containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a protected Downlink NAS Transport (Configuration Update Command, security header type 2). Instead of replying with a Configuration Update Complete or Reject as mandated by 3GPP TS 24.501, the UE initiated a UE-originating Deregistration Request approximately 200 ms later. This deregistration occurred without any intermediate NAS messages, indicating the UE terminated the session abruptly after receiving the protected command. Per 3GPP standards, a UE must process valid protected NAS messages (decrypt and verify integrity) and respond context-appropriately—either accepting/rejecting the update or handling integrity failures via standardized procedures (e.g., sending a 5GMM Status message with cause #96 for integrity failure). The UE's deregistration request deviates from this protocol. Since the Configuration Update Command was properly protected, the UE should have validated it using the established 5G-AKA keys. Deregistration without prior rejection or failure indication suggests either: (a) the UE failed to properly verify the message (e.g., ignored integrity checks), or (b) it implemented non-compliant error handling. Both scenarios violate 3GPP security requirements (TS 33.501), as they bypass mandated security checks or responses, potentially exposing the UE to exploitation (e.g., accepting malicious updates or suppressing legitimate network commands). Insecure
44	44	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 6.589772939682007 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.5903379917144775 AMF to UE SACK (Ack=18, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.590748071670532 AMF to UE DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 6.793751955032349 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a UL NAS Transport message containing Registration Complete and a PDU Session Establishment Request, following the completion of 5G-AKA authentication. The AMF responded with a Configuration Update Command and then a Deregistration Request (UE-terminated), which was explicitly noted as protected with both integrity and ciphering (security header type 2). The UE replied with a Deregistration Accept message. According to 3GPP standards (TS 33.501), after 5G-AKA establishes a security context, all subsequent NAS messages—including Deregistration Accept—must be protected with both integrity and encryption to prevent forgery or eavesdropping. The test summary confirmed the AMF's Deregistration Request was protected but omitted any mention of security headers for the UE's Deregistration Accept. Given that the test focused on UE security and deliberately highlighted protection status for the AMF's message, the absence of such detail for the UE's response implies it was sent unprotected. This violates 3GPP requirements, as an unprotected Deregistration Accept could be exploited by attackers to confirm deregistration or infer network activity. Insecure

45	45	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5155510902404785 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5157649517059326 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5159080028533936 AMF to UE DownlinkNASTransport, Configuration update command 0.7195420265197754 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure context between the UE and AMF. The UE then sent an Uplink NAS Transport (including Registration Complete and a PDU Session Establishment Request), followed by the AMF sending a protected Configuration Update Command—integrity-protected and ciphered per the security header type (2). The UE responded appropriately with a Configuration Update Complete message. According to 3GPP standards (TS 33.501), once 5G-AKA completes, all subsequent NAS messages must be integrity-protected, and sensitive messages must be ciphered. The AMF's Configuration Update Command adhered to this by employing both protections, and the UE correctly processed it only after successful verification and decryption, as evidenced by its valid response. This indicates the UE enforced mandatory security checks, rejecting any unverified or tampered messages. No deviation from the standard was observed in the UE's behavior. Secure
46	46	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.425251007080078 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4254679679870605 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4255969524383545 AMF to UE DownlinkNASTransport, Configuration update command 2.629240036010742 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing mutual authentication and security keys. The UE then sent a protected UL NAS TRANSPORT message (including Registration Complete and a PDU Session Establishment Request). The AMF responded with a Configuration Update Command, which was correctly protected with both integrity and ciphering (security header type 2) as mandated by 3GPP TS 33.501 for NAS messages post-authentication. The UE processed this command and replied with a Configuration Update Complete. Crucially, the UE validated the integrity and deciphered the AMF's protected command before responding, and its own Configuration Update Complete message would inherently require protection under the active security context (per TS 24.501). No deviations from security protocols—such as accepting unprotected downlink NAS messages or sending unprotected uplink messages—were observed. The UE adhered to 5G security standards by enforcing protection on all post-authentication NAS exchanges. Secure

47	47	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.4281399250030518 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4283440113067627 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.428462028503418 AMF to UE DownlinkNASTransport, Configuration update command 2.6321370601654053 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an UL NAS TRANSPORT message (including Registration Complete and PDU Session Establishment Request) after successful 5G-AKA authentication. The AMF then responded with a protected Configuration Update Command (security header type 2: integrity-protected and ciphered), which was transmitted twice in quick succession. The UE acknowledged this by sending a Configuration Update Complete message. According to 3GPP standards (TS 33.501), once 5G-AKA completes, all subsequent NAS messages must be protected with both integrity and ciphering to prevent eavesdropping or tampering. The AMF correctly protected its downlink message, and the UE appropriately processed it—only responding after verifying integrity and decrypting the command. Crucially, the UE's Configuration Update Complete response would inherently be protected under the established security context (as non-protected NAS messages are rejected post-5G-AKA), indicating adherence to security protocols. No evidence suggests the UE accepted unprotected commands or bypassed security checks. Secure

48	48	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3200 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 2.4352028369903564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4353890419006348 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.435595989227295 AMF to UE DownlinkNASTransport, Security mode command 2.6392359733581543 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport containing Registration Complete and a PDU Session Establishment Request after successful 5G-AKA authentication. The AMF responded with a Configuration Update Command and a Security Mode Command (SMC) protected with a new security context (integrity protected), specifying ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA2. The UE rejected the SMC with a "Security mode rejected, unspecified" message. According to 3GPP TS 33.501, 5G-EA4 is not a standardized ciphering algorithm (valid algorithms are 5G-EA0 to 5G-EA3), and UEs must only accept standardized algorithms to maintain security. The UE's rejection aligns with 5G security requirements, as using an undefined algorithm like 5G-EA4 could compromise confidentiality. The integrity algorithm 128-5G-IA2 was valid, but the invalid cipher justified rejection. The UE correctly operated within the standard by refusing an unsupported security configuration. Secure

49	49	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 17.321523904800415 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.322353839874268 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Security mode command 17.532354831695557 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request via an InitialUEMessage to initiate communication. The AMF responded with a Security Mode Command (SMC) protected with integrity using the new security context (security header type 3), specifying the null cipher algorithm (5G-EA0) for encryption and 128-5G-IA2 for integrity. The UE rejected this command with a Security Mode Reject, citing an unspecified cause. According to 3GPP standards (TS 33.501), the use of 5G-EA0 (null cipher) disables encryption, leaving user data and sensitive signaling exposed to eavesdropping, which is permissible only in exceptional scenarios like emergency services. The UE's rejection of the null cipher—despite supporting the mandatory integrity algorithm (128-5G-IA2)—demonstrates adherence to security best practices by refusing to operate without encryption. This behavior aligns with the standard's emphasis on robust protection, as null cipher undermines confidentiality. The UE's action is secure because it prioritizes defense against passive attacks, consistent with 3GPP's security objectives. Secure
50	50	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 24.788990020751953 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 24.789222955703735 AMF to UE SACK (Ack=27, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating a Service Request for mobile-originated data after completing 5G-AKA, establishing a valid security context. The AMF responded with a protected Deregistration Accept message (UE-terminated), which was integrity-protected and encrypted as confirmed by the test setup. According to 3GPP TS 24.501, upon receiving a protected Deregistration Accept, the UE must silently deregister without sending any response, as the message's integrity protection validates its authenticity. The UE's lack of response aligns precisely with this requirement, demonstrating proper verification of the protected NAS message and adherence to security protocols. No anomalous behavior or protocol violations were observed. Secure

51	51	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 25.642455101013184 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 25.642899990081787 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Message type not compatible with the protocol state) 25.85011601448059 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating communication by sending an unprotected Service Request via an InitialUEMessage. The AMF responded with a protected Deregistration Request (security header type 2: integrity-protected and ciphered), which the UE processed and acknowledged with a Deregistration Accept. Critically, the 5G-AKA had been completed beforehand, establishing a valid security context. According to 3GPP standards (TS 33.501), once security is activated, the UE must reject any unprotected NAS messages carrying sensitive parameters. However, the Deregistration Request—though sent in an unexpected protocol state (post-Service Request)—was correctly protected using the existing security context. The UE validated the message's integrity and deciphered it before responding, adhering to 5G security requirements that mandate protection for such mobility management messages. No evidence suggests the UE processed an unprotected sensitive message or bypassed security checks. The state mismatch noted ("Message type not compatible with the protocol state") relates to protocol logic, not a security violation, as the UE enforced cryptographic protection correctly. Secure
52	52	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 11.176167011260986 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 11.17656421661377 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command 11.383517980575562 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After the successful completion of 5G-AKA, establishing a security context, the UE sent a Service Request to initiate communication. The AMF responded with a protected Configuration Update Command (security header type 2: integrity-protected and ciphered), adhering to 3GPP security requirements for downlink NAS messages post-authentication. However, the UE subsequently sent a Deregistration Request (UE originating) without indicating any security protection in the test summary or packet capture. According to 3GPP standards (TS 33.501), once a security context is active—confirmed by the UE's prior processing of the protected downlink message—all subsequent NAS messages, including Deregistration Request, must be integrity-protected and ciphered (security header type 2) to prevent forgery or manipulation. The UE's failure to protect this message violates the mandatory security procedures, exposing it to potential attacks such as unauthorized session termination or spoofing. Insecure

53	53	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 17.000593185424805 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.001089096069336 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal UE) 17.204612970352173 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Service Request to the AMF, which is permissible as the initial message in a new connection. The AMF responded with a protected Deregistration Request (integrity-protected and ciphered) using security header type 2, indicating "Illegal UE" as the reason. The UE then replied with a Deregistration Accept message. Critically, the Deregistration Accept was sent without protection, as evidenced by the absence of security header notation in the packet capture and the lack of explicit mention of protection in the test summary. According to 3GPP standards (TS 24.501), after 5G-AKA completes and establishes a NAS security context, all subsequent NAS messages—including Deregistration Accept—must be both integrity-protected and ciphered to prevent tampering and eavesdropping. The UE's failure to protect this message violates the 5G security protocol, exposing it to potential attacks such as forgery or interception. Insecure
54	54	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 100 UE provided: No response The packet capture during the test using wireshark is: 1.321023941040039 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.3216829299926758 AMF to UE DownlinkNASTransport, 5GMM status (Conditional IE error) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a protected Service Request to the AMF after successful 5G-AKA authentication, indicating an established security context. The AMF responded with a protected DownlinkNASTransport message containing a 5GMM status with cause #100 ("Conditional IE error"), signaling an issue with conditional information elements. The UE provided no response to this message. According to 3GPP TS 24.501, the 5GMM status message (especially with cause #100) does not require a NAS-level response from the UE; it is designed to terminate the ongoing procedure without further action. The UE correctly adhered to protocol specifications by not generating a response, avoiding unnecessary exposure or processing of erroneous conditions. Both messages were protected per 5G security requirements, leveraging the established keys from 5G-AKA to ensure confidentiality and integrity. The UE's silence aligns with standard-mandated behavior for handling this error cause, demonstrating protocol-compliant security. Secure

55	55	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003898143768310547 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an InitialUEMessage containing a Registration Request to the AMF over an unsecured NAS connection, as 5G-AKA authentication had not yet been initiated. The AMF responded with a DownlinkNASTransport message containing an Authentication Reject, sent in plaintext due to the absence of an established security context. The UE exhibited no further communication after receiving the reject message, consistent with 3GPP TS 24.501 requirements. According to 5G standards (3GPP TS 33.501), NAS messages prior to authentication completion must be unprotected, as encryption keys are derived during 5G-AKA. The UE's lack of response aligns with protocol specifications, which mandate that UEs silently discard the security context and cease communication attempts upon Authentication Reject without sending acknowledgments or retries. This prevents potential amplification attacks or state synchronization issues. While the plaintext transmission is inherently vulnerable to eavesdropping, this is an expected behavior in the pre-authentication phase, and the UE's adherence to protocol termination procedures mitigates further exposure. Secure
56	56	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00040602684020996094 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The UE initiated communication by sending an Initial Registration Request in plaintext, as expected before 5G-AKA completion. The AMF responded with an Authentication Reject message, also sent in plaintext due to the absence of an established security context. According to 3GPP standards (TS 24.501 and TS 33.501), NAS messages prior to authentication are unprotected, and an Authentication Reject terminates the registration procedure without requiring a UE response. The UE correctly abstained from further communication, avoiding unnecessary exposure of credentials or signaling. This aligns with protocol specifications, as responding could risk session fixation or resource exhaustion attacks. Thus, the UE's silent termination upon receiving the unencrypted reject was the secure, standards-compliant action. Secure

57	57	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003440380096435547 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request via an InitialUEMessage (plaintext, as no security context existed). The AMF responded immediately with a DownlinkNASTransport containing an Authentication Reject message, also sent in plaintext. The UE provided no response to this rejection. According to 3GPP standards (TS 24.501), an Authentication Reject must be handled by the UE deleting any stored security context, entering a DEREGISTERED state, and treating the USIM as invalid for 5G services until rebooted or reinserted. Crucially, the UE **must not** respond to this message to prevent signaling storms or security vulnerabilities, as no valid security context exists post-reject. Here, the UE's lack of response aligns with the standard, demonstrating proper termination of the session without exposing vulnerabilities. The plaintext transmission is acceptable at this stage since 5G-AKA—mandatory for activating NAS security—was never completed. Thus, the UE acted securely by adhering to protocol-mandated silence. Secure
58	58	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003209114074707031 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request in plaintext, as 5G-AKA had not yet been completed to establish a security context. The AMF responded with an Authentication Reject message, also sent in plaintext, to which the UE provided no further response. According to 3GPP standards (TS 33.501 and TS 24.501), NAS messages prior to 5G-AKA completion—including Authentication Reject—are inherently unprotected, as encryption/integrity protection requires keys derived from a successful authentication. The UE's lack of response aligns with protocol requirements: upon receiving Authentication Reject, the UE must abort the registration attempt, invalidate temporary credentials, and refrain from further communication until restart or reinitialization. This behavior prevents potential exploitation (e.g., forced de-synchronization or denial-of-service via forged rejections) by terminating the session without processing unprotected commands. Thus, the UE's compliance with protocol-specified termination constitutes secure behavior. Secure

59	59	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002620220184326172 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request via an InitialUEMessage, indicating mobile-originated signalling as the establishment cause. The AMF responded with a DownlinkNASTransport containing an Authentication Reject message, sent in plaintext since 5G-AKA authentication had not yet been completed. The UE exhibited no further communication after receiving this rejection. According to 3GPP standards (TS 24.501, TS 33.501), NAS messages prior to authentication completion lack encryption and integrity protection, making the plaintext transmission of the Authentication Reject acceptable. Crucially, upon receiving an Authentication Reject, the UE must: 1. Immediately halt all ongoing NAS procedures. 2. Delete stored security context (e.g., K~AMF~, 5G-GUTI). 3. Treat the current USIM as invalid for 5G until manual intervention (e.g., SIM restart). 4. Refrain from sending further NAS messages. The UE's lack of response aligns precisely with these requirements—it terminated communication without attempting retries or countermeasures. This prevents potential attack vectors like bidding-down or replay attacks during the vulnerable pre-authentication phase. By strictly adhering to protocol-mandated silence and context deletion, the UE mitigated risks associated with unauthenticated rejection messages. Insecure actions would include ignoring the reject (e.g., continuing registration attempts) or retaining compromised credentials. Here, the UE's behavior demonstrates compliant security posture. Secure
60	60	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003459453582763672 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The UE initiated the NAS communication by sending an Initial Registration Request in plain text, as 5G-AKA authentication had not yet been completed. The AMF responded with an Authentication Reject message, also sent in plain text due to the absence of an established security context. According to 3GPP TS 33.501, until 5G-AKA completes, NAS messages lack integrity protection and confidentiality, making plain-text transmission expected and compliant at this stage. Critically, the UE exhibited secure behavior by providing no response to the Authentication Reject. The 5G standard mandates that upon receiving this message, the UE must silently discard the rejection, invalidate its current security context (e.g., delete stored 5G-GUTI and related parameters), and refrain from sending any further NAS messages until reinitialization (e.g., reboot or SIM removal). The UE's lack of response aligns precisely with this protocol, preventing potential exploitation (e.g., signaling storms or state confusion) that could arise from unauthenticated interactions. Thus, the UE correctly prioritized security by adhering to standardized failure-handling procedures. Secure

61	61	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0004100799560546875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request via an InitialUEMessage, initiating the registration process. The AMF responded with a Registration Reject message containing 5GMM Cause #111 ("Protocol error, unspecified"), sent in plaintext without encryption or integrity protection. Since 5G-AKA authentication had not been completed, no security context existed between the UE and AMF, meaning NAS messages at this stage are expected to be unprotected per 3GPP standards (TS 33.501). The UE correctly provided no response to the reject message, as no further action is mandated by the standard upon receiving such a rejection during initial registration. The UE adhered to protocol by not transmitting sensitive data (e.g., permanent identifiers) before authentication and by avoiding unnecessary communication after rejection, which could expose it to bidding down attacks or manipulation. Secure
62	62	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.596633911132812 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.597079038619995 AMF to UE SACK (Ack=14, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating a Service Request (uplink) to establish communication for mobile-originated data, following successful 5G-AKA authentication. The AMF unexpectedly responded with a protected Deregistration Accept message (downlink), indicating network-initiated deregistration. According to 3GPP TS 24.501, upon receiving a protected Deregistration Accept (UE-terminated), the UE must accept deregistration without sending a response, as the procedure is completed by the network's message. The UE's lack of response aligns with this requirement. Since the message was integrity-protected and confidentiality-protected (as confirmed by the "Protected" status), the UE could verify its authenticity using established security contexts from 5G-AKA. The UE correctly trusted the protected NAS message, deregistered, and avoided unnecessary signaling—consistent with 5G security protocols. Secure

63	63	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0203 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.10306811332702637 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.10332202911376953 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3094031810760498 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF began with the completion of 5G-AKA, establishing mutual authentication. The UE sent an Authentication Response, after which the AMF transmitted a Security Mode Command (SMC) protected with integrity (security header type 3), specifying ciphering algorithm 128-5G-EA1 and integrity algorithm 128-5G-IA2. This SMC is a critical step to activate the new security context for subsequent protected communications. Instead of responding with the mandatory Security Mode Complete or Reject message as required by 3GPP TS 24.501 and TS 33.501, the UE sent a Deregistration Request without acknowledging or validating the SMC. This omission violates the 5G NAS protocol, as the UE must explicitly confirm the activation of the security context via Security Mode Complete to ensure synchronized security states between UE and network. Skipping this step leaves the security context unverified and risks inconsistent protection states, potentially exposing subsequent messages to manipulation or misinterpretation. Insecure
64	64	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.12326717376709 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.123653173446655 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request (uplink) to initiate mobile-originated data communication after successful 5G-AKA authentication. The AMF responded with a Service Accept message (downlink), which was sent as "Protected"—indicating it was integrity-protected and encrypted using the established 5G security context. The UE provided no subsequent response to this message. According to 3GPP standards (TS 24.501), a Service Accept message does not require a UE response upon successful reception and verification; it concludes the service establishment procedure. The UE's lack of response is expected behavior when the protected message passes integrity checks and is properly processed. Since the AMF's message was protected per 5G-AKA security activation, and the UE neither rejected the message nor exhibited anomalous follow-up actions (e.g., unnecessary re-authentication or connection drops), the UE operated securely within 5G protocols. The "Unknown code (0x45)" in the Wireshark trace is likely an artifact of encrypted payloads or decoding issues and does not indicate a security lapse, as the UE processed the valid Service Accept as intended. Secure

65	65	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.15958499908447266 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16092395782470703 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36401796340942383 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message, confirming successful completion of the preceding 5G-AKA authentication. The AMF then responded with a Security Mode Command, which was integrity-protected using the new security context (indicated by security header type 3) and specified ciphering (128-5G-EA2) and integrity (128-5G-IA1) algorithms. However, the UE rejected this command with a Security Mode Reject (unspecified cause), despite the AMF's message being protected according to standard post-authentication procedures. Per 3GPP standards (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages—including Security Mode Command—must be integrity-protected using the established keys. The UE's rejection of a properly protected Security Mode Command is non-compliant, as the standard mandates acceptance if the message verification passes (which it should, given successful 5G-AKA and correct security context). This rejection halts secure communication setup without justification, leaving the connection vulnerable and violating protocol requirements for maintaining security continuity after authentication. The UE's action undermines the security framework by failing to proceed with the secured context. Insecure

66	66	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0322 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 2.5863499641418457 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.5868079662323 AMF to UE SACK (Ack=9, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.5871849060058594 AMF to UE DownlinkNASTransport, Security mode command 2.7903499603271484 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Configuration Update Command and then a Security Mode Command (SMC). The SMC was integrity-protected using the new security context established during the completed 5G-AKA authentication, specifying ciphering algorithm 128-5G-EA1 (SNOW 3G) and integrity algorithm 128-5G-IA2 (AES). The UE rejected this command with a Security Mode Reject (unspecified cause). According to 3GPP TS 33.501, after 5G-AKA completes, the UE must verify the integrity of the SMC using the newly derived K~AMF~ key. A rejection implies the UE detected an integrity verification failure or invalid parameters (e.g., ABBA mismatch or unsupported algorithms). Since 128-5G-EA1 and 128-5G-IA2 are mandatory UE-supported algorithms per standards, the rejection likely indicates the UE identified a security anomaly—such as incorrect MAC verification or context mismatch—preventing activation of unverified security. This aligns with 3GPP security requirements to reject unverifiable or suspicious SMC messages, thereby protecting against security context downgrade or forgery attacks. Secure

67	67	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.8137481212615967 UE to AMF UplinkNASTransport, Service request 0.8142230510711167 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 1.0217480659484863 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request via an UplinkNASTransport message, indicating an attempt to resume services after 5G-AKA authentication had already established a security context. The AMF responded with a DownlinkNASTransport containing a 5GMM Status message (cause #98, "message type not compatible with protocol state"), which was explicitly noted as protected (encrypted and integrity-protected). The UE then replied with its own UplinkNASTransport carrying a 5GMM Status message (also cause #98), signaling that it deemed the AMF's message incompatible with its protocol state. According to 3GPP standards (TS 24.501), after 5G-AKA completes, all NAS messages must be integrity-protected and encrypted to prevent tampering or eavesdropping. The UE's response—a 5GMM Status message—was sent as a standard reaction to a protocol error, and crucially, it was transmitted within an UplinkNASTransport. Since the security context was active (5G-AKA completed), the UE would have applied encryption and integrity protection to this message by default, as non-protected NAS signaling is only permitted before security activation. The test summary did not indicate decryption failures or integrity violations at the AMF, implying the UE correctly enforced protection. Thus, the UE adhered to 5G security requirements by safeguarding its response. Secure
68	68	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.7269129753112793 UE to AMF UplinkNASTransport, Service request 0.7272160053253174 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.9349148273468018 UE to AMF UplinkNASTransport, Configuration update complete, UplinkNASTransport, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request after completing 5G-AKA, establishing a mutual security context. The AMF responded with a Configuration Update Command, which was protected with integrity (security header type 1) but not encrypted, as indicated by the security header value. The UE processed this command and replied with a Configuration Update Complete, followed by a Registration Request. According to 3GPP standards (TS 33.501), after 5G-AKA, NAS messages must be integrity-protected to prevent tampering, but encryption is optional and network-dependent. The UE correctly validated the integrity of the Configuration Update Command—ensuring it originated from a legitimate AMF—and responded appropriately. Since the standard permits non-encrypted downlink messages if integrity is verified, and the UE enforced this protection without accepting unprotected or tampered commands, its actions align with 5G security requirements. Secure

69	69	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3100 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11985111236572266 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12013506889343262 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3252840042114258 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA authentication, after which the UE sent an Authentication Response. The AMF then responded with a Security Mode Command, which was integrity-protected using the new security context (security header type 3), proposing the null ciphering algorithm (5G-EA0) for encryption and 128-5G-IA2 for integrity. The UE rejected this command with a Security Mode Reject message, citing an unspecified reason. According to 3GPP standards (TS 33.501), after successful authentication, the network must not select the null ciphering algorithm (5G-EA0) for NAS communication, as it offers no confidentiality protection and is only permitted in limited service states (e.g., emergency calls without authentication). Here, since 5G-AKA was completed, the UE is in a registered state, and the use of null ciphering violates the standard's security requirements. By rejecting the Security Mode Command, the UE prevented the establishment of an insecure connection without encryption, thereby adhering to 3GPP mandates that prioritize confidentiality for authenticated sessions. This action demonstrates the UE's compliance with security protocols by refusing a downgrade to null ciphering. Secure

70	70	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.547684907913208 UE to AMF UplinkNASTransport, Registration complete 0.5478739738464355 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message to the AMF after completing 5G-AKA authentication. The AMF responded with a Security Mode Command (SMC) protected using the new security context (security header type 4), specifying the integrity algorithm 128-5G-IA2 and the null ciphering algorithm 5G-EA0, with ABBA set to 0000. The SMC was marked as both integrity-protected and ciphered, but 5G-EA0 provides no actual encryption, leaving the message contents exposed. Critically, the UE provided no response—neither a Security Mode Complete nor a Security Mode Reject—despite protocol mandating one. This non-response violates 3GPP TS 24.501 § 4.4.6, which requires UEs to explicitly accept or reject SMC parameters to ensure unambiguous security context activation. The UE's failure to reject the null cipher (5G-EA0) when integrity was supported (128-5G-IA2) also contradicts standard security principles, as null encryption undermines confidentiality without justification (e.g., emergency services). Combined, the lack of protocol compliance and acceptance of a non-confidentiality-protected SMC demonstrates insecure behavior. Insecure

71	71	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0332 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 4.62968111038208 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 4.630121946334839 AMF to UE SACK (Ack=10, Arwnd=106361) , DownlinkNASTransport, Configuration update command 4.6305460929870605 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA authentication, establishing a shared security context between the UE and AMF. The UE then sent an Uplink NAS Transport message, after which the AMF responded with a Downlink NAS Transport containing a Security Mode Command (SMC). The SMC was marked as "Protected" (security header type 2), indicating it was both integrity-protected and ciphered. However, the SMC specified a NULL integrity algorithm (5G-IA0) and the 128-5G-EA3 ciphering algorithm. Critically, this SMC was sent after 5G-AKA but before security activation, meaning no valid security context existed to process a protected message. The UE provided no response to the SMC. According to 3GPP standards (TS 24.501 and TS 33.501), the SMC must be sent unprotected (security header type 0) when no prior NAS security context exists, as the keys derived during 5G-AKA are not yet active for NAS protection. Sending the SMC as "Protected" (type 2) without an established context violates this requirement, as the UE lacks the active algorithms and keys to validate or decipher the message. The UE's lack of response aligns with standard behavior: it discarded the unprocessable protected message rather than risking improper security activation or exposing vulnerabilities. This prevents potential exploitation (e.g., forced security downgrade or false context acceptance). While a Security Mode Reject (unprotected) could theoretically be sent, the UE's silence is a safe default when integrity checks are impossible due to the invalid protected format. Thus, the UE adhered to security principles by rejecting an improperly secured command. Secure

72	72	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 6.590965032577515 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.591464042663574 AMF to UE SACK (Ack=25, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.5918920040130615 AMF to UE DownlinkNASTransport, Security mode command 6.7950029373168945 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Configuration Update Command and then a Security Mode Command (SMC), which was integrity-protected using the new security context derived from the completed 5G-AKA authentication. The SMC specified ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA2 (both mandatory for 5G UEs per 3GPP TS 33.501) and included ABBA parameter 3300. Instead of accepting the SMC, the UE sent a Security Mode Reject with an "unspecified" cause (#111). The UE's action was **secure**. According to 3GPP standards, the UE should reject the SMC if integrity verification fails or if it cannot validate the security context. Given the SMC was protected with the new context and the UE rejected it despite supporting the mandatory algorithms, the rejection likely indicates an integrity check failure (e.g., due to incorrect key derivation, message tampering, or ABBA mismatch). This aligns with security requirements by preventing activation of an unverified context, which could expose NAS messages to manipulation. The unspecified cause does not undermine the security posture, as the standard permits rejection for integrity issues regardless of granular cause reporting. Secure

73	73	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1599750518798828 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602010726928711 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3605461120605469 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the completion of 5G-AKA, establishing an initial security context. The UE then sent an uplink Security Mode Complete message, indicating it had processed a prior Security Mode Command. Subsequently, the AMF transmitted a downlink Security Mode Command protected with integrity (using 128-5G-IA2) but with null ciphering (5G-EA0), under the new security context (security header type 3). The UE rejected this command with a Security Mode Reject (cause: "unspecified"). According to 3GPP standards (TS 33.501), after 5G-AKA completion, NAS security must be activated via a single Security Mode Command, after which the UE should not accept another Security Mode Command without a new authentication. Here, the AMF sent an unsolicited second Security Mode Command post-completion, violating the standard sequence. The UE correctly identified this anomalous request—potentially due to redundant security activation, mismatched algorithms (e.g., null ciphering), or invalid context—and rejected it. This aligns with security protocols, as processing such a command could compromise context integrity or enable downgrade attacks. The UE's rejection prevents potential exploitation of an invalid security procedure. Secure

74	74	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03b3 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11993098258972168 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12021493911743164 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3277699947357178 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Authentication Response after completing 5G-AKA, confirming mutual authentication and shared key derivation. The AMF then sent a Security Mode Command (SMC), protected with the new security context (security header type 3), specifying ciphering (128-5G-EA3) and integrity (128-5G-IA2) algorithms—both mandatory per 3GPP standards—along with ABBA parameter 03b3. The UE responded with a Security Mode Reject, citing an unspecified cause, thereby refusing to activate the security context. From a security perspective, the UE's rejection aligns with 3GPP security principles (TS 33.501) for several reasons. First, the SMC must be integrity-verified using the new security context keys derived during 5G-AKA. If verification fails (e.g., due to incorrect message authentication code, ABBA mismatch, or unsupported algorithms), rejection is mandatory to prevent security context activation under potentially compromised conditions. Although the AMF selected standardized algorithms, the UE's unspecified rejection suggests it detected an anomaly during verification—possibly an integrity check failure or parameter inconsistency—that it could not attribute to a specific cause. This behavior demonstrates adherence to the zero-trust principle: rejecting unverified or suspicious security commands, even post-authentication, is a critical safeguard against downgrade attacks or forced algorithm mismatches. While the cause "unspecified" limits diagnostic clarity, it is protocol-compliant and avoids exposing implementation details that could aid attackers. Thus, the UE prioritized security assurance over service continuity. Secure

75	75	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0392 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.4745960235595703 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4750940799713135 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.47630810737609863 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected UL NAS TRANSPORT message containing Registration Complete and a PDU Session Establishment Request. After 5G-AKA authentication completed, the AMF sent a Security Mode Command (SMC) protected with security header type 3 ("Integrity protected with new security context"), specifying ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA1. However, the UE provided no response to this SMC. According to 3GPP standards (TS 24.501, TS 33.501), upon receiving an SMC, a UE must always respond with either a Security Mode Complete or Security Mode Reject message to confirm or abort security activation. The absence of any response violates the mandatory handshake procedure, leaving the security context ambiguous and failing to establish protected communication. This omission could enable bidding-down attacks or leave subsequent messages unprotected, as the UE neither validated the AMF's security parameters nor activated the negotiated algorithms. Insecure
76	76	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.16002702713012695 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16026616096496582 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response as part of the ongoing 5G-AKA procedure. Before 5G-AKA could complete, the AMF sent a subsequent Downlink Identity Request message in plain text (unencrypted), explicitly requesting the UE's SUCI. The UE did not respond to this request. According to 3GPP standards (TS 33.501), after initiating 5G-AKA, sensitive NAS messages like Identity Request/Response must be integrity-protected and encrypted once a partial native security context exists. Since 5G-AKA was incomplete, no security context had been established, rendering the AMF's plaintext Identity Request non-compliant. The UE's lack of response aligns with security requirements, as transmitting the SUCI—a permanent identifier—in an unprotected message would expose it to eavesdropping or manipulation. The UE correctly prioritized confidentiality by withholding sensitive data until security activation, adhering to 3GPP mandates for preventing unprotected identity exchanges mid-authentication. Secure

77	77	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0004799365997314453 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20071196556091309 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request to the AMF in plaintext, as 5G-AKA authentication had not yet been completed. The AMF responded with an Identity Request (also in plaintext), explicitly asking for the SUCI (Subscription Concealed Identifier). The UE complied by sending an Identity Response containing the SUCI, transmitted without encryption. This sequence aligns with 3GPP standards (TS 33.501), which mandate that initial NAS messages—including identity transfers before authentication—remain unprotected because no security context exists. The SUCI itself is designed to protect the user's permanent identifier (SUPI) via public-key encryption, making its plaintext transmission acceptable. Since the UE only exposed the SUCI (not the SUPI) and adhered to the protocol's unsecured pre-authentication phase, its actions were standard-compliant and did not introduce unnecessary risk. Secure
78	78	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1600642204284668 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16033601760864258 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36293601989746094 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message alongside a Registration Request, despite not having received a Security Mode Command from the AMF first, which deviates from the 3GPP-specified sequence (TS 33.501, TS 24.501). After 5G-AKA completion, the AMF responded with a Security Mode Command protected with integrity (128-5G-IA2) but using null ciphering (5G-EA0). The UE rejected this command with a Security Mode Reject (cause: "unspecified"). The UE's premature Security Mode Complete—sent without a preceding command—violates protocol, as this message should only be a response to a valid Security Mode Command. This misstep could indicate an improper state transition or vulnerability to manipulation. While rejecting null ciphering aligns with security best practices (as 5G-EA0 offers no confidentiality), the unsolicited Security Mode Complete undermines the protocol's integrity, exposing potential flaws in the UE's implementation. Insecure

79	79	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1600358486175537 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16031789779663086 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36404991149902344 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response after completing 5G-AKA, establishing mutual authentication and shared keys. The AMF then sent a Security Mode Command (SMC) protected with integrity (using 128-5G-IA2) but explicitly selecting the null ciphering algorithm (5G-EA0), indicating no encryption for subsequent communications. The UE rejected this command with a Security Mode Reject (cause: "unspecified"), refusing to proceed under these security parameters. According to 3GPP standards (TS 33.501), the null cipher (5G-EA0) should only be used if no other mutually supported algorithms exist or for specific exceptions (e.g., emergency services). The UE's rejection aligns with security best practices, as accepting null ciphering would expose all future NAS messages to plaintext interception, violating confidentiality requirements. By rejecting the SMC, the UE prioritized security and avoided a downgrade to an insecure configuration, demonstrating compliant behavior. Secure
80	80	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.7228279113769531 UE to AMF UplinkNASTransport, Service request 0.723160982131958 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.9268310070037842 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request after completing 5G-AKA authentication, indicating an active security context. The AMF responded with a Configuration Update Command, which was integrity-protected using a new security context (security header type 3). However, the UE rejected this message by sending a 5GMM status with cause value "Message type not compatible with protocol state" (0x7), as it deemed the command inappropriate for its current state—likely during an ongoing Service Request procedure where only specific messages (e.g., Service Accept/Reject) are expected per 3GPP TS 24.501. This UE action aligns with 5G security standards: 1. **Protocol Compliance**: The UE correctly enforced state-specific message validity, preventing potential ambiguity or security risks from unsolicited commands during an active procedure. 2. **Security Context Handling**: The rejection occurred *after* verifying the message's integrity (security header type 3 confirms integrity protection was applied), ensuring the response was based on protocol logic, not a bypass of security checks. 3. **Error Signaling**: The 5GMM status explicitly signaled the error cause, allowing the network to rectify the issue, as mandated by standards. No evidence suggests the UE ignored security protections (e.g., it processed the integrity check before rejecting based on state). Thus, the UE adhered to 3GPP security requirements by prioritizing protocol state integrity. Secure

81	81	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 2222 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.1596660614013672 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1599440574645996 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Authentication Response after 5G-AKA completion, to which the AMF replied with a Downlink Security Mode Command (SMC). The AMF marked the SMC as "Integrity Protected" (security header type 1) but specified null algorithms (5G-IA0 for integrity and 5G-EA0 for ciphering), rendering the message effectively unprotected due to the absence of a valid MAC. According to 3GPP TS 33.501 and TS 24.501, the SMC must be integrity-protected using a non-null algorithm to prevent bidding-down attacks and ensure authenticity. The UE, upon receiving this malformed SMC (with conflicting header and algorithm indications), discarded it silently without responding. This aligns with 3GPP requirements (TS 24.501, section 5.4.1.2), which mandate discarding non-integrity-protected SMCs and avoiding responses to prevent state ambiguity or exploitation. By rejecting the invalid command implicitly, the UE maintained security posture. Secure

82	82	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0363 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1200721263885498 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12030816078186035 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3220691680908203 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response after completing 5G-AKA authentication. The AMF then sent a Security Mode Command (SMC) protected with security header type 3 (integrity protected with new context), specifying ciphering algorithm 128-5G-EA3 but integrity algorithm 5G-IA0 (null). The UE responded with a Security Mode Reject, citing "unspecified" rejection. Based on 3GPP standards (TS 33.501), the UE's rejection was **secure**. The standard prohibits using null integrity (5G-IA0) for non-emergency sessions, as it leaves NAS messages vulnerable to tampering. The AMF's SMC proposed null integrity despite the completed 5G-AKA (indicating a non-emergency session), violating the requirement that integrity protection must always be active. By rejecting this insecure configuration, the UE adhered to 5G security principles, preventing potential attacks on unverified NAS signaling. Secure
83	83	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 8.89320421218872 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.893432140350342 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating a Service Request via an InitialUEMessage (unprotected, as expected for initial NAS signaling during RRC establishment). The AMF responded with a Service Accept message, which was explicitly noted as "Protected" (indicating encryption and integrity protection via the established 5G-AKA security context). The UE provided no response to the Service Accept. According to 3GPP standards (TS 24.501), the Service Accept message concludes the service request procedure, and no UE acknowledgment or follow-up action is required. The UE's lack of response is thus compliant and expected behavior, as the procedure is complete upon AMF acceptance. The AMF's use of protection aligns with 5G security protocols, ensuring confidentiality and integrity for downlink communication post-authentication. No deviation from the standard or anomalous UE behavior was observed. Secure

84	84	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0083 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11982488632202148 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12009406089782715 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3228750228881836 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication and sending an Authentication Response. The AMF then sent a Security Mode Command (SMC), protected with integrity using the new security context (security header type 3), specifying ciphering algorithm 128-5G-EA2 and integrity algorithm 128-5G-IA2. The UE responded with a Security Mode Reject, citing an unspecified reason, instead of accepting the security setup. According to 3GPP standards (TS 33.501), after 5G-AKA completes, the UE must verify the integrity of the SMC using the newly established K~AMF~ key. A rejection is warranted only if the integrity check fails, the UE cannot support the mandated algorithms (both 128-5G-EA2 and 128-5G-IA2 are compulsory for 5G UEs), or parameters like ABBA are invalid. Given that the test-controlled AMF sent a valid SMC with standard-compliant algorithms and security header, the UE's unspecific rejection—without apparent justification—suggests either an integrity verification failure (indicating potential message tampering, which the UE correctly detected) or an erroneous rejection of valid parameters. In either case, rejecting an SMC that cannot be verified or processed aligns with security protocols, as accepting a compromised or unsupported configuration would be insecure. The UE's action thus demonstrates adherence to security principles by preventing potentially unsafe activation of security contexts. Secure

85	85	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16005301475524902 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16028904914855957 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36393094062805176 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA authentication, establishing a security context between the UE and AMF. Following this, the UE sent a Security Mode Complete message, indicating readiness for secured communication. The AMF then responded with a Security Mode Command message, which was integrity-protected but specified null algorithms for both ciphering (5G-EA0) and integrity (5G-IA0). This command, sent after 5G-AKA completion, effectively requested the UE to disable all NAS security protections. The UE rejected this command with a Security Mode Reject (unspecified), refusing to proceed without valid security algorithms. According to 3GPP standards (TS 33.501), after 5G-AKA succeeds, the network must activate integrity protection and should activate ciphering for NAS messages; proposing null algorithms post-authentication violates this requirement. The UE's rejection aligns with security best practices, as accepting null algorithms would expose subsequent communications to tampering and eavesdropping, undermining the established security context. Secure

86	86	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered (2) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15096688270568848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15124177932739258 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.35789990425109863 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF began after 5G-AKA completion, with the UE unexpectedly sending an initial **unprotected** Security Mode Complete message (including Registration Request) at 0.150966 seconds. This occurred *before* receiving any Security Mode Command from the AMF, violating the 3GPP standard sequence (TS 33.501, TS 24.501). The AMF then correctly sent a **protected** Security Mode Command (integrity-protected and ciphered) at 0.151241 seconds, specifying ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms. The UE responded with a second Security Mode Complete at 0.357899 seconds. The UE's premature transmission of the first Security Mode Complete—without network instruction, prior to security activation, and in an unprotected format—deviates from 5G security protocols. This could allow manipulation or interception of NAS messages, as control-plane security must be activated exclusively via AMF-initiated Security Mode Command after authentication. The action exposes the UE to downgrade or replay attacks by sending critical security-handshake messages in plaintext. Insecure

87	87	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7935822010040283 UE to AMF UplinkNASTransport, Service request 0.793781042098999 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.9976592063903809 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information), InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.9985220432281494 AMF to UE DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request to the AMF, indicating its intent to resume services. The AMF responded with a protected Deregistration Request (security header type 2, integrity-protected and ciphered), which should be secure post-5G-AKA authentication. However, the UE rejected this message by replying with a 5GMM status of "Invalid mandatory information" (cause value #32 per 3GPP TS 24.501), signaling a detected anomaly in the message's structure or content. The UE then reattempted a Service Request via an InitialUEMessage, but the AMF rejected it, citing undecipherable UE identity. Based on 5G standards, the UE's response was **secure**. The UE correctly processed the protected Deregistration Request (validating integrity and deciphering it first) before identifying invalid content—a mandatory security measure to prevent processing malformed or manipulated messages. The subsequent Service Request reinitiation aligns with standard recovery behavior, though the AMF's rejection was unrelated to UE security flaws. The UE adhered to protocols by challenging the suspicious message without compromising keys or context. Secure
88	88	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.1599421501159668 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1602020263671875 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request 0.36409711837768555 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response as part of the 5G-AKA procedure, which had not yet been completed. Subsequently, the AMF sent an Identity Request in plaintext (unencrypted), explicitly requesting the SUCI. The UE complied by providing an Identity Response containing the SUCI. Crucially, this exchange occurred before 5G-AKA authentication finalized, meaning no security context (encryption or integrity protection) was established for NAS messages at this stage. According to 3GPP standards (TS 33.501), the UE is permitted to send the SUCI in response to an unprotected Identity Request prior to authentication completion, as the SUCI itself is designed to protect the subscriber's permanent identifier (SUPI) via public-key encryption. This ensures the SUPI remains confidential even when transmitted without a security context. The UE's adherence to the AMF's request for SUCI in plaintext aligns with 3GPP protocols, as demanding encrypted communication before authentication would be infeasible. No deviation from the standard or premature exposure of sensitive data (like SUPI) occurred. Secure

89	89	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.12005400657653809 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12025594711303711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request 0.3216700553894043 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response as part of the 5G-AKA procedure, indicating an ongoing but incomplete authentication process. The AMF then responded with a plain-text Identity Request (unencrypted) demanding the UE's SUCI. The UE complied by sending an Identity Response containing the requested SUCI, also unencrypted. According to 3GPP standards (TS 33.501), NAS messages—including identity requests/responses—must be unprotected (plain) until 5G-AKA completes and a security context is established. Since 5G-AKA was not finalized at this stage, the UE's transmission of the SUCI in plain text was permissible and aligned with protocol requirements. The AMF-initiated identity request during an ongoing AKA is unusual but does not violate the standard, as networks can re-request identity if initial registration data is insufficient or expired. The UE's adherence to sending unprotected messages without an active security context demonstrates compliant behavior. Secure
90	90	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.11975502967834473 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999011039733887 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request 0.3266119956970215 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response as part of the 5G-AKA procedure. Before 5G-AKA completion (and thus prior to establishing a secured NAS context), the AMF sent an Identity Request in plaintext, explicitly requesting the SUCI. The UE complied by sending an Identity Response containing the SUCI, also in plaintext. According to 3GPP standards (TS 33.501), NAS messages exchanged before 5G-AKA completion lack encryption and integrity protection, making them vulnerable to eavesdropping or manipulation. However, the SUCI is designed to be transmitted unprotected, as it conceals the subscriber's permanent identifier (SUPI) using homomorphic encryption, rendering its exposure non-critical. The UE's response aligned with this allowance, as the SUCI is intended for initial unprotected transmission during registration. While the AMF's out-of-sequence Identity Request after the Authentication Response is atypical (typically occurring earlier in registration), the UE's action did not violate the standard by providing SUCI in plaintext at this stage, as no sensitive data was compromised. Secure

91	91	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7701981067657471 UE to AMF UplinkNASTransport, Service request 0.7708969116210938 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal UE) 0.9781770706176758 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a protected Service Request after successful 5G-AKA authentication, establishing a valid security context. The AMF responded with a protected (integrity-protected and ciphered) Deregistration Request, citing "Illegal UE" as the cause. Instead of processing the deregistration, the UE sent a 5GMM Status message with cause value "Invalid mandatory information," indicating it detected a protocol error in the AMF's message—likely an issue with a mandatory information element (IE) in the Deregistration Request, such as an unrecognized, malformed, or incorrectly valued IE. According to 3GPP TS 24.501, this response is standard when a UE encounters such errors, as it prioritizes protocol compliance over accepting potentially flawed commands. The UE maintained security by leveraging the established security context: it successfully verified the integrity and decrypted the AMF's message before identifying the error, and its 5GMM Status response would inherently be protected under the same context, ensuring confidentiality and integrity. This behavior aligns with 5G standards, as the UE properly validated security and adhered to protocol rules by rejecting invalid network instructions. Secure
92	92	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.7997009754180908 UE to AMF UplinkNASTransport, Service request 0.7998991012573242 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 1.0037281513214111 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request to the AMF after completing 5G-AKA authentication, establishing a security context. The AMF responded with a protected Deregistration Request (integrity-protected and ciphered, security header type 2), initiating UE-terminated deregistration. The UE then replied with a Deregistration Accept message. Crucially, the test summary and packet capture explicitly confirm the AMF's Deregistration Request was protected but omit any indication of security (integrity protection or ciphering) for the UE's Deregistration Accept. Per 3GPP standards (TS 33.501), once 5G-AKA completes, all subsequent NAS messages—including Deregistration Accept—must be integrity-protected to prevent tampering and ensure authenticity. The UE's failure to protect this message violates the mandatory security requirements, exposing it to potential forgery or replay attacks. Insecure

93	93	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 2222 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.15990400314331055 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16019105911254883 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3639252185821533 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message, indicating the prior completion of 5G-AKA. The AMF then sent a protected Security Mode Command (integrity-protected with the existing security context) proposing a new security context with 5G-EA4 for ciphering and **5G-IA0 (null integrity)** for integrity protection. The UE rejected this command with a Security Mode Reject, citing "UE security capabilities mismatch." According to 3GPP standards (TS 33.501), NAS signaling **must always maintain integrity protection**. The use of null integrity (5G-IA0) for NAS messages is explicitly prohibited, as it leaves control plane communications vulnerable to tampering. The UE correctly identified that the AMF's proposed configuration violated this requirement by attempting to disable integrity protection. By rejecting the command, the UE upheld the mandatory security principle that NAS integrity cannot be compromised, ensuring continued protection against forgery or replay attacks. This adherence to the standard demonstrates secure behavior. Secure
94	94	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00028896331787109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20491886138916016 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request in plaintext, as 5G-AKA had not yet been performed to establish a security context. The AMF responded with a plaintext Identity Request, explicitly asking for the SUCI. The UE then provided an Identity Response. According to 3GPP standards (TS 33.501), before 5G-AKA completion, NAS messages are unprotected, and the UE must only disclose the SUCI—not the SUPI—when responding to identity requests in unsecured states. Since the AMF requested SUCI specifically, and the UE responded with an identity (implied to be SUCI per standard compliance), this aligns with 5G security protocols. The UE avoided exposing sensitive credentials (SUPI) in plaintext, adhering to privacy safeguards. Secure

95	95	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.712475061416626 UE to AMF UplinkNASTransport, Service request 0.7131361961364746 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Message type not compatible with the protocol state) 0.9204661846160889 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE initiated communication by sending a Service Request to the AMF. The AMF unexpectedly responded with a protected Deregistration Request (integrity-protected and ciphered), which was incompatible with the current protocol state as the UE was awaiting service setup. Despite this anomaly, the UE processed the request and sent a Deregistration Accept. According to 3GPP standards (TS 24.501 and TS 33.501), once 5G-AKA establishes a security context, all subsequent NAS messages—including uplink transmissions like the Service Request and Deregistration Accept—must be integrity-protected and ciphered to prevent eavesdropping or tampering. The test summary explicitly confirms the downlink Deregistration Request was protected but omits security details for the UE's uplink messages. Given that 5G-AKA was completed and the UE successfully decrypted/verified the AMF's protected message (indicating active security context), the UE was obligated to protect its own messages. The lack of confirmation that the UE protected the Service Request or Deregistration Accept suggests a potential deviation from 3GPP security mandates, leaving the messages vulnerable. Insecure
96	96	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.039906978607177734 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04016995429992676 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2424759864807129 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an initial Identity Response, followed by the AMF issuing an Identity Request for SUCI (Subscription Concealed Identifier) in plaintext, as 5G-AKA authentication had not yet been completed. The UE then responded with a second Identity Response, also in plaintext. According to 3GPP standards (TS 33.501), before 5G-AKA establishes a security context, NAS messages—including Identity Requests and Responses—are permitted to be sent unprotected. Crucially, the UE's transmission of SUCI (a privacy-preserving identifier encrypted with the home network's public key) in plaintext is explicitly allowed and secure under the standard. This design ensures the permanent subscriber identifier (SUPI) remains concealed even when exchanged without encryption. The UE adhered to protocol by providing SUCI as requested, avoiding exposure of sensitive credentials. No deviation from the expected behavior occurred, as the plaintext exchange aligns with 5G's security architecture for pre-authentication identity handling. Secure

97	97	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03965497016906738 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0398409366607666 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24122309684753418 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF occurred before 5G-AKA authentication was completed, meaning no security context (encryption/integrity keys) existed. The UE initially sent an Identity Response. Subsequently, the AMF sent a plaintext Identity Request (as required by 3GPP when no security context is established), explicitly requesting a SUCI. The UE then provided another Identity Response containing the SUCI, also sent in plaintext. According to 3GPP standards (TS 33.501), initial NAS messages—including Identity Request/Response exchanges—are permitted in plaintext prior to authentication, as the SUCI itself cryptographically protects the user's permanent identifier (SUPI) via hybrid encryption with the home network's public key. This design ensures the SUPI remains confidential even when transmitted without NAS-layer encryption. The UE's compliance with sending the SUCI in plaintext during this pre-authentication phase aligns with 5G security protocols, as the SUCI's inherent protection mitigates risks of SUPI exposure. Secure
98	98	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.798314094543457 UE to AMF UplinkNASTransport, Service request 0.7985830307006836 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 1.0063400268554688 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure context between the UE and AMF. The UE initiated a Service Request, prompting the AMF to respond with a protected Configuration Update Command (security header type 3), indicating integrity protection and encryption using the newly established keys. However, the UE rejected this command by replying with a 5GMM status message (cause #96: "Message type not compatible with protocol state"), signaling that the Configuration Update Command was deemed invalid for its current operational state. From a security perspective, the UE's actions align with 3GPP standards (TS 24.501, TS 33.501). The UE correctly processed the AMF's protected message by decrypting and verifying its integrity, confirming the AMF's authenticity. The subsequent 5GMM status response was appropriate protocol behavior, as the UE identified an inconsistency in the message sequence (a Configuration Update Command should not follow a Service Request in this context). This rejection prevents potential state-machine exploits, such as forced reconfigurations during sensitive transitions. The UE maintained security by leveraging established keys for validation and adhering to protocol state rules, demonstrating robust security hygiene without compromising confidentiality or integrity. Secure

99	99	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.5202081203460693 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204141139984131 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE initiated a UL NAS TRANSPORT message containing a PDU session establishment request, which should be protected under the established NAS security context. The AMF responded with a SERVICE ACCEPT message, explicitly noted as "Protected," indicating proper encryption and integrity protection. The UE provided no response to this message, which aligns with 3GPP standards (TS 24.501), as SERVICE ACCEPT is a terminal downlink message that does not require an acknowledgment or follow-up action from the UE. The absence of a response is thus expected behavior. Both messages occurred post-authentication with activated security, ensuring confidentiality and integrity per 5G protocols. No deviation from the standard or unexpected UE actions were observed. Secure
100	100	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 92 UE provided: No response The packet capture during the test using wireshark is: 0.4685640335083008 UE to AMF UplinkNASTransport, Registration complete 0.4687800407409668 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Insufficient user-plane resources for the PDU session) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a secure NAS context. The UE then sent a Registration Complete message to the AMF, confirming registration finalization. In response, the AMF transmitted a protected DownlinkNASTransport message containing a 5GMM Status with Cause #92 ("Insufficient user-plane resources for the PDU session"), which was encrypted and integrity-protected per the active security context. The UE did not generate any subsequent response to this message. According to 3GPP standards (TS 24.501), a 5GMM Status message is a notification that does not inherently require a UE response unless it explicitly rejects a pending UE request (e.g., session establishment). Here, Cause #92 relates to PDU session resources—unrelated to the preceding Registration Complete, which was already acknowledged. The UE correctly processed the protected status message without action, as no standard-mandated response exists for this scenario. The absence of unnecessary communication aligns with security best practices, minimizing attack surface. The UE maintained confidentiality and integrity by relying on established keys, and its silent processing of the status indicates proper protocol adherence without exposing vulnerabilities. Secure

101	101	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 4.873120069503784 UE to AMF SACK (Ack=7, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 4.873471021652222 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport message containing a PDU session establishment request. The AMF responded with a Security Mode Command (SMC) protected with integrity (security header type 3), specifying ciphering algorithm 128-5G-EA3 and integrity algorithm 128-5G-IA2. Crucially, the UE provided no response to this SMC. According to 3GPP standards (TS 33.501), upon receiving an SMC, the UE must validate the integrity of the message using the newly negotiated security context and respond with either a Security Mode Complete (to accept the algorithms) or Security Mode Reject (to indicate failure). The absence of any response violates the mandatory security procedure, leaving the session in an undefined state and failing to establish secured communication. This omission prevents confirmation that the UE validated the network's security parameters or activated the agreed-upon algorithms, creating a critical gap in the security handshake. Insecure

102	102	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7492289543151855 UE to AMF UplinkNASTransport, Service request 0.749459981918335 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9532349109649658 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Service Request to the AMF after completing 5G-AKA authentication. The AMF responded with a Security Mode Command (SMC) message, which was marked as "Integrity protected with new security context" (security header type 3) but specified null algorithms (5G-EA0 for ciphering and 5G-IA0 for integrity). The UE rejected this SMC by responding with a 5GMM Status message containing the cause "Invalid mandatory information." This rejection occurred because the AMF's proposal of null algorithms—especially 5G-IA0 (null integrity)—violates 3GPP TS 33.501, which explicitly forbids using null integrity protection for NAS signaling messages (Section 6.4). By detecting this invalid configuration and refusing to proceed, the UE prevented a security downgrade that would have left subsequent communications without integrity protection. This adherence to the standard's security requirements demonstrates robust security hygiene. Secure
103	103	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5199828147888184 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5202269554138184 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport message (PDU session establishment request) after completing 5G-AKA authentication. The AMF responded with a Downlink NAS Transport message containing a Deregistration Request (UE terminated), which was protected with both integrity protection and ciphering (security header type 2), as required by 3GPP standards after security context establishment. The UE provided no response to this message. According to 3GPP TS 33.501, once 5G-AKA completes, the UE must verify integrity and decrypt all protected NAS messages. A valid Deregistration Request should trigger a Deregistration Accept from the UE. The absence of a response suggests the UE either failed to process a valid message (insecure) or correctly discarded an invalid message (e.g., due to integrity failure). Given the AMF's message was explicitly sent as protected and the UE's lack of response aligns with standard-mandated behavior for failed security checks—where messages must be silently discarded without further action—this indicates the UE performed the required security verification. If the message was tampered or malformed (a likely scenario in a security test), the UE's non-response constitutes secure adherence to 3GPP protocols by preventing processing of potentially compromised messages. Secure

104	104	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5198929309844971 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201320648193359 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (LADN not available) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE initiated a PDU session establishment request via an Uplink NAS Transport message. The AMF responded with a protected Deregistration Request (UE-terminated), which was integrity-protected and ciphered as required by the 5G security context established during 5G-AKA. However, the UE failed to send a Deregistration Accept message in response, despite the AMF's message being correctly protected and valid under 3GPP TS 24.501 standards. According to the protocol, upon receiving a protected and integrity-verified Deregistration Request (UE-terminated) without a re-registration requirement, the UE must acknowledge it with a Deregistration Accept to ensure proper state synchronization and secure session termination. The UE's lack of response indicates non-compliance with 3GPP standards, leaving the deregistration process incomplete and potentially exposing the network to session management vulnerabilities. Insecure
105	105	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5608680248260498 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5614829063415527 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7653870582580566 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure NAS context. The UE then sent an UL NAS TRANSPORT (PDU session establishment request), after which the AMF transmitted a Configuration Update Command (CUC) protected with both integrity protection and ciphering (security header type 2). The UE responded with a Configuration Update Complete. According to 3GPP TS 33.501, after 5G-AKA, all subsequent NAS messages—including the CUC—must be integrity-protected to prevent tampering and ciphering to ensure confidentiality. The UE correctly processed the protected CUC, as evidenced by its valid response, and adhered to the standard by not accepting an unprotected command. The absence of any noted security exceptions (e.g., ignoring an unprotected CUC or mishandling keys) confirms compliant behavior. Secure

106	106	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7586648464202881 UE to AMF UplinkNASTransport, Service request 0.7588739395141602 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9626758098602295 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request to the AMF after completing 5G-AKA authentication. The AMF responded with a Security Mode Command protected under a new security context, specifying 5G-EA4 for ciphering and 128-5G-IA3 for integrity. The UE rejected this command with a Security Mode Reject, citing a security capabilities mismatch. According to 3GPP standards (TS 33.501), the UE must support mandatory algorithms like 128-NIA1/2/3 for integrity and 128-NEA1/2/3 for ciphering, but 5G-EA4 is optional. The rejection indicates the UE does not support at least one proposed algorithm (likely 5G-EA4, as 128-5G-IA3 is an alias for mandatory 128-NIA3). This action is secure because the UE correctly identified a capabilities mismatch and aborted the procedure rather than proceeding with an unsupported algorithm, which could compromise security. The UE adhered to the standard by rejecting non-supported configurations and avoiding unprotected data exchange. Secure
107	107	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.46604204177856445 UE to AMF UplinkNASTransport, Registration complete 0.466264009475708 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Re-Registration Required) 0.6700358390808105 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure context between the UE and AMF. The UE sent an unprotected Registration Complete (as permitted by the standard for this specific message), followed by the AMF sending a protected Deregistration Request (security header type 2: integrity protected and ciphered), which is required for this downlink NAS message. The UE then responded with a Deregistration Accept. However, according to 3GPP TS 33.501 and TS 24.501, all NAS messages after security context establishment—except for specific exclusions like the initial Registration Request or Registration Complete—must be both integrity-protected and ciphered to prevent tampering and eavesdropping. The Deregistration Accept, being a post-security-activation NAS message, falls under this mandatory protection requirement. The test summary and packet capture explicitly note the AMF's Deregistration Request as protected but omit any security indication for the UE's Deregistration Accept, implying it was sent unprotected. This violates 5G security standards, leaving the message vulnerable to manipulation or interception. Insecure

108	108	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5200989246368408 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204448699951172 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7219538688659668 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began after successful 5G-AKA authentication, with the UE sending a UL NAS TRANSPORT containing a PDU session establishment request. The AMF responded with a protected CONFIGURATION UPDATE COMMAND (security header type 3), indicating integrity protection using the newly established security context. Instead of processing the command, the UE replied with a 5GMM STATUS message explicitly stating "Message type not compatible with the protocol state." According to 3GPP TS 24.501, this cause value (#96) is used when a message is received in an incompatible protocol state, suggesting the UE deemed the configuration update invalid during an ongoing PDU session establishment procedure. The UE correctly validated the message's integrity (as evidenced by its ability to parse and reject it with a standardized cause) but adhered to protocol state requirements by rejecting non-contextual network commands. This demonstrates compliant security behavior: The UE leveraged the security context to authenticate the message, then enforced state-machine rules to prevent processing potentially disruptive commands mid-session, aligning with 3GPP security principles. Secure
109	109	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5209951400756836 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215010643005371 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 0.7227599620819092 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began after successful 5G-AKA authentication, with the UE initiating a PDU session establishment via a UL NAS TRANSPORT message. The AMF responded with a protected GMM STATUS message containing 5GMM cause #98 ("message type not compatible with protocol state"), indicating the AMF deemed the UE's request invalid for the current protocol context. Instead of silently aborting the procedure or handling the error internally as mandated by 3GPP TS 24.501, the UE sent another UL NAS TRANSPORT containing a 5GMM STATUS message repeating cause #98 back to the AMF. This response violates 3GPP standards (Section 5.4.4.2), which explicitly prohibit responding to a GMM STATUS message with another GMM STATUS, as it is an unidirectional error report not requiring acknowledgment. The UE's action created unnecessary signaling, exposed it to potential amplification attacks, and disregarded protocol state management rules, demonstrating non-compliant and insecure behavior. Insecure

110	110	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 101 UE provided: No response The packet capture during the test using wireshark is: 0.5881869792938232 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 0.5883810520172119 AMF to UE SACK (Ack=6, Arwnd=106429) , DownlinkNASTransport, 5GMM status (Message not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a secure NAS context. The UE then sent an uplink message containing a Registration Complete, followed by a Deregistration Request (UE originating), which was transmitted in the same UplinkNASTransport. The AMF responded with a protected DownlinkNASTransport message containing a 5GMM Status (Cause 101: "Message not compatible with the protocol state"), indicating that the Deregistration Request was invalid in the current registered state. The UE did not respond to this status message. Based on the 5G standard (3GPP TS 24.501 and TS 33.501), the UE's actions were secure. After 5G-AKA, all NAS messages must be protected, and the UE correctly encrypted its uplink messages (Registration Complete and Deregistration Request). The Cause 101 from the AMF is a protocol-level error unrelated to security, triggered by the premature Deregistration Request. The UE's lack of response to the 5GMM Status is standard-compliant, as status messages do not require acknowledgments. The UE maintained cryptographic protections and avoided unnecessary processing of the invalid message, aligning with security protocols. Secure
111	111	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7300009727478027 UE to AMF UplinkNASTransport, Service request 0.7302379608154297 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9340109825134277 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request to the AMF. The AMF responded with a Security Mode Command specifying **5G-IA0 (null integrity)** as the integrity algorithm and **5G-EA5** as the ciphering algorithm, while marking the message as "integrity protected" (security header type 3) despite the null algorithm offering no actual integrity protection. The UE rejected this command with a **Security Mode Reject (UE security capabilities mismatch)**. According to 3GPP standards (TS 33.501), integrity protection is mandatory for Security Mode Command messages. The use of **5G-IA0 (null integrity)** violates this requirement, as it provides no integrity verification, leaving the message vulnerable to tampering. The UE correctly identified this mismatch by rejecting the command, as its security capabilities (established during 5G-AKA) would not support null integrity for such critical security negotiations. This adherence to protocol ensures that security contexts are only established with valid protection mechanisms. **Secure**

112	112	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7296979427337646 UE to AMF UplinkNASTransport, Service request 0.7299599647521973 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9337029457092285 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request to the AMF, initiating the establishment of a secure connection. The AMF responded with a Security Mode Command (SMC), protected using security header type 3 (integrity protected with new security context), specifying the ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA2. The UE rejected this command with a Security Mode Reject message, citing a "UE security capabilities mismatch." This indicates the UE determined that either the ciphering algorithm (5G-EA5), integrity algorithm (128-5G-IA2), or both were not supported or permitted by its advertised security capabilities. According to 3GPP standards (TS 33.501), the UE must validate that the algorithms selected by the network align with its own capabilities before activating security. Rejecting the SMC in this scenario prevents the use of unsupported or non-compliant algorithms, ensuring the UE does not proceed with potentially vulnerable or undefined security contexts. This behavior aligns with 3GPP security requirements, as it enforces algorithm negotiation integrity and mitigates risks from forced algorithm downgrades or unsupported configurations. Secure

113	113	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 14.246875047683716 UE to AMF UplinkNASTransport, Service request 14.247098922729492 AMF to UE SACK (Ack=15, Arwnd=106496) , DownlinkNASTransport, Security mode command 14.454866886138916 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Service Request to the AMF after completing 5G-AKA authentication. The AMF responded with a Security Mode Command (SMC), which was integrity-protected using the existing security context established during 5G-AKA. This SMC specified new ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms and used security header type 3 to signal activation of a new security context. The UE, however, rejected the SMC with an "unspecified" cause code via a Security Mode Reject message, despite the AMF's command being valid and properly protected. According to 3GPP standards (TS 33.501 and TS 24.501), after successful 5G-AKA, the UE must accept a correctly protected SMC that proposes mandatory-supported algorithms (like 128-5G-EA1/IA2) unless specific verifications fail (e.g., integrity check mismatch or unsupported algorithms). Here, the UE's rejection without a specific cause—despite no indicated errors in algorithm support or AMF behavior—suggests either an internal UE flaw (e.g., key derivation error, faulty integrity verification) or unnecessary deviation from protocol. This behavior disrupts security activation, leaves subsequent messages unprotected, and violates standard procedures, potentially exposing the UE to security risks or service denials. Insecure
114	114	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5208940505981445 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215411186218262 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7234148979187012 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a NAS security context between the UE and the AMF. The UE initiated further communication by sending an Uplink NAS Transport (PDU session establishment request). Subsequently, the AMF sent a Configuration Update Command, which was correctly protected with both integrity and ciphering (security header type 2), adhering to the 5G security requirements post-authentication. The UE responded with a Configuration Update Complete message. However, the test summary and packet capture do not specify the security attributes (e.g., security header type) for the UE's Uplink NAS Transport or the Configuration Update Complete messages. According to 3GPP TS 33.501, once 5G-AKA is completed and a security context is established, all subsequent NAS messages—including uplink transmissions like Configuration Update Complete—must be at minimum integrity-protected to prevent tampering and ensure authenticity. The omission of protection details for the UE's messages, particularly the Configuration Update Complete—a critical response to a secured downlink command—strongly implies these messages were sent without the mandated security headers (e.g., as plaintext or with inadequate protection). This deviation violates 5G security protocols, as UEs must enforce protection for all NAS messages after authentication to mitigate risks like replay or injection attacks. Insecure

115	115	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 14.061744928359985 UE to AMF UplinkNASTransport, Service request 14.062045097351074 AMF to UE SACK (Ack=16, Arwnd=106496) , DownlinkNASTransport, Security mode command 14.26575493812561 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Service Request to the AMF, as security activation had not yet been initiated. The AMF responded with a Security Mode Command (SMC), which was integrity-protected using the new security context established during the prior 5G-AKA authentication. The SMC specified ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA3, with ABBA parameter 0000. Instead of accepting the SMC and activating security, the UE sent a 5GMM status message with cause "Invalid mandatory information" (0x60), rejecting the command. According to 3GPP TS 24.501, the UE must verify the integrity and validity of the SMC before activating security. By rejecting the SMC due to invalid mandatory information—while not reporting an integrity failure (which would use cause 0x61)—the UE correctly identified a semantic error in the message (e.g., unsupported algorithm, malformed IE, or ABBA mismatch) and refused to apply the security context. This aligns with 5G security standards, as the UE prevented potential exploitation from an improperly configured security context and maintained protocol compliance by halting further protected communication until valid parameters are provided. Secure

116	116	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00d2 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.480457067489624 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48129701614379883 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.6844742298126221 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Uplink NAS Transport (PDU session establishment request) after completing 5G-AKA authentication. The AMF responded with a Security Mode Command (SMC) message, which was integrity-protected using the newly established security context (header type 3), specifying ciphering (128-5G-EA2) and integrity (128-5G-IA2) algorithms. The UE rejected this command with a Security Mode Reject (cause: "unspecified"), halting further secured communication. According to 3GPP standards (TS 33.501), after 5G-AKA, the UE must verify the integrity of the SMC using the derived K_AMF key and the selected integrity algorithm. The rejection indicates the UE detected an issue—likely a failed integrity check, unsupported algorithms, or ABBA parameter mismatch—though the exact cause remains unspecified. By rejecting the SMC, the UE prevented the activation of a potentially compromised or unverifiable security context, adhering to security protocols that mandate integrity validation before proceeding. This aligns with 3GPP security principles, as proceeding without verified protection would expose subsequent messages to tampering or eavesdropping. While the rejection may stem from implementation-specific errors, the UE's refusal to accept unverified security parameters constitutes secure behavior under the standard. Secure

117	117	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.5606789588928223 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5618300437927246 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport message containing a PDU Session Establishment Request. The AMF then responded with a Security Mode Command (SMC) message, which was protected (integrity-protected and ciphered) using a new security context, specifying ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA1. Crucially, the UE provided no response to this SMC. According to 3GPP standards (TS 33.501), upon receiving an SMC, the UE must validate the message's integrity using the new security context and respond with either a Security Mode Complete (if validation succeeds) or Security Mode Reject (if it fails). The absence of any response violates this mandatory procedure, leaving the security context activation unconfirmed and disrupting the NAS security setup. This omission indicates the UE failed to adhere to protocol requirements, potentially exposing subsequent communications to security risks like unverified commands or ciphered data without mutual context agreement. Insecure
118	118	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 6.6406471729278564 UE to AMF SACK (Ack=8, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 6.641204118728638 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Configuration update command 6.843037128448486 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure NAS context. The UE initiated communication by sending an Uplink NAS Transport message carrying a PDU session establishment request. The AMF responded with a protected Downlink NAS Transport message (Configuration Update Command), which was both integrity-protected and ciphered (security header type 2) as required by 3GPP standards. The UE acknowledged this with a Configuration Update Complete message via Uplink NAS Transport. However, the test summary explicitly confirms protection status only for the AMF's downlink message, omitting any mention of security mechanisms (integrity protection or ciphering) for the UE's Configuration Update Complete response. According to 3GPP TS 33.501, once 5G-AKA completes and a NAS security context is established, all subsequent NAS messages—including responses to protected commands—must be secured. The absence of documented protection for the UE's final message indicates a deviation from this mandate, leaving the response vulnerable to tampering or eavesdropping. Insecure

119	119	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.5208361148834229 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5222671031951904 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.7242951393127441 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Uplink NAS Transport (PDU session establishment request) after completing 5G-AKA authentication. The AMF responded with a Security Mode Command (SMC) protected with integrity (security header type 3), specifying the null ciphering algorithm (5G-EA0) and the 128-5G-IA1 integrity algorithm. The UE rejected this command with a Security Mode Reject (unspecified cause). According to 3GPP standards (TS 33.501), the UE must verify the integrity of the SMC and validate the selected algorithms. While the integrity algorithm (128-5G-IA1) is mandatory and valid, the null cipher (5G-EA0) disables encryption, exposing NAS messages to eavesdropping. The UE's rejection—likely due to a local policy requiring encryption—aligns with security best practices, as 3GPP permits UEs to enforce higher security (e.g., rejecting null cipher) even if supported. The unspecified cause is acceptable per TS 24.501, as the standard does not mandate detailed causes for algorithm-related rejections. By refusing to proceed without encryption, the UE prioritized confidentiality, demonstrating secure behavior under 3GPP guidelines. Secure
120	120	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.46767306327819824 UE to AMF UplinkNASTransport, Registration complete 0.46790289878845215 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF began with the successful completion of 5G-AKA, establishing a secure context for NAS communication. The UE sent a protected Registration Complete message, confirming its successful registration. Subsequently, the AMF responded with a protected Deregistration Accept message (indicating UE-terminated deregistration), which the UE processed without sending any further response. According to 3GPP standards (TS 24.501), after 5G-AKA completion, NAS messages must be integrity-protected, and the UE must validate message integrity before processing. The Deregistration Accept message was sent as protected, implying it included valid integrity protection. Critically, 3GPP explicitly states that no response is required from the UE upon receiving a protected UE-terminated Deregistration Accept, as this message concludes the deregistration procedure without requiring acknowledgment. The UE's lack of response aligns with this protocol specification and demonstrates proper security behavior by silently terminating the session after verifying the protected message's integrity. Thus, the UE's actions adhered to 5G security requirements. Secure

121	121	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 1.719182014465332 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 1.7194299697875977 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, which is part of the 5G-AKA procedure to establish mutual authentication and security keys. Since 5G-AKA had not yet been completed at this stage, the message was sent unencrypted, as required by the 3GPP standard (TS 33.501) for pre-security-context NAS messages. The AMF then responded with a Service Reject containing 5GMM Cause #111 ("Protocol error, unspecified"), sent in plaintext due to the unestablished security context. The UE correctly ceased communication upon receiving this rejection, as Service Reject terminates the session and mandates no further NAS response per 3GPP TS 24.501. The UE's actions align with the standard: it transmitted pre-authentication messages unencrypted (as encryption is impossible without completed 5G-AKA) and avoided protocol violations by not replying to the Service Reject. No evidence suggests the UE mishandled keys, ignored security procedures, or transmitted sensitive data insecurely. Secure
122	122	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003769397735595703 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request to the AMF via an InitialUEMessage, which was transmitted unencrypted as 5G-AKA authentication had not yet been performed. The AMF responded with a Service Reject message containing 5GMM Cause #9 ("UE identity cannot be derived by the network"), indicating the network failed to identify the UE from the provided credentials. This rejection was sent in plaintext, consistent with the lack of an established security context. Critically, the UE exhibited **no response** to this rejection. According to 3GPP TS 24.501, upon receiving Cause #9, the UE must initiate a new registration attempt by sending another Registration Request that includes its permanent subscription identifier (SUCI) to enable network identification and trigger authentication. The UE's failure to retransmit with SUCI violates the standard's security protocol, as it prevents the initiation of 5G-AKA—which is essential for mutual authentication and subsequent NAS encryption. This inaction leaves the UE in an unauthenticated state and exposes it to persistent service denial or man-in-the-middle attacks. Insecure

123	123	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.03993701934814453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04126906394958496 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24338102340698242 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF, after which the AMF transmitted a Security Mode Command (SMC) protected with integrity (security header type 3), specifying ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA1. Crucially, **5G-AKA authentication had not been completed** at this stage, meaning no shared security context (K~AMF~) existed to validate the message's integrity. The UE correctly rejected the SMC with a "Security mode reject (unspecified)" response. Per 3GPP TS 33.501, NAS security activation (via SMC) must occur **after** successful 5G-AKA, as the derived keys are essential for integrity verification. The AMF violated this sequence by sending a protected SMC pre-authentication, rendering the message unverifiable. The UE's rejection aligns with the standard's security requirements by refusing to process an integrity-protected command without a valid key, preventing potential exploitation (e.g., forced algorithm downgrade or false context activation). Thus, the UE acted securely by enforcing protocol-mandated authentication precedence. Secure
124	124	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an initial Identity Response, followed by the AMF requesting the UE's SUCI via a plaintext Identity Request (as 5G-AKA was incomplete and no security context existed). The UE then responded with another Identity Response containing the SUCI, also transmitted in plaintext. According to 3GPP standards (TS 33.501), SUCI transmission in plaintext is explicitly permitted before 5G-AKA completion, as the SUCI itself protects the subscriber's permanent identifier (SUPI) through elliptic curve encryption using the home network's public key. This design ensures that even unencrypted NAS transport exposes only the concealed identity, mitigating privacy risks. The UE's compliance with this protocol—providing the SUCI without requiring encryption at this stage—aligns with 5G security specifications. Secure

125	125	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00029206275939941406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an InitialUEMessage containing a Registration Request via plain NAS signaling, as 5G-AKA had not yet been initiated. The AMF responded immediately with an Authentication Reject message, also sent in plain text, to which the UE provided no response. According to 3GPP standards (TS 24.501 and TS 33.501), before 5G-AKA completion, NAS messages like Registration Request and Authentication Reject are inherently unprotected since no security context exists. The UE's lack of response aligns with protocol requirements: upon receiving Authentication Reject, the UE must abort the registration attempt, invalidate the current security context, and refrain from further communication until reinitialization. This prevents potential exploitation (e.g., forced re-authentication attacks) by not processing or reacting to unsolicited rejections. The UE correctly prioritized protocol compliance over reacting to an unverified reject command. Secure
126	126	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5059909820556641 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5062329769134521 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7099969387054443 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message after successfully completing the 5G-AKA authentication, establishing a secure NAS context. The AMF then responded with a Deregistration Request (UE terminated), which was correctly protected with both integrity and ciphering (security header type 2) as mandated by 3GPP standards (TS 33.501) for post-authentication NAS messages. The UE subsequently sent a Deregistration Accept message. However, based on the packet capture and test summary, the UE's Deregistration Accept was transmitted without security protection (indicated by the lack of security header notation in the UplinkNASTransport description). This violates 3GPP TS 24.501, which requires all NAS messages—including deregistration responses—to be integrity-protected after security context establishment to prevent tampering and ensure message authenticity. The UE's failure to protect this message undermines the security continuity expected post-5G-AKA. Insecure

127	127	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.03972792625427246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF, which occurred in plaintext as 5G-AKA authentication had not yet been completed. Subsequently, the AMF sent a Deregistration Accept message—also in plaintext—terminating the session, to which the UE provided no response. According to 3GPP standards (TS 33.501), NAS messages like Deregistration Accept must be integrity-protected and encrypted once a security context is established via 5G-AKA. However, since 5G-AKA was never initiated or completed in this exchange, no security context existed, and the standard permits plaintext transmission for initial procedural messages before authentication. The UE's lack of response to Deregistration Accept is normal behavior upon session termination and does not violate protocols. Crucially, the UE did not process any sensitive post-authentication commands or user data in this state, and the plaintext exchange was confined to non-sensitive procedural messages during the pre-security context phase, aligning with standard allowances. Thus, the UE operated within expected security parameters. Secure
128	128	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 00000000000000000000000000000000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Mapped security context ngKSI_KSI: 1 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.03987288475036621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04013490676879883 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24352788925170898 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF. The AMF then sent a plain-text Authentication Request containing a RAND of all zeros, an AUTN of all zeros, ABBA "3031", and ngKSI parameters indicating a mapped security context with KSI value 1. The UE responded with a 5GMM status message indicating "Invalid mandatory information" (cause #96), rejecting the request. According to 3GPP standards (TS 33.501 and TS 24.501), an all-zero AUTN is inherently invalid as it fails structural and cryptographic validation (e.g., MAC verification and SQN checks). The UE should have responded with an Authentication Failure message specifying "MAC failure" (cause #20) or "Sync failure" (cause #21) to properly handle the AUTN error. However, by rejecting the request outright, the UE avoided proceeding with an unauthentic network or compromised parameters, maintaining core security objectives. The use of cause #96—while non-compliant for this scenario—did not expose vulnerabilities or accept invalid authentication, as the UE terminated the procedure without establishing a security context. Thus, the action preserved security despite protocol deviations. Secure

129	129	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3100 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11980295181274414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12005805969238281 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.321152925491333 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response after completing 5G-AKA, indicating successful mutual authentication. The AMF then sent a Security Mode Command protected with integrity (security header type 3), proposing the use of the null ciphering algorithm (5G-EA0) for confidentiality and 128-5G-IA2 for integrity. The UE responded with a Security Mode Reject, citing an unspecified reason, thereby rejecting the proposed security configuration. According to 3GPP standards (TS 33.501), the use of null ciphering (5G-EA0) is permissible only in specific scenarios like emergency services or initial provisioning, but it is strongly discouraged for normal user plane data due to the lack of confidentiality. The UE's rejection aligns with security best practices, as accepting null ciphering would expose all subsequent communications to eavesdropping and violate the principle of confidentiality mandated by 5G security architecture. By rejecting the configuration, the UE prioritized security over network directives, demonstrating adherence to the standard's security objectives. Secure

130	130	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3131 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.04801797866821289 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04822111129760742 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.25036191940307617 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF. The AMF replied with a plaintext Authentication Request containing RAND (353535...35), AUTN (353535...35), ABBA (3131), and ngKSI parameters. The UE then responded with an Authentication Failure message, citing "Non-5G authentication unacceptable" (cause #22 per 3GPP TS 24.501). This occurred because the AUTN's AMF field (bytes 7-8 of AUTN, value 0x3535) lacked the mandatory 5G-specific bit (0x80 in the first byte of the AMF field), indicating a non-5G authentication challenge. Per 3GPP TS 33.501, the UE must reject such challenges in 5G standalone mode to prevent fallback attacks, as accepting non-5G authentication could compromise security. The UE's compliance with this requirement—detecting the invalid AUTN structure and explicitly rejecting it—demonstrates correct adherence to 5G security standards. Secure
131	131	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00038909912109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The UE initiated the registration procedure by sending an unencrypted Initial Registration Request, which is standard behavior when no security context exists. The AMF responded with an unencrypted Registration Reject (5GMM Cause #26: "Non-5G authentication unacceptable") without completing 5G-AKA. Since 5G-AKA—which establishes encryption keys—was never performed, both messages were transmitted in plaintext as required by 3GPP standards. The UE correctly ceased communication upon rejection, avoiding further unprotected exchanges. This aligns with 3GPP TS 33.501 and TS 24.501, which permit initial NAS messages without security and mandate termination after rejection. No sensitive data was exposed, and the UE adhered to protocol by not transmitting additional data post-rejection. Secure

132	132	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 99 UE provided: No response The packet capture during the test using wireshark is: 0.03979802131652832 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040032148361206055 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service reject (Information element non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response in plaintext, as 5G-AKA had not yet been executed to establish a security context. The AMF responded with a Service Reject containing 5GMM Cause #99 ("information element non-existent or not implemented"), also sent in plaintext, after which the UE ceased communication. According to 3GPP standards (TS 33.501), NAS messages prior to 5G-AKA completion must be unprotected, making the plaintext exchange compliant. The UE correctly refrained from encrypting the Identity Response without an established security context, and its lack of response to the Service Reject aligns with protocol expectations for terminal handling of rejections. Cause #99 indicates a syntactic or semantic error in the UE's message, but this does not inherently reflect a security lapse—it may stem from implementation differences or test-specific AMF configurations. The UE adhered to security protocols by avoiding encryption without keys and terminating the session upon rejection, demonstrating no deviation from 5G security requirements. Secure
133	133	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3200 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.0398869514465332 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040138959884643555 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24263286590576172 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF. The AMF then sent a downlink Authentication Request message containing a RAND (3535...35) and AUTN (3535...35), transmitted in plaintext as 5G-AKA was incomplete. The UE responded with an Authentication Failure message, explicitly stating "Non-5G authentication unacceptable" (3GPP cause #22). This rejection occurred because the AUTN value—composed of repeating 0x35 bytes—is syntactically invalid for 5G-AKA, as it lacks the structured fields (e.g., SQN, AMF separation bit) required by 3GPP TS 33.102. Per 5G standards (TS 33.501), the UE must validate AUTN to ensure network authenticity and 5G compatibility. By rejecting this malformed AUTN, the UE correctly identified a potential downgrade attack or network spoofing attempt, adhering to security protocols that prevent non-5G authentication in 5G standalone mode. The plaintext transmission was unavoidable here, as no security context existed yet. Secure

134	134	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 3 UE provided: No response The packet capture during the test using wireshark is: 0.039869070053100586 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040055036544799805 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service reject (Illegal UE) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response message to the AMF, as required during NAS procedures. Since 5G-AKA authentication had not yet been completed, this uplink message—and all prior NAS messages—were transmitted unencrypted, which is standard behavior per 3GPP. The AMF then responded with a Service Reject message containing 5GMM Cause #3 ("Illegal UE"), explicitly indicating the UE is unauthorized for service in the current PLMN. Critically, this downlink message was sent in plaintext, consistent with 5G security protocols that permit unencrypted NAS communication before authentication establishes a security context. The UE, upon receiving the Service Reject, provided no further response, which aligns with 3GPP standards (TS 24.501): A Service Reject with Cause #3 terminates the registration attempt, and the UE must not continue NAS signaling for this session. Instead, the UE should handle the rejection internally (e.g., by abandoning the registration or selecting a new PLMN) without transmitting additional data. The UE's adherence to this protocol—halting communication after an unencrypted rejection—prevents unnecessary exposure of credentials or signaling in an unauthenticated state and complies with security expectations for pre-AKA scenarios. Thus, the UE's actions were secure. Secure
135	135	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00067901611328125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.2038860321044922 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request. The AMF responded with a Security Mode Command (SMC) marked as "Protected" (security header type 3), but it specified null algorithms for both ciphering (5G-EA0) and integrity (5G-IA0). The UE rejected this command with a Security Mode Reject, citing an unspecified reason. Critically, 5G-AKA authentication had not been completed, meaning no shared keys were established to enable actual security. The 3GPP standard (TS 33.501) mandates that null integrity (5G-IA0) must never be accepted for NAS signaling in normal scenarios, as it leaves messages vulnerable to tampering. By rejecting the SMC with null algorithms, the UE adhered to this requirement and prevented an insecure security context from being established. This action aligns with 5G security principles, as accepting null integrity would have exposed subsequent communications to forgery or manipulation. Secure

136	136	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 1.639894962310791 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Identity response 1.6405549049377441 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Security mode command 1.841944932937622 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Identity Response to the AMF. The AMF then responded with a Security Mode Command (SMC) that was marked as "Integrity protected with new security context" (security header type 3), specifying integrity algorithm 128-5G-IA3 and null ciphering (5G-EA0). However, the 5G-AKA authentication procedure had not been completed at this stage, meaning no shared security context (including keys for integrity verification) existed between the UE and AMF. The UE, unable to validate the integrity of the SMC due to the absence of valid keys, rejected it with a Security Mode Reject (cause: "unspecified"). According to 3GPP standards (TS 33.501), NAS security mode procedures must only occur after successful 5G-AKA, as the derived keys are essential for integrity protection verification. The UE's rejection aligns with this requirement, as accepting an integrity-protected command without verified keys would risk processing malicious or unauthenticated instructions. Thus, the UE adhered to security protocols by refusing to proceed without a valid security context. Secure

137	137	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 2f4b62abf69d8352398c608fb3a89563 AUTN: 062d8ab6b7549000811f4ee8b8da8440 ngKSI_TSC: Native security context ngKSI_KSI: 6 UE provided: Authentication response The packet capture during the test using wireshark is: 1.9198977947235107 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Authentication response 1.9201328754425049 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.120612859725952 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unsolicited Authentication Response without having received an Authentication Request from the AMF. Subsequently, the AMF sent an Authentication Request containing RAND, AUTN, and ABBA parameters in plain text, as the 5G-AKA procedure had not yet completed and no security context was established. The UE then sent a second Authentication Response, also in plain text. While unencrypted NAS messages are permitted by the 5G standard (3GPP TS 33.501) prior to security context establishment, the UE's initial transmission of an Authentication Response without a preceding Authentication Request violates the 5G-AKA protocol sequence. This deviation indicates a failure in the UE's state management, as it should only generate an Authentication Response after receiving and validating an Authentication Request (with AUTN). Such unsolicited messages could expose authentication parameters prematurely or enable protocol manipulation attacks, contravening 3GPP security requirements (TS 33.501, Section 6.1.3.2). Insecure

138	138	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5089499950408936 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5091559886932373 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Undergoing) 0.7129359245300293 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE completing 5G-AKA, establishing a NAS security context. The UE then sent a Registration Complete message, confirming successful registration. Subsequently, the AMF transmitted a Deregistration Request (UE-terminated) with security header type 2, indicating it was both integrity-protected and ciphered, as mandated by 3GPP TS 33.501 after security context establishment. The UE processed this request and responded with a Deregistration Accept. Crucially, the UE only established this accept message after successfully verifying the integrity and decrypting the protected Deregistration Request from the AMF, confirming the message's authenticity and origin. This aligns with 3GPP standards, which require UEs to validate security headers and reject unprotected/invalid NAS messages post-authentication. No evidence suggests the UE mishandled the security context (e.g., accepting an unprotected deregistration command or failing to protect its response), and the UE's Deregistration Accept would inherently be protected under the active security context, as implied by the prior 5G-AKA completion and the absence of noted vulnerabilities in the test. Secure

139	139	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 31303030000000007894d5bcdd550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00084686279296875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2040548324584961 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request to the AMF. The AMF responded with a plain-text Authentication Request containing an invalid AUTN (all zeros), a valid RAND, ABBA (0000), and ngKSI parameters. The UE rejected this message with a 5GMM Status message indicating "Invalid mandatory information," halting the 5G-AKA process. According to 3GPP standards (TS 33.501 and TS 24.501), an all-zero AUTN is syntactically incorrect and must be rejected by the UE, as it fails to authenticate the network and poses a security risk. The UE correctly identified the invalid AUTN and terminated the procedure, preventing potential security compromises like bidding-down attacks or connection to untrusted networks. However, the standard mandates that such failures should trigger an Authentication Failure message with a specific cause value (e.g., "MAC failure"), not a generic 5GMM Status. The UE's use of 5GMM Status deviates from protocol specifications, indicating an implementation flaw. Despite this, the core security objective—rejecting the suspicious authentication—was achieved, as the UE avoided establishing a security context with an unauthenticated network. Thus, while non-compliant in error reporting, the UE's substantive action aligned with security requirements. Secure

140	140	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 300068c66b7f000078b48472b0550000 AUTN: 300068c66b7f0000eeb58472b0550000 ngKSI_TSC: Native security context ngKSI_KSI: 1 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007758140563964844 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20353293418884277 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Initial Registration Request to the AMF. The AMF responded with an Authentication Request containing RAND, AUTN, and security parameters (ngKSI_KSI=1, TSC=Native), sent in plaintext as 5G-AKA was incomplete. Instead of replying with an Authentication Response to complete the security setup, the UE abruptly sent a Deregistration Request (UE originating) within 0.2 seconds, terminating the session without establishing a security context. This action is **insecure** per 3GPP standards (TS 33.501). The UE violated the mandatory 5G-AKA sequence, which requires completing authentication before initiating other NAS procedures. By bypassing authentication, the UE failed to establish integrity protection and encryption for NAS messages, leaving subsequent communications vulnerable to eavesdropping or manipulation. The premature deregistration also disrupted the security handshake, indicating non-compliance with protocol expectations and exposing potential implementation flaws that could be exploited in real-world attacks. Insecure
141	141	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.17494893074035645 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.17513012886047363 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF began with the UE sending an Authentication Response message via Uplink NAS Transport, indicating it was participating in the 5G-AKA authentication procedure. The AMF then responded with an Authentication Reject message sent in plaintext (unencrypted) via Downlink NAS Transport, to which the UE provided no further response. Since 5G-AKA had not been completed at this stage, no security context (including encryption or integrity protection) was established, making the plaintext transmission of the reject message standard-compliant per 3GPP TS 33.501. The UE's lack of response aligns with 3GPP TS 24.501 requirements, which mandate that upon receiving an Authentication Reject, the UE must silently abort the registration process, invalidate relevant security parameters, and transition to a DEREGISTERED state without sending additional messages. This prevents unnecessary signaling or potential exploitation by unauthenticated networks. The UE's adherence to these protocols—by not reacting to an unprotected reject message before authentication finalization—demonstrates correct implementation of security measures against session hijacking or bidding-down attacks. Secure

142	142	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000ee95abdf8e550000 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.15996193885803223 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16019487380981445 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.3615410327911377 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response, followed by the AMF sending a downlink Authentication Request containing RAND, AUTN, and security parameters (ngKSI) in plaintext since 5G-AKA authentication was incomplete. The UE then responded with an Authentication Failure message, explicitly rejecting the authentication attempt with the cause "Non-5G authentication unacceptable," indicating it detected an invalid or non-5G-compliant AUTN token. According to 3GPP standards (TS 33.501), the UE must validate the AUTN to ensure network authenticity and 5G compatibility. By rejecting the suspicious AUTN (which contained irregularities like partial zeros and an unexpected structure), the UE adhered to security protocols that prevent potential downgrade attacks or forged network authentication. This behavior aligns with 5G security requirements, as accepting an invalid AUTN could compromise mutual authentication. Secure
143	143	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5046439170837402 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 0.5048840045928955 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE completing 5G-AKA authentication, establishing a secure context for NAS communication. The UE then sent a Registration Complete message, confirming successful registration. Subsequently, the AMF transmitted a Deregistration Request (UE-terminated) message, which was protected with both integrity protection and ciphering (security header type 2), as required after 5G-AKA. According to 3GPP TS 24.501 (Section 5.5.2.3.2), upon receiving an *integrity-protected* Deregistration Request, the UE must respond with a Deregistration Accept message to complete the deregistration procedure securely and maintain protocol state synchronization. However, the UE provided no response to this message, violating the standard's mandatory behavior for protected NAS messages. This non-compliance leaves the network uncertain about the UE's state, potentially causing resource retention or desynchronization vulnerabilities. The UE's failure to respond undermines the security guarantees of the established NAS security context and deviates from 3GPP requirements. Insecure

144	144	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5077369213104248 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080108642578125 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.7157459259033203 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure NAS signaling context. The UE sent a Registration Complete message, after which the AMF transmitted a protected Configuration Update Command (security header type 2: integrity-protected and ciphered). The UE responded with a Configuration Update Complete message. Per 3GPP TS 33.501, once 5G-AKA is finalized, all subsequent NAS messages—including responses to commands—must be protected using the established security context. The UE's Configuration Update Complete should have been integrity-protected and ciphered (security header type 2), as the security context was active and no security context reset occurred. The test summary explicitly notes the AMF's downlink message as protected but omits the security status of the UE's uplink Configuration Update Complete. Since the standard mandates protection for all post-authentication NAS messages, and the UE did not revert to unprotected transmission (security header type 0) or report a security failure, it is inferred that the UE correctly protected its response, maintaining compliance. Secure
145	145_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15980100631713867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16017889976501465 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3686530590057373 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Security Mode Complete message alongside a Registration Request, prior to receiving the Security Mode Command from the AMF. This was followed by the AMF sending a Security Mode Command, which was integrity-protected using the new security context (as indicated by security header type 3) and specifying the 128-5G-IA2 integrity algorithm and null ciphering (5G-EA0). Subsequently, the UE sent another Security Mode Complete message. According to 3GPP standards (TS 33.501), after 5G-AKA completion, all NAS messages must be integrity-protected once the security context is established. The UE's initial transmission of Security Mode Complete was insecure because it was sent unprotected before the AMF's Security Mode Command activated the security context. This violates the protocol, as the UE should only send Security Mode Complete in response to a protected Security Mode Command to ensure message authenticity and integrity. Insecure

146	146	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.1601390838623047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037797927856445 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA authentication, establishing a secure context. The UE then sent an uplink Security Mode Complete message, confirming activation of NAS security. Subsequently, the AMF sent a protected Deregistration Accept (UE-terminated) message, which was encrypted and integrity-protected using the negotiated security keys. The UE provided no response to this message. According to 3GPP standards (TS 33.501), once NAS security is activated via Security Mode Command (acknowledged by Security Mode Complete), all subsequent NAS messages—including Deregistration Accept—must be protected. The UE's silent acceptance of the protected Deregistration Accept is standard-compliant behavior, as this message does not require a response (TS 24.501). The UE validated the message's integrity and encryption, confirming its legitimacy, and avoided unnecessary communication that could expose vulnerabilities. No deviation from protocol or security bypass occurred. Secure
147	147	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.15987586975097656 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16038084030151367 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.3645758628845215 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a security context. The UE sent a Security Mode Complete message, confirming activation of the new security context. The AMF then transmitted a protected Downlink Configuration Update Command (security header type 3, indicating integrity protection with the new context). However, the UE responded with a 5GMM Status message indicating "Message type not compatible with the protocol state" (cause #96). This rejection occurred because the Configuration Update Command was sent during an ongoing initial registration procedure—evidenced by the UE's simultaneous transmission of Security Mode Complete and Registration Request in the same uplink. According to 3GPP TS 24.501, the Configuration Update Command is invalid during registration, as the UE expects only Registration Accept/Reject after Security Mode Complete. By rejecting this out-of-state command, the UE adhered to protocol sequencing rules, preventing potential processing of unauthorized updates during a critical security-sensitive phase. Secure

148	148	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.11970210075378418 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.11996603012084961 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Congestion) 0.3268871307373047 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a secure NAS context. The UE sent a protected Security Mode Complete message, confirming activation of security algorithms. Subsequently, the AMF sent a protected Deregistration Request (integrity-protected and ciphered) indicating UE-terminated deregistration due to congestion. The UE responded with a Deregistration Accept message. According to 3GPP TS 24.501, after security context activation (post-5G-AKA and Security Mode Command), all NAS messages—including Deregistration Accept—must be integrity-protected and ciphered to prevent tampering or eavesdropping. The test summary and packet capture do not indicate that the UE's Deregistration Accept was protected (security header type 2), suggesting it was sent in plaintext (security header type 0). This violates 5G security standards, as the UE failed to maintain protection despite an active security context, exposing the message to potential attacks. Insecure
149	149	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an initial Security Mode Complete message alongside a Registration Request, as observed in the first packet capture (0.160s). This occurred before the AMF transmitted the Security Mode Command (0.160s), which was integrity-protected and specified the ciphering algorithm (5G-EA7) and integrity algorithm (128-5G-IA2). The UE then sent another Security Mode Complete message at 0.365s after receiving the command. According to 3GPP standards (TS 33.501), the Security Mode Complete message must only be sent by the UE in response to a valid Security Mode Command from the network, as it confirms the activation of negotiated security algorithms. Here, the UE's first Security Mode Complete was unsolicited—transmitted without prior receipt of the Security Mode Command—constituting a protocol violation. This premature message could expose the UE to security risks like replay attacks or misinterpretation of security context, as it bypasses the mandated handshake where security activation is unilaterally commanded by the network. Insecure

150	150	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.16013693809509277 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16036486625671387 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.3618440628051758 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a security context. The UE sent a Security Mode Complete message (protected, as required post-authentication), confirming activation of security algorithms. The AMF then sent a protected Deregistration Request (UE-terminated), which was integrity-protected and ciphered per security header type 2. The UE responded with a Deregistration Accept message. However, according to 3GPP TS 33.501 and TS 24.501, once a security context is active (post-5G-AKA and Security Mode Command/Complete), all subsequent NAS messages—including Deregistration Accept—must be protected to ensure confidentiality and integrity. The test summary and packet capture explicitly note the AMF's Deregistration Request as protected but omit security indicators for the UE's Deregistration Accept, implying it was sent unprotected. This violates the 5G standard, as the UE failed to apply mandatory protection despite an active security context, exposing it to potential eavesdropping or manipulation. Insecure
151	151	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00026297569274902344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected initial Registration Request to the AMF, as no security context existed yet. The AMF responded with an unprotected Identity Request message, explicitly asking for the GUTI (a temporary identifier) to facilitate the registration process. According to 3GPP standards (TS 24.501 and TS 33.501), during initial registration prior to 5G-AKA completion, the UE is expected to respond to such unprotected Identity Requests for non-sensitive identities like the GUTI, as this exchange occurs before security establishment. The GUTI is designed to be transmitted in plain text at this stage to avoid exposing the permanent subscriber identity (SUPI) and to enable network procedures. However, the UE provided no response to the AMF's request. This deviation from the protocol—where a compliant UE should reply with the GUTI—prevents the registration from progressing, causing a denial of service. While withholding the GUTI might superficially seem cautious, it violates the standard's prescribed behavior, disrupts network functionality, and does not align with any defined security measure in 5G specifications. The UE's inaction is therefore non-compliant and introduces operational insecurity by halting the authentication flow without justification. Insecure

152	152	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as expected prior to authentication. Without completing 5G-AKA to establish a mutual security context, the AMF immediately sent a Configuration Update Command (CUC) marked as "Protected" with an "Unknown" security header. The UE provided no response to this downlink message. According to 3GPP standards (TS 33.501), NAS message protection requires a valid security context established through successful 5G-AKA authentication and Security Mode Command (SMC) procedures. Transmitting protected NAS messages before this context exists violates protocol requirements, as the UE lacks the keys to validate or decrypt such messages. The UE's non-response aligns with standard security expectations: processing an unsolicited or unverifiable protected message without authentication could expose it to manipulation (e.g., forced de-registration or configuration attacks). By ignoring the invalid CUC, the UE avoided potential security risks stemming from an unauthenticated entity. Secure
153	153	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3200 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007700920104980469 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.20126700401306152 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request. The AMF responded with a Security Mode Command (SMC) that was integrity-protected (security header type 3) but was sent *before* 5G-AKA authentication completed. The SMC specified ciphering with 128-5G-EA3 but null integrity protection (5G-IA0). The UE rejected this by responding with a 5GMM Status message indicating "Invalid mandatory information." According to 3GPP standards (TS 33.501), NAS security (including SMC) must only be activated *after* successful 5G-AKA authentication, which establishes mutual authentication and fresh keys. Here, the AMF prematurely sent a protected SMC without completing 5G-AKA, leaving the UE without the necessary keys to verify the message's integrity. The UE correctly identified this violation by treating the SMC as invalid due to the missing security context, thereby preventing potential security risks like processing unverified commands. This adherence to protocol mandates—rejecting unprotected or contextless security commands—demonstrates secure behavior. Secure

154	154	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0009160041809082031 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as 5G-AKA authentication had not yet been completed, leaving the NAS security context unestablished. Subsequently, the AMF sent a Configuration Update Command (CUC) protected with both integrity protection and ciphering (security header type 2). According to 3GPP TS 33.501 and TS 24.501, a UE must not process protected NAS messages without a valid security context, as decryption and integrity verification require keys established during 5G-AKA. Here, the UE provided no response to the CUC. While ignoring the message aligns with the standard's mandate to reject unprotected or unverifiable messages, the absence of any recovery action (e.g., initiating re-registration or a Security Mode Reject) violates 3GPP requirements. The UE should have triggered a security recovery procedure to re-establish a valid context, preventing potential denial-of-service (DoS) scenarios where malformed protected messages could permanently stall the session. The lack of such remediation leaves the UE vulnerable to exploitation. Insecure
155	155	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00041294097900390625 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as expected for the initial NAS message prior to authentication. However, the AMF responded with a Deregistration Accept message marked as "Protected" without first completing the 5G-AKA authentication procedure. According to 3GPP standards (TS 33.501), NAS messages requiring protection (integrity/confidentiality) must only be sent after successful 5G-AKA establishes a security context and keys. Since 5G-AKA was not completed, the UE lacked the necessary keys to validate or decrypt the protected message. The UE's lack of response indicates it discarded the message, as processing an unverifiable protected NAS message would violate security requirements by risking acceptance of forged commands (e.g., forced deregistration). This adherence to discarding unverifiable protected messages aligns with 3GPP security protocols. Secure

156	156	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007860660552978516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.2037971019744873 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request. The AMF responded with a Security Mode Command (SMC) marked as "Integrity protected with new security context" (header type 3), but specified null algorithms for both ciphering (5G-EA0) and integrity (5G-IA0). The UE rejected this command with a Security Mode Reject (cause: unspecified), despite the AMF's message being labeled as protected. According to 3GPP standards (TS 33.501), NAS signaling mandates integrity protection after security setup, and null integrity (5G-IA0) is explicitly prohibited for SMC except in pre-authentication edge cases. Here, 5G-AKA had not completed, but the AMF's use of header type 3 falsely implied valid integrity protection while specifying null algorithms—a configuration that violates standard security requirements. The UE correctly identified this inconsistency and rejected the command, as accepting null integrity would have left subsequent messages unprotected and vulnerable to tampering. This adherence to protocol safeguards against downgrade attacks and maintains security hygiene. Secure
157	157	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006291866302490234 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as expected before security context establishment. Without completing the mandatory 5G-AKA authentication procedure, the AMF immediately responded with a Deregistration Request (UE-terminated) that was marked as "Integrity protected and ciphered" (Security Header Type 2). Since 5G-AKA had not been performed, the UE lacked the necessary security keys to decrypt or validate this message. Per 3GPP TS 33.501, a UE **must not process or respond to** protected NAS messages without an established security context, as they cannot be verified for authenticity. The UE's lack of response aligns with this security requirement, as accepting an unverifiable protected message could expose it to spoofed commands. By ignoring the message, the UE avoided potential exploitation (e.g., forced deregistration attacks) and adhered to 5G security protocols. Secure

158	158	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999805450439453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024100303649902 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF, followed by the AMF sending a subsequent Identity Request for the IMEISV in plain text (unencrypted and unprotected), as the 5G-AKA authentication had not yet been completed. The UE did not respond to this request. According to 3GPP standards (TS 24.501, section 5.6.2), a UE must only provide non-essential identities like IMEISV if the Identity Request message is integrity-protected, which requires an established security context from a completed 5G-AKA. Since the AMF's request was sent without security (plain text) and 5G-AKA was incomplete, the UE's lack of response aligns with the standard's security requirements. This prevents the exposure of sensitive device identifiers (IMEISV) over unsecured channels, mitigating potential tracking or spoofing attacks. Secure
159	159	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 13 UE provided: No response The packet capture during the test using wireshark is: 0.03987693786621094 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04032492637634277 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Roaming not allowed in this tracking area) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response message to the AMF in plaintext, as the 5G-AKA authentication had not yet been completed. The AMF then responded with a plaintext Downlink NAS Transport message containing a 5GMM Status message, indicating cause #13 ("Roaming not allowed in this tracking area"). The UE did not generate any further response to this rejection. According to 3GPP standards (TS 24.501 and TS 33.501), initial NAS messages like Identity Response are permitted to be sent unprotected before 5G-AKA establishes a security context, as encryption/integrity is not mandatory) available. The UE's cessation of communication upon receiving the rejection aligns with protocol expectations, as the 5GMM Status message (especially with cause #13) is terminal and requires no response. No sensitive post-authentication data was transmitted unprotected, and the UE avoided protocol-violating actions like retransmission or further unprotected messaging. Thus, the UE's behavior adhered to 5G security protocols. Secure

160	160	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.038893938064575195 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039427995681762695 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response, which is permissible without security as part of the initial authentication handshake since 5G-AKA had not yet been completed. The AMF then sent a Configuration Update Command as a plaintext NAS message (security header type 0), indicating no integrity protection or encryption. The UE did not respond to this command. According to 3GPP TS 24.501 and TS 33.501, after initial unprotected messages (like Identity Request/Response), NAS messages—including Configuration Update Command—must be protected once authentication is initiated, unless they are part of the explicit allowlist for unprotected exchanges (e.g., Authentication Request, Security Mode Command). The Configuration Update Command is not on this allowlist and should be protected by a NAS security context derived from 5G-AKA. Since 5G-AKA was incomplete and no security context existed, the UE's discard of the unprotected command aligns with the standard's security requirements, preventing processing of potentially malicious or tampered configuration updates. The absence of a response further indicates correct rejection, as the standard does not mandate acknowledgments for invalid messages. Secure
161	161	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0400080680847168 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04023408889770508 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Identity Response to the AMF as part of the initial NAS procedure. The AMF then responded with a Deregistration Accept message marked as "Protected," indicating it was encrypted and integrity-protected using NAS security keys. Critically, the 5G-AKA authentication had not been completed at this stage, meaning no security context (including keys) had been established between the UE and the network. According to 3GPP standards (TS 33.501), NAS protection (encryption/integrity) must not be applied until after 5G-AKA successfully establishes a shared security context. The UE's lack of response to the protected Deregistration Accept suggests it discarded the message, as it could not validate or decrypt it without valid keys—consistent with standard-mandated behavior to reject protected messages received pre-authentication. This prevents processing potentially malicious spoofed commands. While the AMF's transmission of a protected message pre-authentication was non-compliant, the UE's silent discard aligns with security requirements by avoiding undefined state transitions or error leaks. Secure

162	162	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.03969311714172363 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003500938415527 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Identity Response, which is standard behavior before 5G-AKA completion, as initial NAS messages may lack security. However, the AMF responded with a Service Accept message marked as "Protected" despite 5G-AKA not being completed, meaning no security context (keys for encryption/integrity) was established. According to 3GPP standards (TS 33.501), protected NAS messages require a valid security context derived from a completed 5G-AKA. The UE's lack of response to the protected Service Accept is appropriate, as it cannot process secured messages without keys. This aligns with security protocols, as engaging with unverifiable protected messages could risk processing malicious content. The UE correctly prioritized security by ignoring the message, while the AMF's premature protection violates the standard. Secure
163	163	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039769887924194336 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399930477142334 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Identity Response during initial NAS communication, prior to 5G-AKA completion. The AMF then sent a Deregistration Request message marked as "Integrity protected and ciphered" (security header type 2). Crucially, 5G-AKA had not been completed, meaning no shared security context (K~AMF~, derived keys) existed between the UE and AMF. According to 3GPP TS 33.501, NAS security (integrity protection and ciphering) **must not** be activated until after successful 5G-AKA authentication and key agreement. The UE provided no response to the protected Deregistration Request. This UE behavior is **secure** per 5G standards. Since no valid security context was established, the UE correctly discarded the protected message. Processing it would have required accepting security-protected NAS traffic without prior authentication—a critical violation of 3GPP security principles (TS 33.501 Sec. 6.12). The absence of a response aligns with standard security expectations: the UE ignored an illegitimate protected message received in an insecure state, preventing potential exploitation. Secure

164	164	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.03993701934814453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04126906394958496 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24338102340698242 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Identity Response. The AMF then sent a Security Mode Command (SMC) marked as "Integrity protected with new security context" (security header type 3), specifying ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA1. Crucially, this occurred **before** 5G-AKA authentication was completed, meaning no shared keys existed to validate the SMC's integrity protection. The UE correctly rejected this command with a Security Mode Reject (cause: "unspecified") because it could not verify the message's integrity without established keys. According to 3GPP standards (TS 33.501), NAS security activation must follow successful authentication and key agreement (5G-AKA). The UE adhered to this by refusing to process an integrity-protected command without a valid security context, preventing potential exploitation from unverified network instructions. Secure

165	165	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3100 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 5G- IA0 (null) Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.03973889350891113 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040254831314086914 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24545598030090332 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response in plain text, as 5G-AKA authentication had not yet been completed. The AMF responded with a Security Mode Command (SMC) in plain text, specifying the ciphering algorithm 128-5G-EA2 and the null integrity algorithm (5G-IA0). Instead of responding to the SMC with a Security Mode Complete or Security Mode Reject message as required by 3GPP TS 24.501, the UE sent a Deregistration Request (UE originating) in plain text without activating any security measures. This action occurred despite the SMC explicitly disabling integrity protection (via 5G-IA0) and before 5G-AKA established a secure context, violating the 5G security protocol which mandates that sensitive NAS messages like Deregistration Request must be integrity-protected and ciphering-enabled after SMC processing. The UE's failure to complete the security setup and its transmission of a critical service message in plain text exposed it to forgery or manipulation attacks, deviating from standard safeguards. Insecure
166	166	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.07990884780883789 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.0801239013671875 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF began with the UE sending an Authentication Response as part of the ongoing 5G-AKA procedure. Before 5G-AKA could be completed (i.e., before mutual authentication and full security context establishment), the AMF sent a Configuration Update Command to the UE. This downlink NAS message was marked as "Integrity protected" (Security Header Type 1), indicating the AMF attempted to enforce integrity protection. However, per 3GPP standards (TS 33.501), NAS security (including integrity protection) must only be activated *after* successful 5G-AKA completion, which had not yet occurred. The UE correctly recognized that the security context was incomplete and thus could not validate the message's integrity or origin. By providing no response, the UE discarded the unprotected command, adhering to the protocol's security requirements that mandate rejecting protected NAS messages received prior to security context activation. This behavior prevented potential processing of unverified or malicious instructions, maintaining security integrity. Secure

167	167	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.07818889617919922 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.07842707633972168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF as part of the ongoing 5G-AKA procedure, which had not yet been completed. The AMF then responded with a plain-text (unencrypted and unintegrity-protected) Identity Request, specifically asking for the UE's IMEISV. The UE provided no response to this request. According to 3GPP standards (TS 33.501 and TS 24.501), sensitive identities like IMEISV must only be transmitted after the establishment of a secure NAS connection, which requires successful completion of 5G-AKA to activate integrity protection and encryption. Since 5G-AKA was incomplete, the AMF's Identity Request lacked the mandatory security context, and the UE correctly refrained from disclosing the IMEISV to avoid exposing sensitive equipment information in an unprotected message. This adherence to the protocol's security requirements—prioritizing confidentiality and integrity of identity data—demonstrates compliant behavior. Secure
168	168	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.24675607681274414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.24697303771972656 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Service accept 0.4485650062561035 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, part of the ongoing 5G-AKA procedure which was not yet completed. Without completing 5G-AKA (and thus without establishing a security context), the AMF sent a Service Accept message marked as "Protected." The UE then initiated a Deregistration Request (UE originating). According to 3GPP standards (TS 33.501), NAS message protection (encryption/integrity) requires a completed 5G-AKA to derive security keys. Since 5G-AKA was incomplete, the UE should have been unable to process the "Protected" Service Accept, as it lacked the keys to validate or decrypt it. The UE's subsequent Deregistration Request—sent without security context—indicates it did not adhere to standard security protocols. Proper behavior would involve ignoring the invalid protected message or responding with a security error (e.g., "MAC failure"), not initiating a new NAS procedure. This deviation exposes a flaw in the UE's security enforcement. Insecure

169	169	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.1594829559326172 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15969610214233398 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response (uplink) to the AMF, which was transmitted in plain text because 5G-AKA authentication had not yet been completed. The AMF then responded with a DownlinkNASTransport message containing a 5GMM Status (cause #26: "Non-5G authentication unacceptable"), also sent in plain text. The UE did not send any further response to this status message. According to 3GPP standards (TS 24.501), NAS messages must be integrity-protected and encrypted after successful 5G-AKA authentication. Since 5G-AKA was incomplete, plaintext transmission was technically compliant at this stage. However, cause #26 indicates the AMF rejected the UE's authentication method, which should terminate the procedure. The UE's lack of response aligns with standard behavior, as no additional action is mandated when authentication fails. Crucially, the UE did not transmit sensitive data (e.g., SUPI, service requests) post-failure, avoiding exposure. While the plaintext exchange was necessitated by the incomplete 5G-AKA, the UE ceased communication upon receiving the error, adhering to protocol expectations for failure handling. Secure
170	170	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11972379684448242 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999678611755371 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Authentication Response to the AMF as part of the ongoing 5G-AKA procedure, which had not yet completed. Before the 5G-AKA could conclude and establish a mutually verified security context, the AMF sent a Deregistration Request message to the UE. This downlink message was marked as "Integrity protected and ciphered" (security header type 2), indicating it was encrypted and integrity-protected. However, the UE did not respond to this message. According to 3GPP standards (TS 33.501), NAS security (integrity protection and ciphering) must not be activated until after the 5G-AKA successfully completes and the Security Mode Command (SMC) procedure finalizes the security context. Since the 5G-AKA was still in progress when the AMF sent the protected Deregistration Request, the UE lacked the valid security context required to decrypt or verify the message. The UE's non-response aligns with the standard's security requirements: processing such a protected message without an active security context would violate protocol rules, potentially exposing the UE to malformed or malicious packets. By ignoring the message instead of attempting to process it, the UE adhered to security best practices, preventing potential exploitation of incomplete key establishment. Secure

171	171	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15981698036193848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16000986099243164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message after successfully completing the 5G-AKA authentication, confirming the activation of NAS security (integrity protection and encryption) as per the established security context. Immediately following this, the AMF transmitted an Identity Request for the IMEISV in plaintext (unencrypted and without integrity protection). The UE did not respond to this request. According to 3GPP standards (TS 33.501), once the Security Mode Complete is sent, all subsequent NAS messages—including those from the AMF—must be protected using the negotiated security algorithms. The AMF's plaintext Identity Request violated this requirement by bypassing encryption and integrity checks. The UE's lack of response demonstrates adherence to the standard, as it correctly discarded the unprotected message, avoiding potential exploitation (e.g., exposing sensitive identity data or processing malicious commands). This behavior aligns with security protocols mandating rejection of unprotected NAS messages post-security activation. Secure
172	172	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15984892845153809 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16009902954101562 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE completing 5G-AKA and sending a Security Mode Complete message, confirming activation of NAS security (encryption and integrity protection). The AMF then responded with an Identity Request for the GUTI, but transmitted this message in plaintext without encryption. The UE did not respond to this request. According to 3GPP standards (TS 33.501), after Security Mode Complete is sent, all subsequent NAS messages must be protected using the established security context to ensure confidentiality and integrity. The UE, having activated security, correctly identified the plaintext Identity Request as non-compliant with security protocols. By ignoring the unprotected message—rather than processing or responding to it—the UE adhered to security requirements, mitigating risks such as manipulation or eavesdropping of sensitive identity information. This behavior aligns with the standard's mandate to reject unprotected NAS messages post-security activation. Secure

173	173	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.15993309020996094 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16013097763061523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) 0.3612639904022217 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing mutual authentication and security keys. The UE then sent a Security Mode Complete message, confirming activation of NAS security (encryption and integrity protection) as required by 3GPP TS 33.501. However, the AMF responded with a Service Reject (cause 111: "Protocol error, unspecified") sent in plaintext, violating 5G security standards which mandate protected NAS messaging after security activation. Upon receiving this unprotected message, the UE correctly identified the security breach and initiated a UE-originating Deregistration Request. This action aligns with 3GPP TS 24.501, which requires UEs to discard unprotected NAS messages received after security establishment and terminate the session to prevent potential exploitation. The UE's adherence to protocol-mandated security measures demonstrates robust defensive behavior. Secure
174	174	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: c2ada16de5afa04c9abbf0b2aba327aa AUTN: 3030303030303000ee55922b5d550000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.15995287895202637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016292572021484 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message, confirming the activation of NAS security context after 5G-AKA completion. Subsequently, the AMF transmitted an Authentication Request in plaintext (unprotected). According to 3GPP standards (TS 33.501), once NAS security is activated via Security Mode Complete, all subsequent NAS messages—including Authentication Request—must be integrity-protected and encrypted if confidentiality is enabled. The UE's lack of response to this unprotected message aligns with standard requirements: a properly secured UE must discard unprotected NAS messages received after security activation to prevent potential downgrade attacks or manipulation. By ignoring the non-compliant request, the UE demonstrated correct adherence to 5G security protocols, maintaining the integrity of the established security context. Secure

175	175	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.15975189208984375 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15996503829956055 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a security context between the UE and the AMF. Following this, the UE sent a Security Mode Complete message, which should have been the first protected (encrypted and integrity-protected) uplink NAS message after security activation, as mandated by the 5G security standard (3GPP TS 33.501). Subsequently, the AMF transmitted a Service Accept message downlink in plaintext, without any encryption or integrity protection. The UE did not generate any response to this unprotected downlink message. According to 3GPP standards, once security is activated via 5G-AKA and the Security Mode Command procedure, all subsequent NAS messages—both uplink and downlink—must be protected to prevent eavesdropping, tampering, or replay attacks. The UE's failure to reject or respond to the unprotected Service Accept message (e.g., by discarding it, initiating a security error procedure, or triggering re-authentication) violates these requirements. This inaction indicates the UE processed or ignored the unsecured message instead of enforcing mandatory protection, leaving it vulnerable to man-in-the-middle attacks and compromising the integrity of the NAS signaling. Insecure
176	176	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.47094106674194336 UE to AMF UplinkNASTransport, Registration complete 0.47116804122924805 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message, indicating the conclusion of the initial NAS procedures, including a completed 5G-AKA authentication that established a secure context. Subsequently, the AMF sent an Identity Request for SUCI in plaintext format (unencrypted and without integrity protection). The UE did not respond to this request. According to 3GPP standards (TS 33.501), once 5G-AKA successfully establishes a security context, all subsequent NAS messages must be encrypted and integrity-protected to prevent eavesdropping, tampering, or downgrade attacks. The UE's lack of response to the unsecured Identity Request aligns with these requirements, as processing an unprotected message after security activation would violate the standard and expose vulnerabilities. By ignoring the request, the UE demonstrated adherence to security protocols, avoiding potential exploitation. Insecure

177	177	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 1230c172c0fe20b56039f8264c2856d4 AUTN: 2d236d5db431900054adfe579b1ec661 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.4670701026916504 UE to AMF UplinkNASTransport, Registration complete 0.46730613708496094 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message to the AMF, indicating the conclusion of its registration procedure. Subsequently, the AMF responded with an unencrypted and unprotected Authentication Request message containing a RAND, AUTN, and other parameters. This sequence is problematic because the Registration Complete message is typically sent *after* successful authentication and security activation in 5G standalone deployments, implying that a security context should already be established at this stage. According to 3GPP standards (TS 33.501), once the security context is active (post-5G-AKA completion), all NAS messages must be integrity-protected and encrypted to prevent eavesdropping and tampering. The AMF's transmission of a plaintext Authentication Request after the UE signaled Registration Complete violates this requirement, as such sensitive authentication material should never be sent unprotected. The UE's lack of response to this unprotected message aligns with the standard's security expectations: a compliant UE must reject or ignore unsecured NAS messages once security is activated, as processing them could expose vulnerabilities to man-in-the-middle attacks or credential theft. Thus, the UE's inaction demonstrates adherence to 5G security protocols. Secure
178	178	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 6.593172073364258 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.593342065811157 AMF to UE SACK (Ack=24, Arwnd=106401) , DownlinkNASTransport, Identity request 6.797163009643555 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE sent a Registration Complete message to the AMF, indicating successful establishment of the security context. The AMF then responded with an Identity Request for SUCI, transmitted in plaintext without encryption or integrity protection. Instead of providing the requested SUCI, the UE initiated a Deregistration Request (UE originating). According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA is completed, all subsequent NAS messages must be integrity-protected and encrypted to prevent tampering and eavesdropping. The AMF's plaintext Identity Request violated this requirement, as it is a sensitive command that could be forged by attackers to harvest SUPI/SUCI. The UE's response—ignoring the unprotected request and triggering deregistration—aligns with security protocols, which mandate discarding unverified messages and terminating the session to mitigate potential threats like bidding-down attacks or identity theft. This demonstrates the UE correctly enforced security policies by rejecting the insecure AMF message and safeguarding subscriber identity. Secure

179	179	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.265115976333618 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2653589248657227 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.469132900238037 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a NAS security context. The UE sent a protected Registration Complete message, confirming security activation. The AMF then responded with an unprotected Configuration Update Command (security header type 0), violating 3GPP TS 24.501 mandates requiring integrity protection for all NAS messages post-security activation. Instead of discarding this unprotected message or initiating recovery (e.g., re-registration), the UE processed the command and sent a protected Deregistration Request. This action demonstrates a critical security flaw: the UE accepted and acted upon an unprotected NAS directive after security context establishment. Per 3GPP standards, UEs must reject all unprotected NAS messages post-authentication to prevent manipulation by adversaries. By processing the plaintext command, the UE exposed itself to potential spoofing attacks where an attacker could inject malicious configuration updates or trigger deregistration. Insecure
180	180	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.5163559913635254 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.5165369510650635 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.5166728496551514 AMF to UE DownlinkNASTransport, Configuration update command 2.7203638553619385 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE completing 5G-AKA, establishing a secure context for NAS communication. The UE then sent an Uplink NAS Transport (including Registration Complete and PDU Session Establishment Request). The AMF responded with two Downlink NAS Transport messages containing a Configuration Update Command, both sent as plaintext (security header type 0), lacking encryption or integrity protection. Subsequently, the UE initiated deregistration by sending a Deregistration Request (UE originating). According to 3GPP standards (TS 33.501), after successful 5G-AKA, all NAS messages must be integrity-protected and encrypted, with only rare exceptions (e.g., Authentication Reject, 5GMM Status without security). The Configuration Update Command is not an allowed exception, as it may carry sensitive network parameters. The UE should have discarded this unprotected message and potentially initiated recovery procedures. Instead, the UE processed it and triggered deregistration, violating security requirements by accepting an unprotected command that could be maliciously injected. This exposes the UE to spoofed network attacks. Insecure

181	181	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3100 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: No response The packet capture during the test using wireshark is: 2.4268798828125 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4271068572998047 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.42726993560791 AMF to UE DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Downlink NAS Transport message carrying an Authentication Request, which included RAND, AUTN, ABBA, and ngKSI parameters. Crucially, this Authentication Request was sent in plaintext, as required by the 5G-AKA protocol before security establishment. However, the UE failed to respond to this Authentication Request, despite protocol mandates (3GPP TS 33.501) requiring either an Authentication Response (if AUTN validation succeeds) or an Authentication Failure message (if validation fails). This lack of response violates 5G NAS procedure requirements, as the UE must actively participate in the authentication process to either complete key derivation or explicitly reject invalid credentials. The silence prevents the AMF from progressing security setup or diagnosing failures, leaving the session unsecured and non-compliant with 3GPP standards. Insecure

182	182	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.5082509517669678 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 0.5084729194641113 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Configuration update command 0.5085830688476562 AMF to UE DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a secure context for encrypted and integrity-protected NAS communication. The UE then sent a protected UL NAS TRANSPORT message containing multiple requests (e.g., PDU session establishment, deregistration). The AMF responded with an unprotected SERVICE REJECT (5GMM cause 111: "Protocol error, unspecified"), transmitted in plaintext despite the active security context. The UE exhibited no further establishment request, UplinkNASTransport, Deregistration request (UE originating) completion, all subsequent NAS messages—including rejections—must be integrity-protected and encrypted unless explicitly exempted. SERVICE REJECT is not among the allowed exceptions (e.g., authentication failures or security mode commands) when a security context exists. The UE correctly discarded the unprotected SERVICE REJECT, as processing it could expose vulnerabilities to downgrade or injection attacks. Its lack of response aligns with protocol requirements to ignore unsecured messages post-authentication, mitigating potential threats. Secure

183	183	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000eeb598a00f560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5556139945983887 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.555833101272583 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5559549331665039 AMF to UE DownlinkNASTransport, Authentication request 0.7596380710601807 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Configuration Update Command and then sent an Authentication Request message in plain text (as expected, since no security context existed yet), containing RAND, AUTN, and ABBA parameters. Instead of responding with a standard Authentication Response or Authentication Failure message as mandated by 3GPP TS 33.501 for 5G-AKA, the UE abruptly sent a Deregistration Request (UE originating). This deviation occurred despite the authentication procedure being incomplete and the UE having no established security context to protect the deregistration message. According to 3GPP standards, upon receiving an Authentication Request, the UE must either validate the AUTN and return an Authentication Response or explicitly reject it with an Authentication Failure message indicating the cause (e.g., MAC failure, synch failure). The UE's premature deregistration bypasses this critical security protocol, fails to report authentication issues to the network, and could indicate improper handling of authentication challenges or potential vulnerabilities to desynchronization attacks. Insecure

184	184	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 4.666133165359497 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 4.66637396812439 AMF to UE SACK (Ack=10, Arwnd=106401) , DownlinkNASTransport, Configuration update command 4.666524171829224 AMF to UE DownlinkNASTransport, Identity request 4.8701331615448 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a security context for encrypted and integrity-protected NAS communication. The UE sent an Uplink NAS Transport (Registration Complete + PDU Session Establishment Request). The AMF responded with a Configuration Update Command and an unprotected (plain) Identity Request for the UE's IMEI, violating 3GPP TS 33.501, which mandates NAS encryption after 5G-AKA. Instead of complying, the UE initiated a Deregistration Request (UE originating). This action aligns with 3GPP TS 24.501, which requires UEs to discard unprotected NAS messages post-authentication and allows deregistration to mitigate potential security threats like downgrade attacks or credential theft. The UE correctly prioritized security enforcement over network demands. Secure
185	185	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 62 UE provided: No response The packet capture during the test using wireshark is: 2.4262688159942627 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4268429279327393 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.427194833755493 AMF to UE DownlinkNASTransport, Registration reject (No network slices available) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing the 5G-AKA authentication, establishing a security context. The UE then sent an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request. The AMF responded with two downlink messages: first, a Configuration Update Command (whose security status is unspecified in the summary), and second, a Registration Reject with 5GMM Cause #62 ("No network slices available"), explicitly noted as sent in plaintext without encryption or integrity protection. The UE did not respond to the Registration Reject. According to 3GPP standards (TS 24.501), once 5G-AKA completes, all subsequent NAS messages must be integrity-protected to prevent tampering and ensure authenticity. The UE is required to verify integrity and discard any unprotected NAS messages received after security context establishment. Here, the Registration Reject was sent plain, violating this mandate. The UE's lack of response indicates it correctly identified the unprotected message as invalid and ignored it, aligning with standard-prescribed behavior to mitigate potential attacks (e.g., forged rejections). Thus, the UE acted securely by adhering to 5G security protocols. Secure

186	186	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3200 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 5.633437156677246 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 5.634006023406982 AMF to UE SACK (Ack=11, Arwnd=106496) , DownlinkNASTransport, Security mode command 5.634031057357788 UE to AMF SACK (Ack=8, Arwnd=106454) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE sent an unprotected PDU session establishment request via UL NAS TRANSPORT. The AMF responded with a Security Mode Command (plain, no integrity protection) specifying ciphering (5G-EA6) and integrity (128-5G-IA1) algorithms. Instead of activating security and replying with a Security Mode Complete message as required by 3GPP TS 33.501, the UE immediately sent an unprotected Deregistration Request. This violates the 5G security protocol, which mandates that the UE must complete the security activation procedure before transmitting any subsequent NAS messages (including Deregistration Request). By bypassing security activation, the UE exposed sensitive NAS signaling (e.g., deregistration details) to potential tampering or eavesdropping. Insecure
187	187	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 2.197134017944336 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 2.197467088699341 AMF to UE SACK (Ack=11, Arwnd=106334) , DownlinkNASTransport, Configuration update command 2.1975760459899902 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a UL NAS TRANSPORT message containing multiple elements (Registration Complete, PDU Session Establishment Request, and Deregistration Request) after 5G-AKA authentication had been successfully completed. Following this, the AMF transmitted an Identity Request message in plaintext (unencrypted and without integrity protection), explicitly requesting the UE's IMEISV identity. The UE did not respond to this request. According to 3GPP security standards (TS 33.501), once 5G-AKA completes, all subsequent NAS messages—including Identity Requests—must be integrity-protected and encrypted to mitigate eavesdropping, spoofing, and privacy breaches. The AMF's plaintext Identity Request violates this requirement, as sensitive identity requests must never be sent unprotected after security context establishment. The UE's lack of response aligns with 3GPP-mandated behavior (TS 24.501, Section 5.4.1.2), which dictates that UEs must ignore and discard any unprotected NAS messages received post-security activation to prevent potential attacks exploiting unsecured channels. By refusing to disclose the IMEISV in response to an unprotected command, the UE adhered to security protocols, avoiding exposure of sensitive information to potential interception or manipulation. Secure

188	188	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.8423888683319092 gNB to AMF UEContextReleaseComplete, InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.8428249359130859 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA authentication, establishing a security context for encrypted and integrity-protected NAS communication. The UE initiated a service request for mobile-originated data, which was sent uplink to the AMF. In response, the AMF sent a deregistration accept message (indicating UE-terminated deregistration) as plain text, without leveraging the established security context for encryption or integrity protection. The UE exhibited no response to this downlink message.According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA completes, all subsequent NAS messages—including deregistration accept—must be confidentiality and integrity protected if a security context exists. The UE's lack of action aligns with the mandated security protocol: upon receiving an unprotected NAS message while possessing an active security context, the UE must discard the message and refrain from processing it to prevent exploitation. This behavior demonstrates adherence to 5G security requirements by rejecting unsecured communications that could indicate tampering or spoofing. Secure
189	189	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.602246046066284 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.602970123291016 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request in plaintext (as expected, since NAS security activation had not yet been initiated for this session). The AMF then responded with a Security Mode Command (SMC) message, which was sent as a plain NAS message (security header type 0) without integrity protection or encryption. This SMC message is intended to activate the agreed-upon security algorithms (5G-EA6 for encryption and 128-5G-IA2 for integrity) for subsequent NAS signaling. Critically, the UE provided no response to this SMC. According to 3GPP standards (TS 33.501), the Security Mode Command **must** be integrity protected to ensure its authenticity and prevent tampering. This is because the SMC instructs the UE to enable specific security algorithms; an unprotected SMC could be forged or altered by an attacker to downgrade security or disrupt service. The UE's lack of response aligns with 3GPP requirements: upon receiving an unprotected SMC after a completed 5G-AKA (which establishes a security context), the UE **must** discard the message and **not** proceed with security activation. Responding to an unprotected SMC would expose the UE to manipulation of security parameters. By ignoring the unsecured command, the UE correctly adhered to the standard, preventing potential security exploits like algorithm downgrade attacks or false security activation. Secure

190	190	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1010 RAND: 7479eaccb74fb3be01aa8b2b6ff1abcb AUTN: dd84e27507488000bb521f82528f6f6e ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 16.614274978637695 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 16.614504098892212 AMF to UE SACK (Ack=22, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request via an InitialUEMessage, indicating a request for mobile-originated data. The AMF responded with a DownlinkNASTransport containing an Authentication Request, sent in plaintext without encryption or integrity protection, which included RAND, AUTN, ABBA parameters, and ngKSI for a native security context. Although the test summary noted that 5G-AKA was previously completed, implying the UE possessed a valid native security context (as referenced by ngKSI=2), the UE's Service Request was sent without the mandated NAS integrity protection. According to 3GPP TS 24.501, Section 5.4.1.2, the Service Request must be integrity protected when a NAS security context exists. The absence of such protection—evident from the plaintext description in the packet capture and the lack of security indicators—exposes the message to tampering or forgery. Furthermore, the UE's failure to respond to the Authentication Request suggests potential processing issues, but the primary vulnerability lies in the unprotected Service Request, violating 5G security protocols. Insecure

191	191_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1010 RAND: 765bcfb5ee4bd70eb854f2deac92aea9 AUTN: 7f72e2496ad28000fd0cf5cd8a2492b7 ngKSI_TSC: Native security context ngKSI_KSI: 4 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 8.671967029571533 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.672221899032593 AMF to UE SACK (Ack=14, Arwnd=106496) , DownlinkNASTransport, Authentication request 8.874675035476685 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request to the AMF, initiating communication. The AMF responded with a Downlink NAS Transport containing an Authentication Request, which included RAND, AUTN, ABBA (1010), and ngKSI (KSI=4) for a native security context. Crucially, this message was sent unencrypted, as 5G-AKA had not yet established a security context for this session. The UE rejected the authentication attempt by responding with an Authentication Failure message, specifying the cause "ngKSI already in use," indicating that the ngKSI value 4 was already associated with an active security context in the UE. According to 3GPP standards (TS 24.501, Section 5.4.1.3), a UE **must** reject an Authentication Request if the provided ngKSI matches an existing native security context stored in the UE. Allowing re-use of an active ngKSI could enable security context confusion or forced de-synchronization attacks, where an attacker might overwrite valid keys. By explicitly rejecting the request and preserving the existing context, the UE adhered to the protocol's security requirements. This prevents unauthorized invalidation of established security parameters and maintains consistency between the UE and network. The plaintext transmission of the Authentication Request is standard-compliant, as NAS security is only applied post-successful authentication. Secure
192	192	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 35.06067895889282 UE to AMF SACK (Ack=27, Arwnd=106496) , UplinkNASTransport, Service request 35.06101393699646 AMF to UE SACK (Ack=36, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, which establishes a secure context, the UE sent an encrypted Service Request to the AMF. The AMF responded with an Identity Request for the TMSI, transmitted in plaintext without encryption or integrity protection. The UE correctly ignored this request and provided no response. According to 3GPP security standards (TS 33.501), once a secure context is established via 5G-AKA, all subsequent NAS messages—including Identity Requests—must be confidentiality and integrity protected to prevent eavesdropping and tampering. The UE's refusal to process an unprotected NAS message aligns with these requirements, as accepting it could expose sensitive data or enable impersonation attacks. The AMF's failure to encrypt the Identity Request violates the standard, but the UE's non-compliance with the insecure command represents secure behavior. Secure

193	193	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 9.49011492729187 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.490720987319946 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating communication by sending a Service Request via an InitialUEMessage, indicating mobile-originated data as the establishment cause. The AMF responded with a DownlinkNASTransport containing a Configuration Update Command, which was marked as "Protected" but exhibited an "Unknown" security header type in the test summary. Crucially, the UE provided no response to this command. According to 3GPP standards (TS 33.501), after successful 5G-AKA authentication, all subsequent NAS messages must be integrity-protected and optionally encrypted using the established security context. The "Unknown" security header suggests either an unsupported protection type or a malformed security header that the UE could not validate. The UE's lack of response aligns with standard security requirements: if a NAS message fails integrity verification or uses an unrecognized security header, the UE must silently discard it to prevent processing potentially tampered commands. This behavior ensures that unverified configuration updates—which could compromise network security—are not executed. Since the UE discarded the suspicious message instead of processing it or exposing an error, it adhered to 3GPP security protocols. Secure
194	194	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 18.81248188018799 UE to AMF UplinkNASTransport, Service request 18.8126699924469 AMF to UE SACK (Ack=18, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction involved the UE sending a Service Request after completing 5G-AKA, which should have established a security context for encrypted NAS communication. The AMF responded with an Authentication Reject message sent in plaintext (unencrypted), to which the UE provided no response. According to 3GPP standards (TS 33.501, clause 6.7), once 5G-AKA is successfully completed, all subsequent NAS messages—including those from the network—must be integrity-protected and encrypted using the negotiated keys, with no explicit exception for Authentication Reject after successful authentication. The UE's acceptance of an unencrypted Authentication Reject message, without challenging the lack of security protection (e.g., via a security mode rejection or ignoring the message), violates this requirement. This indicates the UE processed a critical security command without verifying its integrity or confidentiality, exposing it to potential downgrade attacks or forged rejection messages by adversaries. Insecure

195	195_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 9.680989980697632 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.681249141693115 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Identity request 9.884641170501709 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request (unencrypted, as permitted by 3GPP for initial connection setup), followed by the AMF responding with an Identity Request demanding the SUCI. Critically, this Identity Request was sent in plaintext without encryption or integrity protection, despite the prior completion of 5G-AKA, which established a valid security context. The UE then transmitted the SUCI in an Identity Response. According to 3GPP TS 33.501, after 5G-AKA completion, all subsequent NAS messages carrying sensitive data like SUCI **must** be confidentiality-protected to prevent eavesdropping and tracking. The SUCI, being a privacy-sensitive identifier, requires encryption when transmitted. The UE's failure to enforce this protection—by responding to an unprotected Identity Request with an unencrypted SUCI—violates the standard, as it exposes subscriber identity to potential interception. The network should have activated NAS security via Security Mode Command before requesting SUCI, but the UE remains responsible for not sending protected data over an insecure channel. Insecure
196	196	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 9.49011492729187 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.490720987319946 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating a Service Request via an InitialUEMessage after completing 5G-AKA authentication, which establishes NAS security keys. The AMF responded with a Configuration Update Command message, marked as "Protected" in the test summary. However, the security header type was reported as "Unknown," and the UE did not generate any response (e.g., Configuration Update Complete or Reject). According to 3GPP standards (TS 24.501), after 5G-AKA, all NAS messages must be integrity-protected and encrypted unless explicitly exempted. The "Unknown" security header suggests potential issues—such as an invalid header value, incorrect integrity protection, or ciphering—that would prevent the UE from verifying the message. The UE's lack of response aligns with standard security protocols: it discarded the unverifiable message without processing it, avoiding potential exploitation of corrupted or malicious payloads. This behavior demonstrates adherence to 5G security requirements by prioritizing message validation over forced processing. Secure

197	197	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005860328674316406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (UE shall) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request via an InitialUEMessage (NAS message), indicating the start of the registration process. Since 5G-AKA authentication had not yet been performed, no security context existed between the UE and AMF. Despite this, the AMF responded with a DownlinkNASTransport message containing a Deregistration Request (UE-terminated), which was marked as "Integrity protected and ciphered" (security header type 2). The UE did not generate any response to this message. According to 3GPP standards (TS 33.501), (NAS security (integrity protection and ciphering) must not be applied before 5G-AKA completes and a security context is established. The UE, lacking keys to verify or decrypt the protected message, correctly ignored it, as processing such a message without a valid security context would violate protocol security requirements. The absence of a response aligns with secure behavior, as reacting to an unverifiable protected message could expose vulnerabilities. Secure
198	198	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15979790687561035 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16023778915405273 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA and sending a Security Mode Complete message, confirming the activation of NAS security (integrity protection and encryption) as negotiated during the Security Mode Command procedure. Subsequently, the AMF sent an Identity Request for the GUTI in plaintext, without any security protection. The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once NAS security is activated (after Security Mode Complete), all subsequent NAS messages must be integrity-protected and encrypted. The UE is required to discard any unprotected NAS messages received after security activation to prevent potential attacks, such as downgrade or impersonation attempts. By ignoring the plaintext Identity Request, the UE adhered to this security requirement, demonstrating correct validation of message protection and avoiding exposure of sensitive identity information. Secure

199	199	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.1600339412689209 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602790355682373 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication and sending a Security Mode Complete message to the AMF, the UE received a subsequent Identity Request (for IMEISV) from the AMF sent in plaintext, without encryption or integrity protection. According to 3GPP standards (TS 33.501), once 5G-AKA concludes and NAS security context is activated via Security Mode Command/Complete, all subsequent NAS messages must be protected with both integrity and encryption. The UE's lack of response to the unprotected Identity Request aligns with 3GPP security requirements, as processing such a message would violate the mandated protection mechanisms. By discarding the unsecured request instead of exposing sensitive identity information (IMEISV), the UE correctly enforced security policies, preventing potential exploitation of unprotected communication. Secure
200	200	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.1511218547821045 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15138006210327148 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message, confirming successful activation of NAS security after 5G-AKA authentication. Subsequently, the AMF sent an Identity Request for SUCI in plaintext (unencrypted and without integrity protection). The UE provided no response to this request. According to 3GPP standards (TS 33.501), after Security Mode Complete is sent, the UE must enforce NAS security context activation, meaning all subsequent messages must be integrity-protected and encrypted if confidentiality is required. The UE's refusal to process the unprotected Identity Request aligns with these requirements, as accepting plaintext messages post-security activation would violate core security principles by exposing sensitive data (like SUCI) and risking manipulation. The lack of response demonstrates the UE correctly discarded the non-compliant message, preventing potential exploits. Secure

201	201	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.15867114067077637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15893101692199707 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a security context, and sending a Security Mode Complete message to confirm activation of encryption and integrity protection for subsequent NAS communications. The AMF then responded with an Identity Request for the UE's IMEI, transmitted in plaintext without the mandated security protections. The UE correctly did not respond to this request. According to 3GPP standards (TS 33.501), after Security Mode Complete is sent, all subsequent NAS messages—including Identity Request—must be confidentiality-protected (encrypted) and integrity-protected to prevent eavesdropping and tampering. The UE's lack of response aligns with the standard's security requirements, as it discarded an unprotected message that should have been secured, thereby avoiding potential exposure of sensitive identity information. Secure
202	202	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.15091204643249512 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15117597579956055 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of the 5G-AKA authentication, establishing a security context. The UE then sent a Security Mode Complete message, confirming activation of NAS security (integrity protection and ciphering) as mandated by 3GPP TS 33.501. Immediately after, the AMF transmitted an Identity Request for SUCI in plaintext (unprotected). Critically, the UE did not respond to this request. According to 3GPP standards (TS 24.501, Section 4.4.5), once NAS security is activated via Security Mode Complete, all subsequent NAS messages—including Identity Request—**must** be integrity-protected and ciphered. The AMF's plaintext Identity Request violated this requirement, as unprotected messages post-security activation are forbidden unless explicitly exempt (e.g., during initial registration). The UE's non-response aligns with standard security protocols, which dictate that such unprotected messages must be discarded to prevent potential downgrade attacks or manipulation. By ignoring the non-compliant request, the UE upheld security obligations and avoided exposing sensitive identity information (SUCI) over an insecure channel. Secure

203	203	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15087509155273438 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15108299255371094 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE completing the 5G-AKA authentication, establishing a secure context, and sending a Security Mode Complete message—indicating activation of NAS security (encryption and integrity protection) as mandated by 3GPP standards (TS 33.501). Subsequently, the AMF sent an Identity Request for the GUTI, but transmitted this message in plaintext without encryption or integrity protection. The UE did not respond to this request. According to 3GPP specifications, after Security Mode Complete is sent, all subsequent NAS messages must be protected to prevent eavesdropping or tampering. The AMF's plaintext Identity Request violates this requirement. The UE correctly ignored the unsecured message, aligning with standard security protocols (TS 24.501), which dictate that UEs must discard unprotected messages once security is activated to avoid processing potentially compromised instructions. This non-response demonstrates adherence to security norms. Secure
204	204	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15074801445007324 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15094995498657227 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE sent a Security Mode Complete message (indicating activation of negotiated security algorithms) followed by a Registration Request. The AMF responded with an Identity Request for the IMEISV in plaintext, without encryption or integrity protection. The UE provided no response to this request. According to 3GPP standards (TS 33.501), once security mode procedures are complete and a security context is established (post–Security Mode Complete), all subsequent NAS messages—including Identity Request—must be integrity-protected and encrypted. The UE's lack of response to an unprotected post-security-activation message aligns with 5G security requirements, as processing such a message could expose vulnerabilities to downgrade or spoofing attacks. By ignoring the non-compliant plaintext request, the UE upheld the security context. Secure

205	205	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4575481414794922 UE to AMF UplinkNASTransport, Registration complete 0.4577751159667969 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message to the AMF after successfully completing 5G-AKA authentication, which establishes a secure NAS signaling context. Following this, the AMF sent an Identity Request message to the UE, explicitly requesting the SUCI identity. Critically, this downlink message was transmitted in plaintext without encryption or integrity protection. The UE did not respond to this request. According to 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages—including downlink commands like Identity Request—must be confidentiality and integrity protected to prevent eavesdropping, tampering, or spoofing. Transmitting such a sensitive request (which could expose subscriber privacy via SUCI) in plaintext violates these requirements. The UE's lack of response aligns with security expectations, as it correctly ignored an unprotected message that should have been secured under the active security context. This prevents potential attacks where an adversary could harvest identities or inject malicious requests. Secure
206	206	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4691789150238037 UE to AMF UplinkNASTransport, Registration complete 0.46941208839416504 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After the successful completion of the 5G-AKA authentication procedure, which establishes a secure context between the UE and the AMF, the UE sent a Registration Complete message (indicating the conclusion of the registration process). Subsequently, the AMF transmitted an Identity Request message in plaintext (unencrypted and without integrity protection), explicitly requesting the UE's SUCI. The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA is completed, all subsequent NAS messages must be confidentiality and integrity-protected using the derived security keys to mitigate eavesdropping, tampering, and replay attacks. The UE's failure to respond to an unprotected Identity Request aligns with these requirements, as processing or acknowledging such a message could expose sensitive information or facilitate security compromises. By ignoring the unsecured request, the UE adhered to the protocol's security mandates, which prohibit handling non-protected NAS messages post-authentication. Secure

207	207	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 2.019134998321533 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.0193519592285156 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Identity request 3.000807046890259 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a secure context, and sending a protected Registration Complete message. Subsequently, the AMF transmitted an Identity Request for SUCI in plaintext (unencrypted and unprotected), followed by a retransmission when no response was received. According to 3GPP standards (TS 33.501), after 5G-AKA completion, all NAS messages must be integrity-protected and encrypted to ensure confidentiality and security. The UE correctly ignored the unprotected Identity Request, as processing such messages would violate 5G security protocols and expose vulnerabilities to eavesdropping or manipulation. The lack of response aligns with the requirement to reject unprotected communications once security is activated, demonstrating adherence to the standard. Secure
208	208	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4989509582519531 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.49918699264526367 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication and sending a Registration Complete message, which should have activated NAS security context (integrity protection and encryption) as per 3GPP TS 33.501. Subsequently, the AMF sent an Identity Request for SUCI explicitly in plaintext (unencrypted and without integrity protection), as confirmed by the test summary and packet capture. The UE did not respond to this request. According to 3GPP standards, once 5G-AKA completes and a security context is established (after Registration Complete), all subsequent NAS messages—including Identity Request—must be confidentiality-protected and integrity-protected to mitigate eavesdropping, tampering, and replay attacks. The UE's lack of response aligns with security requirements: TS 33.501 mandates that UEs must discard unprotected NAS messages received after security activation to prevent processing potentially malicious or forged commands. By ignoring the plaintext Identity Request instead of complying or exposing sensitive data (like SUCI), the UE adhered to security protocols, demonstrating correct behavior. Secure

209	209	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48286890983581543 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48304104804992676 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a secure context, and sending a Registration Complete message to the AMF. Subsequently, the AMF transmitted an Identity Request message in plaintext (unencrypted and without integrity protection), explicitly requesting the UE's SUCI. Crucially, this request occurred *after* 5G-AKA had been completed, meaning the security context was active and all NAS messages should have been protected per 3GPP standards (TS 33.501). The UE correctly provided no response to this unprotected request. According to 5G security protocols, once authentication is finalized, UEs must reject any unprotected NAS messages (except for specific, pre-defined exceptions like Service Reject or Authentication Reject, which do not apply here). By ignoring the plaintext Identity Request instead of complying or exposing sensitive credentials like SUCI, the UE adhered to the standard's security requirements, preventing potential eavesdropping or manipulation of unprotected exchanges. Secure
210	210	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48984408378601074 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4900491237640381 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA and sending a Registration Complete message, indicating that a security context (including keys for encryption and integrity protection) was established between the UE and AMF. The AMF then responded with an Identity Request message, explicitly asking for the UE's SUCI, but transmitted this message in plaintext without encryption or integrity protection. Critically, the UE provided no response to this request. According to 3GPP security standards (TS 33.501), once 5G-AKA is completed and NAS security is activated, all subsequent NAS messages—including Identity Requests—**must** be protected with integrity and confidentiality. Transmitting such a sensitive request (for SUCI, a privacy-sensitive identifier) unprotected violates these requirements, as it exposes the UE to risks like eavesdropping, spoofing, or privacy compromise. The UE's lack of response aligns with the standard's security protocols: It correctly rejected the unprotected message, as processing it would have undermined the established security context. This non-response demonstrates adherence to 3GPP safeguards against unprotected post-authentication commands. Secure

211	211	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 4.666033029556274 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 4.666288137435913 AMF to UE SACK (Ack=20, Arwnd=106429) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE sent a Registration Complete message to the AMF, indicating successful security context establishment. Subsequently, the AMF sent an unprotected (plain) Identity Request message to the UE, demanding the TMSI identity. The UE provided no response to this request. According to 3GPP standards (TS 24.501 and TS 33.501), once 5G-AKA completes, all subsequent NAS messages—including Identity Request—must be integrity-protected and encrypted to prevent eavesdropping or manipulation. The UE's lack of response aligns with the standard's security requirements: it must reject or ignore any unprotected NAS messages received after authentication, as processing them could expose sensitive data or enable attacks. By discarding the unsecured Identity Request instead of complying, the UE adhered to 5G security protocols. Secure
212	212	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.7599759101867676 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.7602298259735107 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating communication via an Uplink NAS Transport message (PDU session establishment request) after completing 5G-AKA authentication. The AMF responded with a Downlink NAS Transport containing an Identity Request for the UE's IMEISV, sent in plaintext without encryption or integrity protection. The UE did not respond to this request. According to 3GPP standards (TS 33.501), once 5G-AKA completes and a security context is established, all subsequent NAS messages—including Identity Requests—**must** be confidentiality and integrity protected to prevent eavesdropping and tampering. The UE's lack of response aligns with the standard's security requirements, as it correctly ignored an unprotected NAS message received after authentication, avoiding potential exposure of sensitive identity information (e.g., IMEISV) to attackers. This behavior demonstrates adherence to 5G security protocols by enforcing mandatory protection of post-authentication signaling. Secure

213	213	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.7595288753509521 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.7598080635070801 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began after the completion of 5G-AKA, which establishes a security context between the UE and AMF. The UE initiated a UL NAS TRANSPORT containing a PDU session establishment request. The AMF responded with a downlink Identity Request message, sent in plain text without encryption or integrity protection, asking for the SUCI. The UE provided no response to this request. According to 3GPP standards (TS 33.501), after successful 5G-AKA, all subsequent NAS messages must be protected using the established security context to ensure confidentiality and integrity. The Identity Request—being a post-authentication message—must be encrypted and integrity-protected. Since the AMF sent this request unprotected, the UE correctly identified a security violation. By ignoring the request, the UE adhered to the standard, which mandates discarding unprotected messages that require security after authentication. This prevents potential exploits like eavesdropping or manipulation of unprotected identity requests. Secure
214	214	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.7997701168060303 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.8000459671020508 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began after the completion of 5G-AKA, establishing mutual authentication and a security context between the UE and AMF. The UE initiated a PDU session establishment request via an Uplink NAS Transport message, expecting subsequent NAS communications to be protected per 3GPP standards. However, the AMF responded with an Identity Request for the TMSI, sent in plaintext without encryption or integrity protection. The UE correctly did not respond to this request. According to 3GPP TS 33.501 and TS 24.501, once 5G-AKA completes, all NAS messages—including Identity Requests—must be confidentiality and integrity protected to prevent eavesdropping, tampering, or identity tracking. The UE's non-compliance with the unprotected request aligns with security requirements, as responding would risk exposing sensitive information and undermine the established security context. By ignoring the plaintext message, the UE adhered to protocol mandates designed to safeguard against downgrade attacks and unauthorized data disclosure. Secure

215	215	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.5246391296386719 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5248539447784424 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5249319076538086 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began after the successful completion of 5G-AKA, establishing a NAS security context. The UE sent an Uplink NAS Transport containing Registration Complete and a PDU Session Establishment Request. Subsequently, the AMF transmitted two downlink messages: a Configuration Update Command and an Identity Request (seeking IMEISV), both sent in plaintext without encryption or integrity protection. The UE provided no response to the Identity Request. According to 3GPP standards (TS 33.501), once 5G-AKA completes and a NAS security context is activated, all subsequent NAS messages must be integrity-protected and encrypted to prevent eavesdropping, tampering, and spoofing. The AMF's transmission of an Identity Request in plaintext violates this requirement, as post-authentication messages should never be sent unprotected. The UE's lack of response aligns with 3GPP specifications (TS 24.501 § 4.4.5), which mandate that UEs **discard** unprotected NAS messages received after security activation to mitigate potential exploits (e.g., fake network commands). By ignoring the unsecured request, the UE correctly prioritized security over compliance, avoiding exposure of sensitive identity data (IMEISV) and demonstrating adherence to 5G security protocols. Secure.
216	216	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.5509819984436035 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5512139797210693 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5513119697570801 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE and AMF successfully completing 5G-AKA, establishing a secure context for subsequent NAS communications. The UE then sent an UplinkNASTransport message containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Configuration Update Command and an unprotected (plain) Identity Request message demanding the UE's SUCI. Critically, the UE provided no response to this Identity Request. According to 3GPP standards (TS 33.501 and TS 24.501), after 5G-AKA completion, all NAS messages—except for a established set of pre-authentication exceptions—must be integrity-protected and encrypted using the established security context. The Identity Request here was sent post-authentication and post-Registration Complete (indicating security activation), yet it was transmitted unprotected. The UE's lack of response aligns with 3GPP mandates: receiving an unprotected NAS message after security activation constitutes a security violation, and the UE must discard such messages to prevent potential exploits (e.g., bidding-down attacks or credential harvesting). This behavior demonstrates adherence to security protocols, as responding would have risked exposing sensitive information (SUCI) over an unprotected channel. Secure

217	217	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.531268835067749 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5314879417419434 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5316059589385986 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request, following the completion of 5G-AKA mutual authentication. Subsequently, the AMF sent two downlink messages: a Configuration Update Command and an Identity Request for the IMEISV. Critically, the Identity Request was transmitted in plaintext without encryption or integrity protection. According to 3GPP standards (TS 33.501), after 5G-AKA successfully establishes a security context, all subsequent NAS messages—including Identity Request—must be confidentiality and integrity protected to prevent eavesdropping, tampering, or impersonation attacks. The UE's lack of response to this unprotected Identity Request aligns with 5G security requirements, as processing an unprotected security-sensitive message post-authentication would violate protocol specifications and expose the device to risks like identity theft or location tracking. By ignoring the request, the UE correctly enforced security policies mandating protected NAS exchanges once keys are established. Secure
218	218	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 13.027754783630371 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 13.028036832809448 AMF to UE SACK (Ack=11, Arwnd=106361) , DownlinkNASTransport, Configuration update command 13.02815294265747 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a UL NAS Transport message containing Registration Complete and a PDU Session Establishment Request after completing 5G-AKA, which establishes a NAS security context. Subsequently, the AMF sent a Downlink NAS Transport message containing an Identity Request for the UE's TMSI, transmitted in plaintext without encryption or integrity protection. The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA completes and a NAS security context is active, all subsequent NAS messages—except for specific unprotected exceptions like initial registration—must be confidentiality and integrity protected to prevent eavesdropping and spoofing. The Identity Request, which solicits sensitive subscriber identity information, is not among the allowed exceptions and must be secured. The UE correctly ignored the unprotected Identity Request, as processing it would violate security protocols and expose it to potential attacks like identity tracking or impersonation. This non-response aligns with 5G security requirements, demonstrating the UE's adherence to mandated protections. Secure

219	219	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.5992319583892822 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5994939804077148 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a security context for encrypted and integrity-protected NAS communication. The UE then initiated a PDU session setup by sending a UL NAS Transport message. The AMF responded with an Identity Request message, explicitly requesting the UE's TMSI, but transmitted this message in plaintext without encryption or integrity protection. Crucially, the UE provided no response to this request. According to 3GPP standards (TS 33.501), after 5G-AKA completion, all subsequent NAS messages must be protected using the negotiated security context to prevent eavesdropping, tampering, or identity compromise. The UE's failure to respond aligns with security requirements, as it should discard or ignore any unprotected NAS messages received post-authentication to avoid processing potentially malicious or intercepted commands. This behavior demonstrates adherence to the standard's mandate for mandatory NAS protection after security context establishment. Secure
220	220	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.6309528350830078 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.63124680519104 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport message containing a PDU session establishment request, following the completion of 5G-AKA authentication. Subsequently, the AMF responded with a Downlink NAS Transport message containing an Identity Request for the UE's TMSI, explicitly noted as being sent in plaintext (unencrypted). The UE provided no response to this request. According to 3GPP standards (TS 33.501), once 5G-AKA is completed, a secure NAS signaling connection must be established, mandating that all subsequent NAS messages—including Identity Requests—be encrypted and integrity-protected using the negotiated keys. The UE's lack of response to an unprotected Identity Request aligns with 3GPP security requirements, as processing such a message after security activation would violate confidentiality and integrity protocols. By ignoring the plaintext request, the UE prevented potential exploitation of unprotected identity disclosure and maintained protocol compliance. Insecure

221	221	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 8.961992025375366 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.962584972381592 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Service Request to the AMF, which is standard behavior as this initial message often triggers security activation. Following a completed 5G-AKA (which establishes keys for confidentiality and integrity), the AMF responded with a Service Accept message sent in plaintext without encryption or integrity protection. Critically, the UE accepted this unprotected Service Accept and provided no response, indicating it processed the message despite the pre-existing security context. According to 3GPP standards (TS 33.501), once 5G-AKA succeeds, all subsequent NAS messages—including Service Accept—must be integrity-protected and encrypted to prevent tampering or spoofing. The UE's failure to reject this plaintext message violates core 5G security principles, as it exposes the connection to attacks like forgery or downgrade attempts. Insecure
222	222	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 8.977952003479004 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.978222846984863 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an InitialUEMessage containing a Service Request (mo-Data cause) to the AMF, which was unencrypted as expected for initial access. After 5G-AKA completion—which establishes mutual authentication and security context—the AMF responded with a Service Accept message. Critically, this downlink NAS message was transmitted in plaintext without encryption or integrity protection, as explicitly noted in the test summary and corroborated by the packet capture. The UE exhibited no response to this message. According to 3GPP standards (TS 33.501), once 5G-AKA completes, *all* subsequent NAS messages (including Service Accept) must be confidentiality-protected (encrypted) and integrity-protected to mitigate eavesdropping, tampering, and replay attacks. The UE is required to reject any post-authentication NAS message lacking these protections. Here, the UE’s silent acceptance of an unencrypted Service Accept—a message that typically carries sensitive parameters like network slicing details or security updates—violates this mandate. This failure to enforce encryption indicates a critical security lapse, leaving the communication vulnerable to interception or manipulation. Insecure

223	223	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 1.0053770542144775 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0059680938720703 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating a Service Request (uplink) to resume services, following a completed 5G-AKA procedure that established mutual authentication and security contexts. The AMF responded with an unprotected Service Reject (downlink) containing 5GMM Cause #9 ("UE identity cannot be derived by the network"), indicating the AMF could not associate the request with a valid security context. Critically, the UE took no further action upon receiving this plaintext reject. According to 3GPP standards (TS 24.501 and TS 33.501), after successful 5G-AKA, all subsequent NAS messages—including Service Reject—must be integrity-protected and encrypted using the established keys, except for specific unprotected messages explicitly allowed (e.g., Authentication Request/Response during initial AKA). Cause #9 does not justify bypassing security, as the UE had already authenticated; accepting an unprotected reject in this state violates mandatory security requirements. The UE should have detected the lack of protection, discarded the message, and potentially initiated recovery (e.g., re-registration), but its silence constitutes a failure to enforce security policies. Insecure
224	224	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 0.9605340957641602 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.9612541198730469 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began after successful 5G-AKA authentication, where the UE initiated communication by sending a Service Request. The AMF responded with an unprotected Service Reject message containing 5GMM cause #9 ("UE identity cannot be derived by the network"), transmitted in plain text without encryption or integrity protection. According to 3GPP standards (TS 24.501), cause #9 specifically permits the AMF to send this rejection unprotected when identity derivation fails, as security contexts cannot be applied without validated UE identification. However, upon receiving cause #9, the UE is required to invalidate its current 5G-GUTI and initiate a registration procedure to re-establish its identity and security context. The UE's failure to respond—providing no subsequent action—violates this mandatory procedure, leaving it in an unregistered state without attempting to resolve the identity issue. This non-compliance exposes the UE to persistent service denial and fails to trigger necessary security re-establishment, constituting insecure behavior under 3GPP protocols. Insecure

225	225	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.7581770420074463 UE to AMF UplinkNASTransport, Service request 0.7587769031524658 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request message to the AMF after successfully completing the 5G-AKA authentication, establishing a security context. The AMF responded with an unprotected Service Reject message (sent in plain text) containing 5GMM Cause #111 ("Protocol error, unspecified"), to which the UE provided no further response. According to 3GPP TS 24.501 (Section 5.5.1.2.4), upon receiving an unprotected Service Reject with a cause value other than #31 or #95 (explicit exceptions), the UE must transition to the 5GMM-DEREGISTERED state and initiate re-registration to re-establish a secure connection. The UE's failure to respond—indicating it neither re-registered nor attempted to recover the session—violates this requirement. This inaction leaves the UE in an undefined state, susceptible to denial-of-service (DoS) attacks or session desynchronization, as it ignores mandated security recovery procedures. Consequently, the UE's behavior deviates from 5G security standards and constitutes an insecure response. Insecure
226	226	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 21 UE provided: No response The packet capture during the test using wireshark is: 0.7632501125335693 UE to AMF UplinkNASTransport, Service request 0.7634460926055908 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Service reject (Synch failure) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request message to the AMF after successful 5G-AKA authentication, which establishes a security context requiring subsequent NAS messages to be integrity-protected and encrypted. The AMF responded with an unprotected (plain) Service Reject containing 5GMM Cause #21 ("Synch failure"), violating 3GPP TS 24.501 and TS 33.501 mandates that post-authentication NAS messages must be secured. The UE correctly ignored this unprotected rejection, as 3GPP standards require UEs to discard any NAS messages lacking integrity protection once a security context is active. This prevents processing potentially tampered or malicious injections. By not responding, the UE adhered to security protocols, demonstrating robust implementation against unprotected downlink messages. Secure

227	227	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03d2 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.5453281402587891 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5457210540771484 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5461199283599854 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing mutual authentication and session keys. The UE then sent an unprotected UL NAS TRANSPORT message. Subsequently, the AMF sent a Security Mode Command (SMC) to activate NAS security, which was integrity-protected using algorithm 128-5G-IA2 (AES-CMAC) and specified ciphering algorithm 5G-EA6 (128-bit SNOW 3G), along with the ABBA parameter. The UE did not respond to the SMC—neither with a Security Mode Complete nor a Security Mode Reject message. According to 3GPP standards (TS 24.501, section 5.4.2), upon receiving an SMC, the UE must always respond: if the integrity verification passes and the algorithms are supported, it sends Security Mode Complete; if the integrity passes but the algorithms are unsupported or parameters are invalid, it sends Security Mode Reject (e.g., with cause #26 for unsupported algorithms). The absence of a response indicates the UE failed to adhere to this protocol. Even if the UE encountered issues like unsupported 5G-EA6 (a non-mandatory algorithm) or an integrity check failure, a rejection or silent discard (only permissible for integrity failures) would be expected, but no standard-compliant behavior explains the complete lack of reaction. This deviation leaves the security context unresolved, exposes the session to potential threats like bidding-down attacks, and violates 3GPP security procedures. Insecure

228	228	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00f2 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 2.722198963165283 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.7225029468536377 AMF to UE SACK (Ack=8, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.722743034362793 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Configuration Update Command and then a Security Mode Command (SMC). The SMC was marked as "Protected" but specified null algorithms for both ciphering (5G-EA0) and integrity (5G-IA0), meaning no actual encryption or integrity protection was applied. The UE provided no response to this SMC. According to 3GPP standards (TS 33.501), after 5G-AKA completes, the SMC must activate NAS security. The use of null algorithms is permitted only in specific non-secure deployments, but the UE is still required to respond with either Security Mode Complete (accepting the algorithms) or Security Mode Reject (if they violate its security policy). The UE's failure to respond violates protocol requirements, leaves the security context ambiguous, and fails to establish subsequent protected communication. This non-compliance exposes the session to potential bidding-down attacks or manipulation, as the UE did not validate or challenge the insecure algorithm choice. Insecure
229	229	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.8296740055084229 UE to AMF UplinkNASTransport, Service request 0.8299529552459717 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating a Service Request after completing 5G-AKA, establishing a NAS security context. The AMF responded with a Configuration Update Command sent as a plain NAS message (security header type 0), lacking both integrity protection and encryption. The UE did not process or respond to this command. According to 3GPP standards (TS 33.501 and TS 24.501), once NAS security is activated, all subsequent NAS messages—including Configuration Update Command—must be integrity-protected to prevent tampering and ensure authenticity. The UE correctly identified the unprotected message as invalid per protocol requirements and discarded it, avoiding potential exploitation (e.g., malicious configuration changes). This adherence to discarding non-compliant messages aligns with security specifications, demonstrating robust threat mitigation. Secure

230	230	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.6443009376525879 UE to AMF UplinkNASTransport, Registration complete 0.644589900970459 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command, Unknown code (0x31) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message in plaintext, as expected at that stage. The AMF then responded with a Security Mode Command (SMC) message, which was also sent in plaintext (security header 0), specifying ciphering algorithm 5G-EA4 and integrity algorithm 5G-IA5. Critically, the UE provided no response to this SMC. According to 3GPP standards (TS 33.501), after 5G-AKA completion, the AMF must integrity-protect the SMC to prevent tampering or downgrade attacks. The SMC here lacked both integrity protection and encryption, violating the requirement that security activation commands be sent with integrity protection once authentication is complete. The UE's failure to reject this unprotected SMC—either by ignoring it or responding with a Security Mode Reject (cause #98 or similar)—constitutes a security lapse. Proper UE behavior would enforce mandatory integrity protection for SMC processing, but its inaction here accepted an unprotected critical command, exposing subsequent communications to potential manipulation. Insecure

231	231	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3100 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.4284870624542236 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4289300441741943 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4293291568756104 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an uplink NAS transport message (Registration Complete + PDU Session Establishment Request) after completing 5G-AKA authentication. The AMF then responded with a Configuration Update Command and a Security Mode Command (SMC). Critically, the SMC—which carried security algorithm negotiations (5G-EA6 for ciphering, 5G-IA5 for integrity) and ABBA parameters—was transmitted **unprotected** (plain NAS message with security header type 0), despite 5G-AKA having established a security context. The UE provided no response to this SMC. This UE behavior is **insecure** per 3GPP standards (TS 33.501, Sec. 6.9). The SMC is a security-critical establishment message always be integrity-protected to prevent tampering, as it activates NAS security algorithms. An unprotected SMC is inherently suspicious and could be a downgrade attack or forgery. The standard mandates that UEs **must** reject any unprotected SMC after 5G-AKA completes (TS 24.501, Sec. 4.4.6), requiring either a Security Mode Reject or local abortion of the connection. The UE's silence—implying tacit acceptance—fails to enforce this security control, leaving the system vulnerable to man-in-the-middle attacks where an adversary could manipulate security negotiations. Insecure
232	232	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.7425761222839355 UE to AMF UplinkNASTransport, Service request 0.7428131103515625 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request after completing the 5G-AKA procedure, which establishes a security context requiring subsequent NAS messages to be encrypted and integrity-protected. The AMF responded with an Authentication Reject message sent in plaintext, violating 3GPP TS 33.501, which mandates protected NAS communication post-authentication. The UE exhibited secure behavior by providing no response to this unprotected message. Per 3GPP TS 24.501, a UE must discard any unprotected NAS messages received after security context establishment (except specific exceptions like SERVICE REJECT with cause #3 or #6, which do not apply here). By ignoring the non-compliant Authentication Reject and avoiding further action, the UE correctly prioritized security protocol adherence over processing an invalid command, thereby mitigating potential exploitation from this deviation. Secure

233	233	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.7530779838562012 UE to AMF UplinkNASTransport, Service request 0.7533168792724609 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request message to the AMF after completing the 5G-AKA authentication procedure, which should have established a security context for encrypted and integrity-protected NAS communication. The AMF responded with an Authentication Reject message sent in plaintext (unencrypted and without integrity protection). The UE did not generate any response to this message. According to 3GPP standards (TS 24.501), after successful 5G-AKA, all subsequent NAS messages—including AMF responses—must be protected using the established security context, except for explicitly enumerated exceptions. The Authentication Reject message is not among these exceptions when a security context exists, as it was here (post-5G-AKA). The UE's acceptance of an unprotected Authentication Reject violates the standard's security requirements, as it risks exposing the UE to forgery attacks (e.g., malicious network nodes injecting unverified reject commands). Additionally, the UE's lack of response fails to demonstrate corrective actions like invalidating the compromised security context, further deviating from expected security protocols. Insecure
234	234	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.1599588394165039 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.160261869430542 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, indicating an ongoing 5G-AKA procedure. Before 5G-AKA completion (which establishes security keys), the AMF sent a subsequent Identity Request in plaintext, demanding the UE's TMSI. The UE provided no response to this request. According to 3GPP standards (TS 24.501, section 5.4.5), after transmitting the Authentication Response, the UE enters a state awaiting a Security Mode Command (SMC) to activate NAS security. Any non-security-related NAS messages (like Identity Request) received before SMC must be ignored by the UE if they are not integrity-protected. Here, the Identity Request was unprotected, and the requested identity (TMSI) is not the SUCI—which is the only identity type permitted to be requested unprotected in specific initial registration scenarios, not applicable post-Authentication Response. By ignoring this unprotected request, the UE adhered to standard security protocols, preventing potential exploits like bidding-down attacks or identity capture via rogue requests. Thus, the UE's non-response constitutes secure behavior. Secure

235	235	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.11994314193725586 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12015604972839355 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, a step in the 5G-AKA procedure that establishes mutual authentication and security keys. Before 5G-AKA completion, the AMF sent a plain-text (unencrypted) Identity Request demanding the UE's IMEISV—a sensitive, permanent equipment identifier. The UE provided no response to this request. According to 3GPP standards (TS 33.501), UEs must not disclose permanent identifiers like IMEISV unless the request is integrity-protected and the network is authenticated, which requires successful 5G-AKA. Since 5G-AKA was incomplete, the UE lacked proof of the AMF's authenticity and could not verify the request's legitimacy. By withholding the IMEISV, the UE adhered to security protocols that prevent tracking and spoofing attacks from rogue networks. This non-compliance with an unprotected identity request aligns with 3GPP-mandated protections for subscriber privacy and security. Secure
236	236	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0173 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.15990495681762695 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1602330207824707 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3627040386199951 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response after completing 5G-AKA, to which the AMF replied with an unprotected Security Mode Command specifying the ciphering (5G-EA4) and integrity (128-5G-IA2) algorithms. Instead of responding with a Security Mode Complete or Reject message to finalize the security context activation, the UE immediately transmitted a Deregistration Request. This deviation violates the 3GPP 5G security protocol (TS 33.501), which mandates that the UE must complete the Security Mode Command procedure before sending any subsequent NAS messages. By skipping the Security Mode Complete step, the UE sent the Deregistration Request without the required integrity protection or encryption, leaving it vulnerable to tampering or interception. This action demonstrates non-compliance with the standard, as NAS messages after Security Mode Command must be protected once the security context is established. Insecure

237	237	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.12820696830749512 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12850189208984375 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to complete the 5G-AKA procedure, confirming mutual authentication. The AMF then responded with a Security Mode Command (SMC), which was marked as "Protected" and included the ABBA parameter (0000), ciphering algorithm (5G-EA5), and null integrity algorithm (5G-IA0). However, the UE failed to respond with a Security Mode Complete or Security Mode Reject message, as required by the 3GPP 5G standard (TS 24.501, Section 5.4.1). This lack of response violates the protocol, which mandates that the UE must explicitly accept or reject the security parameters to establish a secure NAS context. The use of null integrity (5G-IA0) leaves messages vulnerable to tampering, and the UE's failure to acknowledge or challenge this configuration—especially given the non-standard "Unknown" security header—demonstrates non-compliance. Consequently, the UE did not activate ciphering or validate the SMC, leaving the session unprotected against eavesdropping or manipulation post-authentication. Insecure
238	238	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03967404365539551 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.03995108604431152 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response via Uplink NAS Transport, followed by the AMF issuing an Identity Request for the TMSI in a Downlink NAS Transport message sent in plaintext. Since 5G-AKA had not been completed, no security context existed, making plaintext transmission standard-compliant at this stage. However, the UE failed to respond to the Identity Request. According to 3GPP standards (TS 33.501), UEs must respond to Identity Requests even before security establishment, as plaintext exchanges are expected during initial authentication procedures. The lack of a response—whether due to ignoring the request, implementation errors, or misconfiguration—deviates from protocol requirements. This non-compliance could disrupt registration, enable denial-of-service attacks by stalling the authentication flow, or indicate improper handling of network commands, undermining the reliability and security expectations of 5G NAS signaling. Insecure

239	239	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.04004096984863281 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024195671081543 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF, followed by the AMF sending a plaintext Identity Request for the UE's IMEISV. Since 5G-AKA authentication had not been completed at this stage, no security context (including encryption) was established for NAS messages. The UE correctly provided no response to the request for IMEISV. According to 3GPP standards (TS 33.501), sensitive identities like IMEISV must not be transmitted unprotected. Specifically, Section 6.12.3 mandates that equipment identifiers should only be sent after security activation to prevent eavesdropping or tracking. The UE's refusal to disclose IMEISV in plaintext aligns with this requirement, demonstrating adherence to security protocols by prioritizing confidentiality until authentication completes and encryption is enabled. Secure
240	240	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0363 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.12767410278320312 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1279001235961914 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF after successful 5G-AKA authentication. The AMF then responded with a Security Mode Command, which was transmitted as a plain NAS message (security header 0), specifying ciphering algorithm 128-5G-EA3, integrity algorithm 128-5G-IA1, and ABBA parameter 0363. Crucially, the UE provided no response to this command. According to 3GPP standards (TS 33.501), after 5G-AKA completion, the Security Mode Command must be integrity-protected to prevent tampering with security parameters. Since the AMF sent this critical message unprotected, the UE's lack of response aligns with security requirements: it discarded the unverified command rather than processing it, thereby avoiding potential exploitation (e.g., algorithm downgrade attacks). This behavior demonstrates adherence to 5G security protocols. Secure

241	241	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.16009092330932617 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1604149341583252 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an uplink message containing Security Mode Complete and a Registration Request, followed by the AMF sending a downlink Security Mode Command. According to 5G standards (3GPP TS 33.501), after 5G-AKA completion, the AMF must initiate NAS security activation by sending a Security Mode Command (integrity-protected but not ciphered) before the UE responds with Security Mode Complete. Here, the UE sent Security Mode Complete *before* receiving the AMF's Security Mode Command, reversing the mandated sequence. Furthermore, the UE provided no response (e.g., Security Mode Reject or reattempt) to the AMF's subsequent Security Mode Command, which was protected with integrity (IA2) and null ciphering (EA7). This indicates the UE accepted an out-of-order security handshake and ignored a valid security command, violating the protocol's state machine and failing to enforce proper security negotiation. Such behavior could allow bypassing of security controls or processing of unauthorized commands, creating vulnerabilities. Insecure

242	242	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03f3 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.11997199058532715 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12023186683654785 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, confirming the completion of 5G-AKA authentication. The AMF then responded with a Security Mode Command (SMC), which was protected using the integrity algorithm 128-5G-IA2 and specifying the cipher algorithm 128-5G-EA1 for future communications. According to 3GPP standards (TS 33.501), the SMC must be integrity-protected but not encrypted, as the security context is not yet fully established. The UE's lack of response to the SMC—neither a Security Mode Complete nor a Security Mode Reject—aligns with standard behavior when integrity verification fails. Since the test was controlled (with the AMF potentially sending a malformed or invalidly protected SMC), the UE's silence indicates it discarded the message due to an integrity check failure, preventing activation of an insecure security context. This adheres to 5G security protocols, which mandate discarding unverifiable SMC messages to avoid processing under compromised conditions. Secure

243	243	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0293 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.15967893600463867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15994000434875488 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response after completing 5G-AKA, establishing mutual authentication and deriving session keys. The AMF then responded with a Security Mode Command (SMC) instructing the UE to activate ciphering (128-5G-EA1) and integrity protection (128-5G-IA1) for subsequent NAS messages. Critically, this SMC was sent as a plain/unprotected NAS message (security header type 0), lacking both integrity protection and encryption. According to 3GPP TS 33.501 (5G security architecture), the SMC must always be integrity-protected to prevent tampering, as it confirms cryptographic algorithms and activates security. Sending it unprotected exposes the system to downgrade attacks or malicious parameter alterations. The UE correctly recognized this violation by providing no response, adhering to the standard's requirement to reject unverified security commands. While the UE's inaction was proper, the overall exchange was compromised by the AMF's insecure transmission of the SMC. Insecure

244	244	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0033 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.16002106666564941 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602630615234375 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message, followed by the AMF transmitting a Security Mode Command in plaintext (without integrity protection or encryption). This sequence is inverted from the standard 5G procedure, where the AMF must send the Security Mode Command first to activate security, and the UE responds with Security Mode Complete. Critically, the Security Mode Command—which configures security algorithms—was sent without integrity protection (Security Header: Plain, Cipher Algorithm: null, Integrity Algorithm: IA2 but not applied). According to 3GPP TS 33.501, the Security Mode Command must always be integrity-protected to prevent tampering, as it establishes the security context. The UE's failure to reject this unprotected command (by not responding) violates the standard, which mandates that UEs must discard unverified Security Mode Commands and may initiate recovery procedures. By accepting an unprotected critical security message without reaction, the UE exposed itself to potential downgrade or manipulation attacks. Insecure
245	245	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15975403785705566 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16004419326782227 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, as part of the ongoing NAS communication where 5G-AKA authentication had not yet been completed. Subsequently, the AMF sent an Identity Request (for IMEISV) to the UE in plaintext, as no security context had been established. The UE did not respond to this request. According to 3GPP standards (TS 33.501), UEs must not disclose sensitive identifiers like IMEISV in unprotected NAS messages prior to successful 5G-AKA completion, which establishes encryption and integrity protection. This requirement prevents tracking and spoofing attacks by untrusted networks. The UE's refusal to provide the IMEISV without a security context aligns with these security provisions, as it avoided exposing critical equipment identity in plaintext. Secure

246	246	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.11967587471008301 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11993288993835449 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, as part of the ongoing 5G-AKA procedure. Since 5G-AKA was not yet completed, no security context (encryption/integrity protection) was established. Subsequently, the AMF sent a plaintext Identity Request for the TMSI, which is permissible under 3GPP standards (TS 33.501) at this pre-security stage, as sensitive data like permanent identifiers are not involved. However, the UE did not respond to this request. This lack of response is likely a deliberate security measure by the UE. After initiating authentication, the UE expects the next critical step to be Security Mode Command (SMC) activation. An unexpected Identity Request at this juncture—especially when the UE had already provided initial identity information (e.g., in Registration Request)—could be interpreted as anomalous or potentially malicious. By ignoring the request, the UE avoids exposing even non-sensitive data (TMSI) unnecessarily and adheres to a strict state machine, mitigating risks like bidding-down attacks or session hijacking. This aligns with 3GPP security principles (TS 24.501) that prioritize caution when messages deviate from the expected sequence before security activation. Secure
247	247	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.1999650001525879 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.20019102096557617 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, as part of the ongoing 5G-AKA procedure. Before 5G-AKA could be completed (which establishes a security context for encrypted/integrity-protected NAS messaging), the AMF sent a plain-text Identity Request demanding the UE's IMEISV—a sensitive device identifier. Crucially, the UE provided no response to this request. According to 3GPP standards (TS 33.501, TS 24.501), NAS messages carrying sensitive user/device identities (like IMEISV) must only be transmitted after successful authentication and security activation (i.e., post-5G-AKA and Security Mode Command). Since 5G-AKA was incomplete and the Identity Request was sent unprotected, the UE's refusal to disclose IMEISV aligns with security requirements: it prevented potential eavesdropping or tracking of the device identifier in an insecure state. The UE correctly prioritized confidentiality by awaiting a secured context before responding to sensitive requests. Secure

248	248	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA3 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.11875295639038086 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11905193328857422 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Authentication Response after completing 5G-AKA. The AMF then responded with a Security Mode Command (SMC), which was explicitly marked as "Protected" and included specific security algorithms (128-5G-EA2 for ciphering and 128-5G-IA3 for integrity) along with the ABBA parameter. According to 3GPP standards (TS 33.501), after receiving a protected SMC, the UE must validate the message's integrity using the keys derived during 5G-AKA. If valid, the UE must activate the negotiated security context and respond with a Security Mode Complete message (protected using the new context) to confirm security activation. If the SMC is invalid or unsupported, the UE must send a Security Mode Reject. In this test, the UE provided no response—neither an acknowledgment nor a rejection—despite the AMF's protected SMC. This lack of response violates the 5G security protocol, as it leaves the security context unconfirmed and fails to establish encrypted/integrity-protected communication. The UE's inaction prevents the completion of the security mode procedure, exposing subsequent communications to potential manipulation or eavesdropping. Insecure
249	249	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.7274200916290283 UE to AMF UplinkNASTransport, Service request 0.7277319431304932 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a security context. The UE then sent a Service Request (uplink), after which the AMF responded with a Configuration Update Command (downlink) as a plain NAS message (security header type 0), lacking both encryption and integrity protection. The UE provided no response to this message. According to 3GPP standards (TS 33.501), after 5G-AKA completion, all subsequent NAS messages—except specific initial procedures like authentication or security mode commands—must be integrity-protected and encrypted to prevent tampering and eavesdropping. The Configuration Update Command is not an exempted message and therefore requires full security. The UE's failure to reject the unsecured command—either by ignoring it, initiating recovery procedures, or triggering a security failure—violates these requirements, as it accepts unprotected sensitive network updates. This omission exposes the UE to potential man-in-the-middle attacks or unauthorized configuration changes. Insecure

250	250	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999590873718262 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040209054946899414 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF, followed by the AMF transmitting a plain-text Identity Request for the UE's IMEISV. Since 5G-AKA authentication had not been completed, no security context (including encryption or integrity protection) was established between the UE and AMF at this stage. According to 3GPP standards (TS 33.501), UEs must not transmit sensitive identifiers like IMEISV without encryption, as they are vulnerable to interception and tracking. The UE correctly recognized the absence of a security context and the plain-text nature of the request, leading it to withhold the IMEISV by providing no response. This aligns with 3GPP security requirements, which mandate that sensitive identity transfers occur only after successful 5G-AKA and within protected NAS messages. Secure
251	251	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03961300849914551 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039839982986450195 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF. Subsequently, the AMF sent an Identity Request in plain text (due to incomplete 5G-AKA), specifically requesting the TMSI identity. The UE did not respond to this request. According to 3GPP standards (TS 24.501 and TS 33.501), Identity Requests must be handled by the UE regardless of security context establishment, except when the requested identity is IMSI without integrity protection—which does not apply here, as TMSI was requested. TMSI, being a temporary identifier, does not require integrity protection for the request, and the UE is obligated to respond. The UE's failure to reply violates protocol requirements, potentially indicating flawed implementation or unexpected behavior that could disrupt network procedures or expose vulnerabilities to denial-of-service attacks. Consequently, the UE's action is non-compliant and insecure. Insecure

252	252	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03987598419189453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040084123611450195 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF, followed by the AMF sending a plain-text Identity Request (without encryption, as 5G-AKA was incomplete) asking for the UE's IMEISV. The UE did not respond to this request. According to 3GPP standards (TS 33.501), permanent identifiers like IMEISV must only be transmitted after a security context is established via 5G-AKA, ensuring confidentiality and integrity via encrypted NAS messaging. Since 5G-AKA had not been completed, the UE correctly refrained from disclosing the sensitive IMEISV in plain text, adhering to security protocols that prevent exposure of critical identifiers to potential eavesdropping or manipulation. By withholding the response, the UE avoided a vulnerability that could have been exploited in an insecure channel. Secure
253	253	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.7599589824676514 UE to AMF UplinkNASTransport, Service request 0.7601721286773682 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request uplink message to the AMF after completing 5G-AKA authentication, which should establish security keys for encrypted and integrity-protected NAS communication. The AMF responded with a DownlinkNASTransport containing an Identity Request for the GUTI, explicitly noted as sent "Plain" (unencrypted and without integrity protection). The UE provided no response to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA is completed, all subsequent NAS messages—except specific initial unauthenticated procedures—must be confidentiality and integrity protected to mitigate eavesdropping, tampering, and replay attacks. The Identity Request falls under this mandatory protection requirement post-authentication. The UE's failure to respond aligns with 3GPP security protocols, which dictate that a UE must discard unprotected NAS messages received after security context establishment to prevent processing potentially malicious or forged commands. By ignoring the plaintext Identity Request, the UE adhered to security requirements, avoiding exposure of sensitive identity information (e.g., GUTI) and maintaining protocol compliance. Secure

254	254	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 6.647611856460571 UE to AMF SACK (Ack=7, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 6.6478259563446045 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After successfully completing the 5G-AKA mutual authentication, the UE initiated a PDU session establishment by sending an Uplink NAS Transport message. The AMF responded with a Service Accept message, which was transmitted in plaintext without encryption or integrity protection. According to 3GPP standards (TS 33.501), once 5G-AKA establishes a security context, **all subsequent NAS messages**—including Service Accept—**must be confidentiality and integrity protected** to prevent eavesdropping and tampering. The UE's lack of response to this unprotected message indicates it failed to enforce these security requirements. A compliant UE should have rejected the plaintext Service Accept, triggered a security error (e.g., NAS integrity failure), or initiated recovery procedures to maintain session security. By silently accepting the message, the UE exposed itself to potential man-in-the-middle attacks or injected malicious commands. Insecure
255	255	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 12.160748958587646 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 12.161019086837769 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request via an InitialUEMessage after completing 5G-AKA authentication. The AMF responded with a DownlinkNASTransport containing an Identity Request for the UE's IMEI, sent in plaintext without encryption or integrity protection. The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA is completed, a secure NAS context is established, and all subsequent NAS messages must be integrity-protected and encrypted to prevent eavesdropping or spoofing. The Identity Request here occurred post-authentication and therefore required protection. The UE's lack of response aligns with 3GPP-mandated behavior, as accepting an unprotected NAS message after security context establishment would violate security protocols. This non-response indicates the UE correctly identified the unprotected message as invalid, discarding it to maintain security. Secure

256	256	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 97 UE provided: No response The packet capture during the test using wireshark is: 0.46838808059692383 UE to AMF UplinkNASTransport, Registration complete 0.4686100482940674 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Message type non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message after completing 5G-AKA, which establishes a security context for encrypted and integrity-protected NAS communication. The AMF then responded with an unprotected GMM Status message (sent in plain) containing cause value #97 ("Message type non-existent or not implemented"). The UE provided no response to this message. According to 3GPP standards (TS 24.501), after 5G-AKA succeeds, all subsequent NAS messages must be protected unless explicitly exempted. The GMM Status message with cause #97 is one such exemption (Section 4.4.4.2), allowing it to be sent unprotected under specific error conditions. Crucially, the standard mandates that the UE must ignore and not respond to an unprotected GMM Status message with cause #97 (Section 5.4.1.2) to prevent potential security exploits, such as bidding-down attacks or resource exhaustion through malformed messages. By remaining silent, the UE adhered to this requirement, avoiding any unintended processing of the unprotected message and maintaining protocol compliance. Thus, its inaction was a secure implementation of the standard. Secure
257	257	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4328169822692871 UE to AMF UplinkNASTransport, Registration complete 0.4330179691314697 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication and sending a Registration Complete message to the AMF, which should have been encrypted and integrity-protected per the established security context. Subsequently, the AMF transmitted an Identity Request for SUCI in plaintext (unencrypted), as confirmed by the packet capture. The UE did not respond to this request. According to 3GPP standards (TS 33.501), once 5G-AKA completes and a secure context is established, all subsequent NAS messages—including Identity Request—must be confidentiality and integrity protected to prevent eavesdropping, tampering, or identity harvesting. The UE's lack of response aligns with security requirements, as it correctly rejected an unprotected message post-authentication, avoiding potential SUPI/SUCI exposure or man-in-the-middle attacks. Secure

258	258	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Plain Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.4842751026153564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4844861030578613 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport 2.688286066055298 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message, indicating successful completion of the 5G-AKA authentication, which establishes a secure NAS context. The AMF then sent a Deregistration Request downlink message in plaintext (unprotected), violating 3GPP TS 33.501 mandates that require NAS messages to be integrity-protected and ciphered after security context establishment. Instead of processing the unprotected request, the UE discarded it (as required by standards) and independently initiated a new UE-originating Deregistration Request, which was sent as an integrity-protected and ciphered uplink message (Security Header Type 2). This behavior aligns with 3GPP TS 24.501, where UEs must reject unprotected NAS messages after security activation and may locally trigger deregistration as a safeguard. The UE correctly prioritized security by ignoring the invalid downlink and protecting its own response. Secure
259	259	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 99 UE provided: No response The packet capture during the test using wireshark is: 0.5207638740539551 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.521324872970581 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Information element non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After the successful completion of 5G-AKA mutual authentication, which established a secure NAS context, the UE initiated a PDU session setup by sending an encrypted UL NAS TRANSPORT message. The AMF responded with an unprotected GMM STATUS message (cause 99 – "semantically incorrect message") in plaintext, violating 3GPP TS 24.501 § 4.4.5, which mandates that all NAS messages after security activation must be integrity-protected and encrypted. The UE exhibited insecure behavior by processing and responding to this unprotected message. Per 3GPP standards (§ 5.4.3.2), the UE must discard any NAS message without security protection after 5G-AKA completion and may initiate recovery procedures. The UE's failure to detect or react to this security violation indicates non-compliance, leaving it vulnerable to downgrade attacks or malicious message injection. Insecure

260	260	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 101 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5113871097564697 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.511634111404419 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, 5GMM status (Message not compatible with the protocol state) 0.7153670787811279 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE completing 5G-AKA authentication, establishing a secure context, and sending a Registration Complete message (encrypted, as required post-authentication). The AMF then responded with a plaintext GMM Status message containing cause #101 ("Message not compatible with the protocol state"), which is permissible under 3GPP TS 24.501 for specific error causes even after security activation. Subsequently, the UE initiated a Deregistration Request (UE originating). Critically, this Deregistration Request was sent as a protected NAS message, consistent with 3GPP security requirements that mandate encryption and integrity protection for all NAS messages (except explicitly allowed exceptions like certain status messages) once 5G-AKA completes. The UE correctly processed the allowable plaintext GMM Status without compromising the security context and responded with a properly secured message, demonstrating adherence to the standard. No evidence suggests the UE mishandled keys or sent sensitive data unprotected. Secure
261	261	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0101 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.7511579990386963 UE to AMF UplinkNASTransport, Service request 0.7514059543609619 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE initiating a Service Request after completing 5G-AKA authentication. The AMF responded with a Security Mode Command (SMC), which was marked as "Protected" and included specific algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity) along with ABBA parameter 0101. However, the UE failed to respond to the SMC. According to 3GPP standards (TS 33.501 and TS 24.501), after 5G-AKA completes, the SMC must be integrity-protected (but not encrypted) to activate NAS security. The UE is required to validate the SMC's integrity and respond with either a Security Mode Complete (if valid) or Reject (if invalid) message. The absence of any UE response—neither an acknowledgment nor an error—indicates non-compliance. This breaks the security activation flow, leaving subsequent communications unprotected and violating the protocol's mandatory handshake. The UE's inaction could enable attacks like bidding down or session hijacking, as the network cannot confirm security context synchronization. Insecure

262	262	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.914944887161255 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.915573835372925 AMF to UE SACK (Ack=13, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request in plain text via an InitialUEMessage, as NAS security had not yet been established. The AMF responded with a Security Mode Command (SMC) in plain text, specifying null ciphering (5G-EA0) and integrity protection (128-5G-IA2). Crucially, the SMC lacked integrity protection and encryption, despite the prior completion of 5G-AKA authentication, which established shared keys for security. According to 3GPP standards (TS 33.501, Section 8.2.2.1), the SMC must be integrity-protected to prevent tampering, as it activates security algorithms for subsequent NAS messages. The UE's failure to respond—such as rejecting the SMC with a Security Mode Reject message—indicates it did not enforce this requirement. This omission leaves the UE vulnerable to attacks, such as malicious algorithm downgrades or spoofed commands, as it accepted an unprotected SMC without challenge. Insecure
263	263	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 74 UE provided: No response The packet capture during the test using wireshark is: 0.5198588371276855 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5200669765472412 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Registration reject (Temporarily not authorized for this SNPN) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After successfully completing the 5G-AKA mutual authentication, which established a secure NAS context, the UE sent a UL NAS TRANSPORT message (containing a PDU session establishment request). The AMF responded with a REGISTRATION REJECT message (5GMM cause #74: "Temporarily not authorized for this SNPN") sent in plaintext without encryption or integrity protection. The UE exhibited no response to this unprotected message. According to 3GPP standards (TS 33.501, TS 24.501), once 5G-AKA completes and a secure context is established, **all subsequent NAS messages must be both integrity-protected and encrypted**. The UE is required to verify these protections and discard any non-conforming messages. By silently accepting an unprotected REGISTRATION REJECT after security context establishment, the UE failed to enforce mandatory security checks. This deviation allows potential threat actors to inject unauthenticated reject messages, undermining session integrity and violating 3GPP security requirements. The lack of reaction (e.g., ignoring the message or initiating recovery) further demonstrates non-compliance. Insecure

264	264	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 6 UE provided: No response The packet capture during the test using wireshark is: 2.427165985107422 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4275641441345215 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4278719425201416 AMF to UE DownlinkNASTransport, Registration reject (Illegal ME) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE sent an Uplink NAS Transport message containing a Registration Complete and PDU Session Establishment Request. The AMF responded with a Configuration Update Command (protected), followed by a Registration Reject message with 5GMM Cause #6 ("Illegal ME") sent in plaintext without encryption or integrity protection. The UE provided no response to the unprotected Registration Reject. According to 3GPP standards (TS 24.501 and TS 33.501), once 5G-AKA completes and a security context is established, all subsequent NAS messages must be confidentiality and integrity protected. The Registration Reject is a security-critical NAS command that explicitly requires protection. The UE correctly ignored this unprotected message, as processing it could expose vulnerabilities to spoofing or manipulation attacks. By discarding the message instead of reacting, the UE adhered to security protocols designed to prevent exploitation of unprotected NAS signaling post-authentication. Secure

265	265_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1111 RAND: 0e38a634245d3e4aea72a7f7a7148161 AUTN: 3d9033e57f3e8000d3eb278394dd7c46 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 1.0084679126739502 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0087080001831055 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Authentication request 1.216444969177246 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Service Request to initiate communication. The AMF responded with a plaintext Authentication Request containing a RAND, AUTN, and ngKSI value of 5 (indicating a native security context). The UE rejected this request with an "Authentication failure (ngKSI already in use)" message, signifying it already possessed an active native security context associated with ngKSI=5 and refused to overwrite it or process conflicting authentication. According to 3GPP TS 33.501, reusing an ngKSI for a native security context while an existing context is active is prohibited, as it could lead to security context desynchronization or bidding-down attacks. The UE's adherence to this protocol by explicitly rejecting the reused ngKSI—instead of silently accepting it or overwriting the context—demonstrates correct implementation of 5G security standards. This prevents potential exploitation where an attacker might force context confusion to compromise security algorithms or keys. Secure
266	266	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.5199589729309082 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.520190954208374 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA, which established a security context for encrypted and integrity-protected NAS communication as per 3GPP standards. Following this, the UE sent an UplinkNASTransport message containing a PDU session establishment request, which should have been protected under the active security context. However, the AMF responded with an Authentication Reject message sent in plaintext, without encryption or integrity protection. The UE exhibited no further response, aligning with standard behavior for handling this message type. According to 3GPP TS 24.501, the Authentication Reject is explicitly permitted to be sent unprotected even after security activation, as it is among a limited set of exceptions (e.g., messages related to authentication failures or security mode commands) that bypass protection requirements. The UE's acceptance of this plaintext message and subsequent lack of action complies with the standard, which mandates that such messages trigger context deletion without a response. While this design leaves a known vulnerability to forgery-based denial-of-service attacks, the UE's adherence to protocol specifications constitutes secure behavior within the defined framework. Secure

267	267	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.5199449062347412 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201799869537354 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a security context, and sending a UL NAS Transport (PDU session establishment request). The AMF responded with an unprotected Authentication Reject message, to which the UE provided no response. According to 3GPP standards (TS 33.501 and TS 24.501), after 5G-AKA completion, all NAS messages must be integrity-protected and encrypted to prevent tampering and eavesdropping, except for specific initial procedures like Authentication Request or Identity Request. The Authentication Reject message, while permitted without protection during initial authentication, should not be sent unprotected after security context establishment, as this violates post-authentication security requirements. By accepting an unprotected Authentication Reject after successful 5G-AKA, the UE processed a potentially malicious message that forces deregistration, exposing it to denial-of-service attacks. This behavior contradicts the standard's mandate for protected NAS communication post-authentication, indicating a security flaw in the UE's implementation. Insecure
268	268	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.7500498294830322 UE to AMF UplinkNASTransport, Registration complete 0.7504808902740479 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Registration Complete message after a successful 5G-AKA authentication, establishing a secure NAS context. The AMF then responded with a Configuration Update Command, which was marked as "Protected" but carried an "Unknown" security header value. The UE did not generate any response to this command. According to 3GPP standards (TS 24.501 and TS 33.501), after 5G-AKA completion, all NAS messages must be protected with recognizable security headers (e.g., integrity-protected or ciphered, using values 1–4). An "Unknown" security header indicates an invalid or reserved value (5–15), which the UE must discard without processing or responding, as it cannot verify the message's integrity or origin. The UE's silent discard aligns with security protocols to prevent processing malformed or potentially malicious messages. No further recovery action (e.g., re-registration) was observed, but the immediate non-response to the invalid header is compliant and secure. Secure

269	269	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.46799302101135254 UE to AMF UplinkNASTransport, Registration complete 0.4681861400604248 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE completing 5G-AKA, establishing a security context, and sending a Registration Complete message. The AMF then responded with a Deregistration Accept message sent in plaintext (unencrypted and without integrity protection). The UE exhibited no response to this message. According to 3GPP standards (TS 33.501), after successful 5G-AKA, all subsequent NAS messages—including Deregistration Accept—must be confidentiality-protected and integrity-protected to mitigate eavesdropping, tampering, and replay attacks. The UE's failure to reject or respond to an unprotected NAS message violates these requirements, as it should have detected the security compromise, discarded the message, initiated recovery procedures, or transitioned to a limited service state. This inaction indicates non-compliance with mandatory security protocols. Insecure
270	270	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999805450439453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024100303649902 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Identity Response to the AMF. Subsequently, the AMF sent an unprotected Identity Request for the IMEISV (PEI), to which the UE provided no response. Crucially, 5G-AKA—the authentication and key agreement procedure—had not been completed at this stage, meaning no security context (e.g., encryption or integrity protection) was established. According to 3GPP standards (TS 33.501, Section 6.12.3), UEs must not transmit the PEI (IMEISV) in plaintext NAS messages except during initial registration under specific conditions (e.g., no valid 5G-GUTI and in a non-allowed area). Here, the AMF's request occurred post-initial UE communication and without authentication, placing it outside these exceptions. By not responding, the UE correctly adhered to security protocols, avoiding exposure of sensitive identity data (IMEISV) to an unauthenticated network entity. This prevents potential tracking or spoofing attacks. Thus, the UE's action aligns with 3GPP security requirements. Secure

271	271	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.03961491584777832 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.03991198539733887 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response (uplink), followed by the AMF requesting the UE's IMEI via a plaintext Identity Request (downlink), as 5G-AKA authentication had not yet been completed. The UE did not respond to this request. According to 3GPP standards (TS 24.501 and TS 33.501), NAS messages exchanged before 5G-AKA completion lack encryption and integrity protection, making plaintext transmission expected for initial procedures. However, the standard mandates that the UE must respond to a valid Identity Request for the IMEI—a non-sensitive equipment identifier—to facilitate network functions like device authentication and registration. The UE's failure to respond constitutes non-compliance with protocol requirements, potentially disrupting service establishment without a justified security rationale (e.g., IMEI disclosure in pre-authentication phases is explicitly permitted). This deviation could indicate flawed implementation, unintentional misconfiguration, or an unnecessary obstruction of standard procedures, undermining protocol reliability. Insecure
272	272	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007159709930419922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2011561393737793 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The UE initiated communication by sending an unprotected Initial Registration Request, which is standard for establishing initial contact. The AMF responded with a Service Accept message marked as "Protected," despite the 5G-AKA authentication not being completed and no security context established. According to 3GPP standards (TS 33.501), NAS messages must only be marked as protected after successful 5G-AKA, which establishes keys for encryption and integrity protection. The UE should have rejected the Service Accept message because its "Protected" status was invalid without a security context, indicating a potential security threat (e.g., spoofed AMF). Instead, the UE accepted it and proceeded to send a Deregistration Request unprotected. This request, while permissible without security context, followed improper handling of the Service Accept. By processing an invalid protected message without discarding it or triggering security recovery, the UE violated 5G security protocols, creating a vulnerability to man-in-the-middle attacks or forged network commands. Insecure

273	273	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11984086036682129 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12007284164428711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Authentication Response during the ongoing 5G-AKA procedure, as the security context had not yet been established. Subsequently, the AMF sent a Deregistration Request message that was marked as "Integrity protected and ciphered" (security header type 2), despite 5G-AKA not being completed. According to 3GPP standards (TS 33.501), NAS message protection (integrity and ciphering) must only be applied **after** successful 5G-AKA authentication and key establishment, which includes the Security Mode Command (SMC) procedure. The UE, lacking valid keys to verify or decrypt the protected message, correctly discarded the Deregistration Request and provided no response. This aligns with standard requirements, as processing such a message without a security context would constitute a vulnerability. The UE's adherence to protocol by ignoring the message demonstrates secure behavior. Secure
274	274	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.11959981918334961 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1198418140411377 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Authentication Response to the AMF, as part of the ongoing 5G-AKA procedure. Before completing 5G-AKA (which requires mutual authentication and key derivation), the AMF sent a Deregistration Request that was integrity-protected but not encrypted. According to 3GPP standards (TS 33.501), NAS security context activation occurs only after successful 5G-AKA completion, which includes the Security Mode Command (SMC) exchange. At this pre-SMC stage, the UE lacks an established security context and should only accept specific unprotected NAS messages (e.g., Authentication Request, SMC). The Deregistration Request, being a protected management message unrelated to security setup, must not be processed without a valid security context. The UE's lack of response indicates it discarded the message, as it could not verify its integrity or legitimacy. This aligns with 3GPP security requirements, which mandate rejecting protected messages during initial authentication to prevent processing unverified commands from untrusted networks. Secure

275	275	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007669925689697266 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal ME) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as 5G-AKA authentication had not yet been completed and no security context existed. The AMF then responded with a Deregistration Request (UE-terminated) marked as "Integrity Protected and Ciphered" (security header type 2) with a deregistration cause of "Illegal ME." However, since 5G-AKA was incomplete, the UE lacked the necessary keys to decrypt or verify the integrity of this protected message. According to 3GPP standards (TS 33.501), NAS security (integrity protection and ciphering) requires successful 5G-AKA to establish shared keys. The UE, unable to process the message without valid security context, correctly ignored it and provided no response. This adherence to protocol—rejecting protected messages before authentication—prevented potential exploitation from unverified network commands. Secure
276	276	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3232 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 1.6001770496368408 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Identity response 1.6007089614868164 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response in plain text, as 5G-AKA authentication had not yet been completed. The AMF then responded with a Security Mode Command (SMC), also sent in plain text, specifying ciphering algorithm 5G-EA6 and integrity algorithm 128-5G-IA1. Critically, the SMC lacked integrity protection and was transmitted before any security context establishment. According to 3GPP standards (TS 33.501), the SMC must be the first integrity-protected message in NAS signaling to prevent manipulation (e.g., algorithm downgrade or ABBA tampering). Since 5G-AKA was incomplete, no security keys existed to validate the SMC's authenticity. The UE correctly ignored this unprotected command, as processing it would violate core security principles by accepting an unverified directive to activate security algorithms. This non-response aligns with 5G security requirements, as accepting an unsigned SMC would expose the UE to man-in-the-middle attacks. Secure

277	277	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.04006814956665039 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040535926818847656 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Identity Response, as 5G-AKA had not yet been completed. Subsequently, the AMF sent a Configuration Update Command, which was marked as integrity-protected (Security Header Type 1). Per 3GPP TS 33.501, NAS messages must only be integrity-protected and encrypted after successful 5G-AKA establishes a security context. Since 5G-AKA was incomplete, the UE lacked the necessary keys to verify the message's integrity or process it securely. The UE correctly discarded the unprotected message without responding or acting upon it, avoiding potential exploitation of unverified commands. This aligns with 3GPP security requirements, as processing a protected message without a valid security context would violate the standard. Secure
278	278	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.3110721111297607 UE to AMF UplinkNASTransport, Identity response 2.311551094055176 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Configuration update command 2.3115811347961426 UE to AMF SACK (Ack=3, Arwnd=106437) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF. Without completing 5G-AKA authentication or establishing a NAS security context, the AMF sent a Configuration Update Command as a plain (unprotected) NAS message. The UE did not respond to this command with a Configuration Update Complete as typically expected but instead initiated a Deregistration Request, also sent as a plain NAS message. According to 3GPP standards (TS 33.501), sensitive NAS messages like Configuration Update Command must be integrity-protected and encrypted once security is activated. Since 5G-AKA was incomplete and no security context existed, the UE should have rejected or ignored the unprotected command, as processing it risks exploitation by attackers (e.g., malicious reconfiguration or denial-of-service). By reacting to the plain command—triggering deregistration—the UE processed an insecure directive it should have discarded, violating standard security protocols. Insecure

279	279	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007669925689697266 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as expected before authentication. The AMF responded with a Deregistration Accept message marked as "Protected," despite 5G-AKA authentication not being completed. According to 3GPP standards (TS 33.501), NAS security must be activated via 5G-AKA before protected messages are exchanged, as the UE lacks valid keys to decrypt or validate such messages until authentication concludes. The UE's lack of response to the protected Deregistration Accept is appropriate because: (1) the UE could not process the message without an established security context, (2) accepting unverified deregistration commands would risk premature termination of service, and (3) the standard mandates ignoring protected messages received pre-authentication. This behavior prevents potential exploits from unauthenticated network instructions. Secure
280	280	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007870197296142578 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected initial registration request to the AMF, as expected without prior authentication. However, the AMF responded with a protected deregistration accept message before completing the 5G-AKA authentication procedure. According to 3GPP standards (TS 33.501), NAS security context—necessary for encrypting/integrity-protecting messages—is only established after successful 5G-AKA. Since 5G-AKA was "not completed yet," the UE lacked the keys to process protected messages. The UE's lack of response to the deregistration accept indicates it rejected the message, adhering to the standard by not acting on unverified protected traffic without a valid security context. This aligns with security requirements to prevent processing of unauthorized protected commands. Secure

281	281	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00080108642578125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an **unprotected Initial Registration Request** to the AMF, as 5G-AKA authentication had not yet been completed. The AMF responded with a **Configuration Update Command (CUC)**, which was marked as *protected* (security header type 4: integrity-protected and ciphered using a new security context). Critically, the UE **provided no response** to this downlink message. According to 3GPP standards (TS 33.501 and TS 24.501), a UE must not process protected NAS messages (like the CUC) without first establishing a valid security context via 5G-AKA. Since 5G-AKA was incomplete, the UE lacked the keys to verify the message's integrity or decrypt it. The UE should have either: 1. **Discarded the message** as invalid due to the absence of a matching security context. 2. **Initiated re-registration** to recover from the security failure. The UE's lack of action—**no response, no re-registration attempt**—indicates it may have accepted or ignored an unverifiable protected message. This violates 3GPP security requirements, as it could allow exploitation (e.g., malicious configuration updates) without triggering mandated recovery procedures. **Insecure**
282	282	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006248950958251953 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, which is standard before security establishment. The AMF responded with a Configuration Update Command (CUC) that was marked as "Integrity protected and ciphered" (security header type 2), despite 5G-AKA authentication not being completed. Since 5G-AKA is a prerequisite for deriving the security keys needed to validate or decrypt protected NAS messages, the UE lacked the context to process this message. Per 3GPP TS 24.501 and TS 33.501, a UE must discard protected NAS messages received before security context establishment and may optionally respond with an error only if it can integrity-protect the reply (which it cannot here). The UE's lack of response aligns with the standard, as processing or acknowledging an unverifiable protected message would pose security risks (e.g., accepting malicious reconfigurations). Thus, the UE correctly prioritized security by discarding the invalid message. Secure

283	283	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006029605865478516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as expected without prior 5G-AKA completion. The AMF responded with a **Service Accept** message marked as "Protected," implying encryption and integrity protection. Critically, the UE provided **no response** to this protected downlink message. According to 3GPP standards (TS 33.501), NAS security (including confidentiality and integrity protection) must be established *after* successful 5G-AKA authentication. Since 5G-AKA was explicitly "not completed yet," no valid security context existed for the UE to decrypt or verify the AMF's protected Service Accept. The UE's lack of response aligns with the standard: accepting or processing protected NAS messages without a negotiated security context would violate fundamental security principles, as it could expose the UE to maliciously crafted packets or man-in-the-middle attacks. By ignoring the improperly protected message, the UE correctly prioritized security protocol adherence over network responsiveness. Secure
284	284	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006928443908691406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2013227939605713 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request, as 5G-AKA had not yet been completed. The AMF responded with a Service Accept message marked as "Protected," despite the absence of an established security context. The UE then sent an unprotected Deregistration Request (UE originating) without challenging the AMF's "Protected" message. According to 3GPP standards (TS 33.501), NAS message protection requires successful 5G-AKA authentication to derive security keys. Since 5G-AKA was incomplete, the UE should have rejected the Service Accept message for lacking verifiable integrity protection and encryption, as it could be a forgery or manipulation attempt. By processing the message and proceeding with deregistration, the UE violated the 5G security protocol, leaving it vulnerable to man-in-the-middle attacks or unauthorized network impersonation. Insecure

285	285	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039772987365722656 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (PLMN not allowed) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Identity Response message to the AMF, which is expected at this stage since 5G-AKA had not yet been completed and no security context was established. The AMF then responded with a Deregistration Request message that was marked as "Integrity protected and ciphered" (security header type 2). However, given that 5G-AKA was incomplete, the UE lacked the necessary keys to decrypt or validate this message. Per 3GPP standards (TS 33.501), a UE must not process integrity-protected or ciphered NAS messages without an active security context, as they cannot be authenticated, posing risks such as accepting malicious network commands. The UE correctly ignored the Deregistration Request by providing no response, avoiding potential exploitation (e.g., forced deregistration by an attacker). This adherence to security protocols—rejecting unprotected processing of secured messages—aligns with 5G security requirements. Secure
286	286	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00036406517028808594 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as 5G-AKA had not yet been completed and no security context existed. The AMF responded with a DownlinkNASTransport message containing a 5GMM Status (Cause 98: "Message type not compatible with the protocol state"), which was marked as "Protected" despite the absence of an established security context. The UE did not respond to this message. According to 3GPP TS 24.501 and TS 33.501, a UE without a valid security context must discard any protected NAS messages, as it lacks the keys to decrypt or verify integrity. The UE's lack of response aligns with this requirement, as processing the message would violate security protocols. By discarding the message and not engaging further, the UE avoided potential vulnerabilities from unverified or malicious content, demonstrating adherence to 5G security standards. Secure

287	287	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 3 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.000408172607421875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Illegal UE) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as 5G-AKA had not yet been completed to establish a security context. The AMF responded with a DownlinkNASTransport message containing a 5GMM Status (Cause #3: "Illegal UE"), which was marked as "Protected"—meaning it was encrypted and integrity-protected. However, since 5G-AKA was incomplete, no valid security context existed for the UE to decrypt or verify this message. Per 3GPP standards (TS 24.501, Section 4.4.4.2), a UE must not process protected NAS messages without an established security context, as they cannot be authenticated and may be malicious. The UE correctly ignored the protected message by providing no response, avoiding potential exploitation (e.g., accepting forged rejections or leakage of sensitive data). This adherence to protocol—rejecting unprotected processing of protected messages pre-security-context—demonstrates secure behavior. Secure
288	288	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00081181526184082 03 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.20334196090698242 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an unprotected initial registration request to the AMF. The AMF responded with a Security Mode Command (SMC) that was marked as "Integrity protected with new security context" using 128-5G-IA2 for integrity protection and 5G-EA0 (null ciphering), despite 5G-AKA authentication not being completed. The UE rejected this SMC with a 5GMM status message indicating "Invalid mandatory information," as it lacked the necessary security context (keys) to verify the integrity of the SMC. According to 3GPP standards (TS 33.501), the SMC must be integrity-protected using keys derived from a completed 5G-AKA, which had not occurred. The UE correctly identified the unverifiable protected message as invalid, adhering to security protocols by refusing to process it without validated keys. This prevents potential security breaches from unauthenticated commands. Secure

289	289	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 6.12048602104187 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Identity response 6.120656967163086 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF, followed by the AMF issuing a subsequent Identity Request for the GUTI. This downlink request was transmitted in plain text, as the 5G-AKA authentication had not yet been completed, meaning security contexts were not established and NAS message encryption was not required at this stage. However, the UE failed to respond to the AMF's Identity Request for the GUTI, deviating from the 5G NAS protocol (3GPP TS 24.501). According to the standard, a UE must always reply to an Identity Request with either the requested identity or a valid cause code (e.g., if the identity is unavailable), even in pre-authentication states. The lack of response violates protocol specifications, potentially disrupting the registration flow and indicating improper handling of legitimate network commands. This behavior could stem from a firmware flaw or misconfiguration, leaving the UE non-compliant and vulnerable to service disruption or exploitation by rogue network elements. Insecure
290	290	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.039791107177734375 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040058135986328125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response to the AMF. Subsequently, the AMF sent an Identity Request for the IMEISV in plain text, as the 5G-AKA authentication had not yet been completed. The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), NAS messages transmitted before 5G-AKA completion lack encryption and integrity protection, making them vulnerable to interception or tampering. The IMEISV is a sensitive identifier that should not be exposed unencrypted. The standard mandates that UEs must not provide such identifiers in response to plain-text requests before security establishment, as this could facilitate tracking or spoofing attacks. By withholding the IMEISV, the UE adhered to security protocols, preventing potential leakage of device-specific information over an insecure channel. Secure

291	291	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03981208801269531 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04005002975463867 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Identity Response via an Uplink NAS Transport message, followed by the AMF sending an Identity Request for the TMSI identity in a Downlink NAS Transport message transmitted in plain text, as 5G-AKA authentication had not yet been completed. The UE failed to respond to this Identity Request. According to 3GPP standards (TS 33.501 and TS 24.501), NAS messages exchanged before 5G-AKA completion are inherently unprotected, and UEs are required to respond to identity requests during initial registration procedures to facilitate network authentication. The UE's lack of response constitutes non-compliance with protocol requirements, as it should have either provided the requested identity (if available) or returned an error cause (e.g., "identity not available"). This deviation disrupts the registration flow and may indicate improper handling of pre-authentication messaging, potentially exposing the UE to denial-of-service (DoS) risks or operational failures. While no sensitive data was leaked due to the absence of a response, the failure to adhere to standardized procedures reflects an insecure implementation. Insecure
292	292	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.11100292205810547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11120295524597168 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated)((PEI not accepted) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending an Authentication Response to the AMF, which is part of the ongoing 5G-AKA procedure. Before 5G-AKA could be completed (including the Security Mode Command exchange needed to establish a valid security context), the AMF sent a Deregistration Request message marked as "Integrity protected" (Security Header Type 1). Since the 5G-AKA process was incomplete, the UE lacked the necessary security keys to verify the message's integrity or authenticity. Per 3GPP standards (TS 33.501 and TS 24.501), a UE must not process protected NAS messages without an established security context, as they cannot be validated. The UE correctly discarded the unverifiable Deregistration Request and provided no response, avoiding potential exploitation of unauthenticated commands. This aligns with security requirements by prioritizing context establishment before processing protected messages. Secure

293	293	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.651521921157837 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 2.65175199508667 AMF to UE SACK (Ack=13, Arwnd=106429) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication and sending a Registration Complete message to the AMF. Subsequently, the AMF sent a Configuration Update Command as a plain (unprotected) NAS message, indicated by the security header type "Plain NAS message (0)". The UE did not respond to this command. According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages **must** be integrity-protected and encrypted if required by the security policy. The Configuration Update Command is a critical mobility management message that must be protected to prevent spoofing or manipulation. The UE's lack of response—neither processing the unprotected command nor explicitly rejecting it (e.g., via a Registration Request with cause #96 or a Security Mode Reject)—aligns with the standard's requirement to discard unsecured messages after security activation. This behavior prevents potential exploitation of unauthenticated commands, maintaining protocol integrity. Thus, the UE acted securely by ignoring the unsecured message, adhering to 3GPP security mandates. Secure
294	294	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 31313131313131313131005fb686550000 AUTN: 3030303030303000ee555fb686550000 ngKSI_TSC: Mapped security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 0.11998605728149414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.12024092674255371 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message, confirming successful activation of NAS security (ciphering and integrity protection) as part of the 5G-AKA process. Immediately afterward, the AMF sent an Authentication Request message containing sensitive parameters (RAND, AUTN) in plaintext, without encryption or integrity protection. According to 3GPP 5G standards (TS 33.501 and TS 24.501), once security is activated via Security Mode Complete, all subsequent NAS messages must be protected. The UE's lack of response to this unprotected Authentication Request violates the standard, as it should have rejected the message due to missing security headers and initiated a recovery procedure (e.g., restarting registration). Accepting or ignoring an unprotected message after security activation exposes the system to eavesdropping or manipulation attacks, indicating non-compliance with mandatory security protocols. Insecure

295	295	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.16016411781311035 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16040301322937012 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a security context. The UE then sent a protected **Security Mode Complete** message (indicating successful activation of NAS security as per the AMF's prior Security Mode Command), bundled with a **Registration Request**. The AMF responded with an unprotected **Service Reject** (5GMM Cause #111: "Protocol error, unspecified") in plaintext, violating the 3GPP security requirement that all NAS messages after security activation must be integrity-protected and encrypted if negotiated. According to 3GPP TS 24.501, once a security context is established (post-Security Mode Complete), the UE must discard any unprotected NAS messages and take no further action. The UE correctly discarded the AMF's plaintext Service Reject and provided no response, adhering to the standard by avoiding processing or reacting to an insecure message that could indicate a downgrade attack or manipulation. This behavior aligns with security protocols designed to mitigate threats like bidding-down attacks or rogue network impersonation. Secure
296	296	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 30303030303030007894133402560000 AUTN: 31313131313131313100133402560000 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 0.15969300270080566 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15989303588867188 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the UE sending a Security Mode Complete message, confirming the activation of NAS security (integrity protection and encryption) following a Security Mode Command from the AMF. This step typically concludes the initial security setup phase, meaning subsequent NAS messages should be protected using the established security context. However, the AMF then sent an Authentication Request in plaintext (unencrypted and without integrity protection), which is a critical deviation. According to 3GPP 5G standards (TS 33.501), once security is activated via Security Mode Complete, all following NAS messages must be protected. The UE's lack of response to this unprotected Authentication Request is appropriate, as the standard mandates discarding unsecured messages post-security activation to prevent potential downgrade attacks or manipulation. This adherence to protocol—ignoring the non-compliant message—demonstrates secure behavior by the UE. Secure

297	297	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.16003108024597168 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16027402877807617 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	After completing the 5G-AKA authentication, the UE sent a Security Mode Complete message (indicating successful activation of security algorithms) to the AMF. The AMF responded with a Deregistration Accept message (terminating the UE's registration) sent in plaintext without integrity protection or encryption. The UE did not generate any response to this message. According to 3GPP standards (TS 33.501), once 5G-AKA and the Security Mode Command/Complete exchange establish a security context, all subsequent NAS messages—including Deregistration Accept—must be integrity-protected to prevent tampering and spoofing. The UE is required to discard any non-integrity-protected NAS messages received after security context activation. Since the UE did not process the unprotected Deregistration Accept (as evidenced by no deregistration-related actions or error messages), it adhered to the standard by ignoring the invalid message, thereby maintaining session continuity and avoiding unauthorized deregistration. Secure
298	298	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.1601550579071045 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16047000885009766 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a security context. The UE then sent a **Security Mode Complete** message, confirming activation of NAS security (encryption and integrity protection) as per the Security Mode Command. Subsequently, the AMF sent an **Authentication Reject** message in **plaintext** (unencrypted and without integrity protection). The UE exhibited **no response** to this message. According to 3GPP standards (TS 24.501 and TS 33.501), once NAS security is activated (after Security Mode Complete), all subsequent NAS messages **must** be protected. An Authentication Reject is a critical NAS command that mandates both encryption and integrity protection to prevent forgery or downgrade attacks. The UE's failure to reject or respond to this unprotected message violates 5G security protocols. By accepting an unprotected critical command post-security activation, the UE ignored fundamental security requirements, exposing itself to potential spoofing or denial-of-service attacks. Insecure

299	299	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.15986394882202148 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16010284423828125 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and AMF began with the completion of 5G-AKA authentication, followed by the UE sending a Security Mode Complete message to confirm activation of NAS security (encryption and integrity protection). Immediately after, the AMF sent an Authentication Reject message in plaintext (unencrypted and without integrity protection), to which the UE did not respond. According to 3GPP 5G standards (TS 24.501 and TS 33.501), the Authentication Reject message is explicitly permitted to be sent unprotected, even after security activation, as it terminates the authentication process and invalidates the security context. The UE's silent acceptance of this unprotected message is compliant, as the standard mandates no response to Authentication Reject and requires the UE to abandon the session without further action. By processing the reject as specified—without protesting the lack of protection or attempting further communication—the UE adhered to protocol-defined security expectations, mitigating risks like session hijacking or forced re-authentication attacks. Secure
300	300	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.15969204902648926 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15989899635314941 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction began with the successful completion of 5G-AKA, establishing a security context between the UE and AMF. The UE then sent a Security Mode Complete message, confirming activation of NAS security (integrity protection and encryption). Subsequently, the AMF sent a plaintext Identity Request (requesting TMSI) without applying any security protections. The UE provided no response to this request. According to 3GPP standards (TS 33.501), once NAS security is activated via the Security Mode Command procedure, **all subsequent NAS messages must be integrity-protected and encrypted**. The Identity Request sent by the AMF violated this requirement by being transmitted in plaintext. The UE's lack of response aligns with 3GPP security specifications: a UE **must ignore or reject** any unprotected NAS messages after security activation to prevent potential exploits (e.g., bidding-down attacks or identity harvesting). By silently discarding the unsecured Identity Request, the UE adhered to security protocols, avoiding exposure of sensitive information like TMSI and maintaining the integrity of the established security context. Secure