UE Response Evaluation Report: Test time: 2025-07-21 01:55:54

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 plain text, as 5G-AKA authentication had not yet been completed to establish a security context. The UE provided no response to this request. According to 3GPP standards (TS 33.501), NAS security (including confidentiality and integrity protection) is activated only after successful 5G-AKA. While the network may request identities like IMEI during initial setup, the UE is permitted—and often configured by policy—to withhold sensitive identifiers such as IMEI when transmitted unprotected, to mitigate privacy risks like device tracking. By not responding, the UE adhered to privacy-centric principles of 5G, avoiding exposure of the permanent equipment identifier in plain text. This aligns with standard-allowed behavior to prioritize user privacy over network demands in unsecured states. 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 in plaintext, as no security context existed. The AMF responded with an Identity Request (also in plaintext) for the SUCI. The UE then provided its SUCI in an Identity Response message, transmitted without encryption. According to 3GPP standards (TS 33.501), NAS messages before 5G-AKA completion are unprotected, and transmitting SUCI in plaintext is explicitly permitted. The SUCI itself is designed to protect the SUPI through home-network public key encryption, making its plaintext transmission during initial registration secure by design. The UE complied with this protocol by responding to the identity request as required, without prematurely enforcing encryption on unprotected NAS messaging. Thus, the UE's actions align with 5G security standards. Secure

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 unencrypted NAS message, as 5G-AKA authentication had not yet been performed. The AMF responded with an Authentication Reject message, also sent unencrypted (in plain text), to which the UE provided no response. According to 3GPP standards (TS 33.501), NAS messages prior to 5G-AKA completion lack confidentiality and integrity protection, making plain-text transmission expected at this stage. The UE's lack of response aligns with standard protocol behavior upon receiving Authentication Reject, which mandates local state cleanup (e.g., deleting temporary identifiers) without further communication. Since the UE correctly processed the reject without exposing sensitive data or reacting anomalously to an unauthenticated command, its actions adhered to security protocols. The absence of encryption here is inherent to pre-authentication messaging and does not constitute a UE vulnerability. 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 authentication had not yet been completed, no secure NAS context existed. The AMF responded with a plaintext Identity Request (unencrypted) for the SUCI, as no keys were available for encryption. The UE then transmitted its SUCI in an Identity Response, also in plaintext, as 5G-AKA remained incomplete. According to 3GPP standards (TS 33.501), transmitting the SUCI before authentication is explicitly permitted and secure. The SUCI itself is a privacy-preserving identifier, encrypting the subscriber's permanent identifier (SUPI) with the home network's public key, ensuring confidentiality even over unencrypted transport. The UE correctly prioritized network-directed identity provisioning over unsolicited transmission in the Registration Request, adhering to standard procedures for initial authentication bootstrapping. No deviation from expected behavior occurred. 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 unencrypted Initial Registration Request to the AMF, as 5G-AKA authentication had not yet been completed. The AMF responded with a plaintext Registration Reject message containing 5GMM Cause #111 ("Protocol error, unspecified"), which terminates the registration procedure according to 3GPP TS 24.501. Instead of halting further communication attempts or waiting for backoff timers, the UE unnecessarily transmitted a Deregistration Request (UE originating) in plaintext. This action is insecure because: (1) The UE was never successfully registered, making deregistration illogical and non-compliant with standard state management (TS 24.501 § 5.5.1.2); (2) Transmitting any NAS message post-rejection without security context violates 5G security principles by exposing sensitive data (e.g., UE identity); (3) It disregards Cause #111's directive to abort the procedure, potentially facilitating eavesdropping or replay attacks. The UE should have transitioned to a DEREGISTERED state without additional transmissions. Insecure
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 Initial Registration Request to the AMF. Since 5G-AKA had not been completed, no security context existed. The AMF responded with a plain (unencrypted) Registration Reject message containing 5GMM Cause 22 (congestion), which is permitted at this pre-authentication stage. However, the UE then transmitted a Deregistration Request (UE originating) in an UplinkNASTransport message. According to 3GPP TS 24.501, upon receiving a Registration Reject with Cause 22, the UE should initiate a timer (T3346) and refrain from sending any new NAS signaling messages (except for emergency services) until the timer expires. The UE's transmission of a Deregistration Request violates this requirement, as it constitutes unnecessary NAS signaling during a congestion state. This behavior could exacerbate network congestion, create signaling storms, and expose the UE to potential tracking or denial-of-service attacks by generating observable traffic when the standard mandates radio silence. The action demonstrates non-compliant handling of congestion procedures, undermining network stability and security protocols. 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. The AMF responded with an Authentication Request containing a RAND value of all zeros and an AUTN value of `32303030007f0000ee555cc720560000`, transmitted in plaintext since 5G-AKA was incomplete. The UE rejected this with an Authentication Failure message, specifying the cause "Non-5G authentication unacceptable." This cause indicates the UE detected that the AUTN did not comply with 5G requirements, specifically the absence of the mandatory 5G separation bit (bit 7 of the first AMF byte set to 1) in the AUTN structure, as defined in 3GPP TS 33.501. The AUTN's AMF field (`0000`) had a separation bit of 0, signaling legacy (non-5G) authentication. By rejecting this non-compliant AUTN and halting the procedure, the UE adhered to 3GPP security standards, preventing potential downgrade attacks or insecure context establishment. Secure

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: 313030300000000078742b94d4550000 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 to the AMF. The AMF responded with an Authentication Request containing a RAND value and an AUTN (Authentication Token) of all zeros, sent in plaintext due to the incomplete 5G-AKA procedure. The UE rejected this request by sending a 5GMM Status message with the cause "Invalid mandatory information" (#96), indicating it detected an issue with a mandatory information element (IE)—specifically, the invalid AUTN. According to 3GPP TS 33.501 and TS 24.501, the AUTN must include a valid MAC (Message Authentication Code) and sequence number for network authentication. An AUTN of all zeros is syntactically incorrect and fails to provide these elements, constituting a semantic error in a mandatory IE. The UE correctly identified this flaw and aborted the authentication process, preventing potential security risks like fake network attacks. While the standard mandates an Authentication Failure message (e.g., for MAC failure) in such cases, the UE's use of a 5GMM Status message with cause #96 is still a compliant rejection mechanism for fundamental IE errors (TS 24.501). The UE prioritized security by refusing to proceed with an invalid authentication, aligning with 5G's security objectives despite the non-ideal message choice. Secure

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 initial Identity Response, followed by the AMF transmitting a plaintext Identity Request (demanding SUCI). The UE then provided another Identity Response. Crucially, 5G-AKA authentication had not been completed at this stage, meaning no security context (keys for encryption/integrity protection) was established. According to 3GPP standards (TS 33.501), initial identity transfers—specifically SUCI—are explicitly permitted in plaintext before authentication, as SUCI is designed to conceal the permanent subscriber identifier (SUPI) using home network public key encryption. The UE's response with SUCI aligns with this exception, as sending it unprotected is mandated when no security context exists and authentication is pending. The UE did not transmit sensitive data (e.g., SUPI) in plaintext, nor did it process protected NAS messages without keys, adhering to protocol requirements. Secure

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: 313131313131313131006f90d2550000 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, followed by the AMF issuing a plaintext Authentication Request containing a RAND, AUTN, and ngKSI_KSI value of 2. The UE rejected this request with an Authentication Failure message, specifically citing "ngKSI already in use" as the cause. According to 3GPP TS 33.501, the ngKSI (Key Set Identifier) uniquely identifies a security context between the UE and network. If the UE receives an ngKSI value (here, 2) that matches an existing active or partial native security context, it must reject the authentication attempt to prevent security context confusion or overwriting. This behavior aligns with the standard's requirement to protect against erroneous key reuse, which could compromise subsequent security procedures. By explicitly rejecting the request and avoiding further processing of the compromised authentication challenge, the UE upheld the 5G security framework. The plaintext nature of the exchange is expected at this pre-authentication stage, as 5G-AKA had not yet completed to enable encryption. 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, which was transmitted unencrypted as the 5G-AKA authentication had not yet been completed. The AMF responded with a Service Reject message containing 5GMM Cause #11 ("PLMN not allowed"), sent in plain text due to the absence of an established security context. The UE, upon receiving this rejection, took no further action, as indicated by "UE provided: No response." According to 3GPP standards (TS 24.501 and TS 33.501), NAS messages like Identity Response and Service Reject are permitted to be sent unprotected before 5G-AKA completion, as encryption/integrity protection relies on keys derived during authentication. The UE's transmission of the Identity Response in plain text aligns with this expectation, as security contexts are negotiated post-authentication. Similarly, its lack of response to the Service Reject is standard-compliant behavior for a permanent rejection (Cause #11), which mandates that the UE cease communication attempts with the forbidden PLMN. No deviation from protocol-specified actions was observed. 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 initial Identity Response (likely containing a temporary identifier like 5G-GUTI) as part of earlier NAS steps. Subsequently, the AMF sent a new Identity Request (plaintext, as 5G-AKA was incomplete) demanding the SUCI. The UE responded with a second Identity Response containing the SUCI, also sent in plaintext. This sequence occurred because 5G-AKA—which establishes encryption keys—had not yet been performed, leaving NAS messages unprotected. According to 3GPP standards (TS 33.501), transmitting the SUCI in plaintext is explicitly permitted during initial registration before authentication, as the SUCI itself is a privacy-preserving identifier (encrypted by the UE using the home network's public key). The UE's compliance with the AMF's request for SUCI without security context aligns with the protocol's design to facilitate initial network access. Sending two Identity Responses is acceptable, as the first may have been for a prior request, and the second explicitly provided the SUCI as instructed. No deviation from the standard or unnecessary exposure of sensitive data (e.g., SUPI) occurred. 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, as part of the initial NAS registration procedure. The AMF then responded with an Authentication Reject message, sent in plain text, to which the UE provided no further response. Crucially, the 5G-AKA authentication process had not been completed at this stage, meaning no security context (including ciphering and integrity protection) had been established between the UE and the AMF. According to 3GPP standards (TS 33.501 and TS 24.501), NAS messages exchanged prior to 5G-AKA completion are inherently unprotected and may be transmitted in plain text without violating security protocols. The UE's lack of response to the Authentication Reject aligns with 3GPP specifications, which mandate that the UE must abort the registration process, enter a DEREGISTERED state, and refrain from further communication upon receiving this message—regardless of its unprotected format. No evidence suggests the UE ignored security protocols or attempted to proceed with an unauthenticated session. Thus, the UE's actions adhered to 5G security requirements by terminating the procedure as expected when authentication fails. 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 message to the AMF via Uplink NAS Transport, which was unencrypted since 5G-AKA authentication had not yet been completed. The AMF responded with a Downlink NAS Transport message containing a Registration Reject, sent in plaintext with 5GMM Cause #22 (indicating network congestion). The UE did not send any further response to this rejection. According to 3GPP standards (TS 24.501 and TS 33.501), before 5G-AKA completes and a security context is established, initial NAS messages (including Identity Response and Registration Reject) may be transmitted unprotected. The UE's acceptance of the plaintext Registration Reject is permissible at this pre-authentication stage, as no security context exists to enforce encryption or integrity protection. Additionally, the UE correctly ceased communication upon rejection, aligning with standard behavior for congestion-related terminations. No evidence suggests the UE processed sensitive data or violated protocol requirements during this exchange. 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 to the AMF, followed by the AMF sending a plain-text Authentication Request containing a RAND (30303030303030007844783aae550000) and an all-zero AUTN (00000000000000000000000000000000), indicating an invalid or malformed authentication token. The UE rejected this request by responding with an Authentication Failure message, explicitly citing "Non-5G authentication unacceptable" as the cause. According to 3GPP standards (TS 33.501), the AUTN is critical for network authentication, and an all-zero AUTN is invalid as it fails to provide the necessary security parameters (e.g., SQN and MAC) for the UE to verify the network's legitimacy. The UE's refusal to proceed aligns with security requirements, as accepting such an invalid AUTN could expose it to spoofing attacks or bidding-down attempts (where the network might force weaker legacy authentication). By terminating the procedure, the UE enforced mutual authentication integrity, a core 5G security principle. 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 to the AMF after completing 5G-AKA, indicating successful mutual authentication. The AMF then responded with a Security Mode Command, sent in plaintext, specifying the ciphering algorithm (128-5G-EA1), integrity algorithm (5G-IA7), and ABBA parameter (3200). This command initiates the activation of NAS security. However, the UE provided no response—neither a Security Mode Complete nor a Security Mode Reject message—leaving the security setup incomplete. According to 3GPP standards (TS 24.501 and TS 33.501), after receiving the Security Mode Command, the UE must validate the algorithms and ABBA value, then respond to confirm or reject security activation. The absence of a response prevents the establishment of integrity protection and encryption for subsequent messages, violating the protocol's security sequence. This omission leaves the UE vulnerable to attacks such as downgrade attempts or manipulation of unprotected NAS messages, as the AMF cannot enforce security without UE confirmation. 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 to the AMF, as part of the 5G-AKA procedure to establish a security context. Before this authentication could complete, the AMF responded with a Service Reject message containing 5GMM Cause #111 ("Protocol error, unspecified"), sent unencrypted (plain) due to the incomplete 5G-AKA. The UE did not transmit any further messages after receiving this rejection. According to 3GPP standards (TS 24.501 and TS 33.501), NAS messages exchanged prior to 5G-AKA completion lack encryption and integrity protection, making them vulnerable to interception or forgery. The UE's cessation of communication aligns with protocol expectations for handling Service Reject messages, which terminate the registration attempt. However, the UE's failure to validate the Service Reject's authenticity or handle the unprotected message cautiously exposes a security gap. Attackers could forge such unsecured rejections to force service denials, and the UE's passive acceptance without countermeasures (e.g., logging the error for diagnostics or restarting registration after a timeout) disregards potential man-in-the-middle threats. While the UE's non-response adheres to basic procedural requirements, its inability to detect or mitigate risks from unauthenticated rejection messages reflects an insecure posture against spoofing attacks during the vulnerable pre-authentication phase. Insecure

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 in plaintext, as 5G-AKA had not yet been completed. The AMF then sent a downlink Identity Request in plaintext, explicitly asking for the SUCI (Subscription Concealed Identifier). The UE responded with an Identity Response containing the SUCI, also transmitted in plaintext. According to 3GPP standards (TS 33.501), NAS messages exchanged before 5G-AKA completion lack encryption and integrity protection, making plaintext transmission expected at this stage. Crucially, the UE correctly provided the SUCI—a public key-encrypted identifier designed to protect user privacy—instead of the sensitive IMSI. This aligns with 3GPP requirements, as the SUCI is intended for transmission in plaintext prior to authentication. While the unencrypted exchange inherently carries risks (e.g., potential eavesdropping), the UE adhered to the protocol by supplying the SUCI as requested, mitigating exposure of raw credentials. No deviation from the standard was observed in the UE's behavior. 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, establishing mutual authentication and keys. The UE sent an Authentication Response, after which the AMF transmitted a Security Mode Command (SMC) protected with integrity using the 128-5G-IA2 algorithm but specifying null ciphering (5G-EA0). The SMC was marked with the security header type 3, indicating integrity protection with a new security context. Instead of accepting these parameters, the UE responded with a Security Mode Reject, citing an unspecified cause. This rejection is significant because while 3GPP standards mandate UE support for null ciphering (5G-EA0), they do not require UEs to accept it when network policies or UE security configurations demand confidentiality. By rejecting the SMC due to the lack of encryption—despite the integrity protection—the UE demonstrated adherence to a stricter security posture, prioritizing data confidentiality as a defense against potential eavesdropping or interception. This aligns with security best practices and the principle of enforcing higher protection levels when feasible, even though the rejection cause was unspecified. Thus, the UE's action enhances security by refusing a vulnerable configuration. 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, followed by the AMF sending an Authentication Request (containing RAND, AUTN, ABBA, and ngKSI parameters) in plaintext, as the 5G-AKA procedure was not yet completed and no security context existed. The UE then responded with a second Authentication Response. According to 3GPP standards (TS 33.501), initial NAS messages prior to 5G-AKA completion are required to be sent unencrypted, as cryptographic keys have not yet been established. The UE's acceptance and processing of the plaintext Authentication Request—and its subsequent response—are compliant with protocol expectations during this pre-security phase. No deviation from the standard was observed in the UE's behavior, as it correctly handled the authentication sequence without prematurely enforcing encryption. 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, followed by the AMF sending a downlink Authentication Request containing RAND, AUTN, and security parameters (ngKSI=4, ABBA=0000) in plain text, as 5G-AKA had not yet established a security context. The UE detected a MAC (Message Authentication Code) failure in the AUTN (Authentication Token), indicating that the MAC embedded in the AUTN did not match the UE's calculation based on its shared secret key (K). Consequently, the UE responded with an Authentication Failure message, explicitly citing "MAC failure" as the cause. This behavior aligns with 3GPP TS 33.501 security standards, which mandate that the UE must validate the AUTN's MAC to authenticate the network and reject the request if verification fails. By doing so, the UE prevented potential connection to an untrusted network impersonating the AMF, demonstrating correct implementation of the security protocol. The plaintext transmission was unavoidable here, as encryption keys are derived only after successful 5G-AKA completion. 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: 3131313131313131310057a1d8550000 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 replied with a plain-text Authentication Request containing RAND, AUTN, ABBA, and ngKSI parameters. The UE analyzed the AUTN and detected that it was formatted for a non-5G authentication method (e.g., 4G EPS-AKA), as indicated by the AUTN structure and the AMF separation bit. Consequently, the UE rejected the authentication attempt with an "Authentication failure (Non-5G authentication unacceptable)" message, as mandated by 3GPP TS 24.501 § 5.4.1.2. This action aligns with 5G security standards, which require UEs to strictly enforce 5G-specific authentication (5G-AKA) to prevent potential downgrade attacks or compatibility issues with legacy systems. By terminating the procedure instead of processing non-compliant credentials, the UE upheld 5G security requirements. 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 successful completion of 5G-AKA mutual authentication, after which the UE sent an Authentication Response. The AMF then issued a Security Mode Command (SMC) protected with integrity using the 128-5G-IA2 algorithm but proposed null encryption (5G-EA0). The SMC was marked with security header type 3, indicating integrity protection under a new security context. Despite the AMF's compliance with 3GPP standards—which permit null encryption for NAS signaling when integrity is enforced—the UE responded with a Security Mode Reject, citing an unspecified reason. This rejection is non-compliant because 3GPP mandates UE acceptance of valid SMC messages when the integrity algorithm (128-5G-IA2, a mandatory-supported algorithm) is usable and the message passes integrity verification. The UE's unspecific rejection halted security context activation, leaving subsequent communications unprotected and violating TS 33.501 security protocols. This behavior suggests a flaw in UE implementation, as it failed to proceed with standardized security measures without justification, exposing the session to potential threats. Insecure

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 between the UE and AMF began with the UE sending an unsolicited Authentication Response message (without prior receipt of an Authentication Request from the AMF). Subsequently, the AMF sent an Authentication Request (including RAND, AUTN, and ABBA parameters) in plaintext, as required by the 5G-AKA protocol before security establishment. The UE then sent a second Authentication Response, which is the expected reply to the AMF's request. According to 3GPP standards (TS 33.501), initial authentication messages like the first Authentication Request/Response must be sent unprotected since no security context exists at this stage. However, the UE's transmission of an unsolicited Authentication Response before receiving the AMF's challenge deviates from the standard protocol sequence, where the network must initiate authentication with an Authentication Request. This unsolicited message could expose sensitive data (e.g., premature authentication parameters) or indicate improper state handling, violating the protocol's security assumptions. While the plaintext exchange of the AMF's Authentication Request and the UE's second response is standard-compliant, the initial unsolicited UE message constitutes an insecure anomaly. 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, as part of the 5G-AKA procedure to establish a security context. However, before this process completed, the AMF responded with an Authentication Reject message sent in plain text (unencrypted), indicating authentication failure. Since 5G-AKA was not finalized, no security context existed, meaning encryption or integrity protection was neither established nor required by the standard at this stage. The UE then initiated a UE-originating Deregistration Request, also unencrypted, acknowledging the rejection and terminating the registration. According to 3GPP standards (TS 33.501), NAS messages exchanged prior to authentication completion—including Authentication Reject and immediate follow-up actions like deregistration—are explicitly permitted to be unprotected, as security keys are derived only after successful authentication. The UE's actions align with this protocol: it processed the reject correctly and responded with a standard deregistration, avoiding further unprotected communication beyond necessary procedural closure. There is no indication of non-compliant behavior or unnecessary exposure of sensitive data. Secure

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 mutual authentication and security keys. The UE then sent a Security Mode Complete message, confirming activation of NAS security. Subsequently, the AMF sent a protected Deregistration Request (security header type 2, indicating integrity protection and ciphering), which the UE processed. The UE responded with a Deregistration Accept message. However, based on the packet capture and test summary, the UE's Deregistration Accept was sent without explicit indication of protection (i.e., no security header type 2). According to 3GPP TS 33.501, after Security Mode Complete, all subsequent NAS messages—including Deregistration Accept—must be integrity-protected and ciphered to prevent tampering and eavesdropping. The UE's failure to protect this message violates the standard, exposing it to potential security threats. 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.	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 (as required by the standard during security context activation). Subsequently, the AMF sent a protected Deregistration Request (security header type 2: integrity-protected and ciphered), which is standard for post-activation downlink messages. The UE responded with a Deregistration Accept message. Crucially, this uplink Deregistration Accept was sent without protection, as indicated by the packet capture's lack of security header notation (contrasting with the explicit "Protected" label for the AMF's message) and the absence of any mention of integrity or encryption in the test summary. According to 3GPP TS 33.501, after security activation, all NAS messages—except specific procedural exceptions like the initial Security Mode Complete—must be integrity-protected and encrypted to mitigate tampering, forgery, and eavesdropping risks. The UE's failure to protect the Deregistration Accept violates this mandate, exposing the network to potential attacks where an adversary could forge acceptance messages. 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, indicating prior completion of 5G-AKA authentication and initial security activation. Subsequently, the AMF transmitted a Security Mode Command message protected with the new security context (security header type 3), specifying ciphering algorithm 128-5G-EA2 but selecting null integrity algorithm (5G-IA0). The UE rejected this command with a Security Mode Reject (unspecified reason). According to 3GPP TS 33.501, null integrity (NIA0) is explicitly prohibited for NAS signaling protection after 5G-AKA completion, except for pre-authentication emergency services. By rejecting the AMF's command proposing NIA0—which would leave NAS messages without integrity protection—the UE adhered to 5G security standards, preventing potential downgrade attacks or manipulation of unprotected signaling. This action demonstrates robust compliance with mandatory security requirements. 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.	After completing the 5G-AKA authentication, the UE sent a Security Mode Complete message, indicating acceptance of prior security parameters. The AMF then sent a Security Mode Command protected with security header type 3 (indicating integrity protection) but specifying null algorithms for both ciphering (5G-EA0) and integrity (5G-IA0). The UE responded with a Security Mode Reject, citing an unspecified reason. According to 3GPP TS 33.501 standards, null algorithms (5G-EA0/5G-IA0) must never be activated simultaneously, as this leaves communications entirely unprotected. The AMF's command violated this by attempting to set both algorithms to null while paradoxically claiming integrity protection—a critical inconsistency. The UE correctly identified this invalid configuration and rejected the command, adhering to 3GPP security requirements by preventing an insecure security context establishment. 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 UE prematurely sending a **Security Mode Complete** message (alongside a Registration Request) in an UplinkNASTransport *before* receiving the AMF's **Security Mode Command**. This was followed by the AMF sending a protected DownlinkNASTransport containing the Security Mode Command (specifying ciphering algorithm 5G-EA7, integrity algorithm 128-5G-IA2, and ABBA parameter 3000), after which the UE sent another Security Mode Complete. According to 3GPP standards (TS 33.501), the Security Mode Command (SMC) must be initiated by the network to activate NAS security after 5G-AKA completion. The UE is then required to wait for, validate, and process the SMC before responding with Security Mode Complete. Here, the UE's first Security Mode Complete was sent proactively without receiving or validating the SMC, violating the protocol sequence. This premature transmission indicates non-compliant behavior, as the UE should never generate Security Mode Complete without cryptographic confirmation of the SMC. Such an action risks processing unprotected or rogue network commands and undermines mutual authentication integrity. 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 UE sending a Security Mode Complete message alongside a Registration Request, indicating the completion of the initial 5G-AKA authentication. The AMF responded with a Security Mode Command, protected with a new security context (security header type 3), which specified the use of the 5G-EA4 ciphering algorithm and null integrity protection (5G-IA0). Subsequently, the UE transmitted a Deregistration Request (UE originating) without any explicit indication of integrity protection or ciphering in the provided capture. According to 3GPP standards (TS 33.501), null integrity protection (5G-IA0) is explicitly prohibited for sensitive NAS signaling messages like Deregistration Request after security activation, as it leaves messages vulnerable to tampering and replay attacks. The UE should have either rejected the AMF's Security Mode Command (due to the invalid selection of null integrity for protected signaling) or applied integrity protection to the Deregistration Request. By accepting the command and sending an unprotected sensitive message, the UE violated 3GPP 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 began with the UE sending a Security Mode Complete message alongside a Registration Request, indicating it had completed security activation steps. Subsequently, the AMF transmitted a Security Mode Command message, which was protected using both integrity protection (128-5G-IA3) and ciphering (5G-EA4) with security header type 2. However, the UE provided no response to this command. According to 3GPP standards (TS 24.501 and TS 33.501), the initial Security Mode Command—which establishes NAS security—must be sent with integrity protection (security header type 1) but without ciphering, as the UE lacks the active ciphering context to decrypt it at this stage. The AMF's use of a ciphered command (type 2) violates this requirement, rendering the message unprocessable by the UE. The UE's lack of response aligns with the standard's expectations, as it cannot act upon an improperly secured command, avoiding potential security compromises like accepting unverified algorithms or keys. Thus, the UE's behavior was correct and secure. Secure
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 successfully completing 5G-AKA and sending a Security Mode Complete message, confirming the activation of NAS security. The AMF responded with a protected GMM Status message containing cause value 6 ("Illegal ME"), indicating a permanent rejection due to invalid mobile equipment. Despite this network rejection—which mandates immediate local deregistration without further signaling per 3GPP TS 24.501—the UE improperly sent a Deregistration Request. This action violated the standard, as the UE should have silently transitioned to a deregistered state, discarded security context (e.g., 5G-GUTI, TAI list), and halted non-emergency communication. By transmitting an unnecessary Deregistration Request after a final rejection, the UE ignored protocol requirements, potentially exposing itself to threats like signaling storms or manipulation, as it continued using the compromised security context. Thus, the UE's behavior was non-compliant and insecure. Insecure

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 a NAS security context. The UE sent a Security Mode Complete message, confirming activation of security algorithms, followed by a Registration Request. Subsequently, the AMF sent a protected Deregistration Request (UE-terminated), which was integrity-protected and ciphered (security header type 2), as required by the 3GPP standard after security context establishment. The UE responded with a Deregistration Accept message. Crucially, the UE's Deregistration Accept was sent without NAS-layer protection (no integrity or ciphering), as evidenced by the absence of security header indicators in the test summary and packet capture description. This violates 3GPP TS 33.501, which mandates that all NAS messages after Security Mode Complete must be protected to prevent tampering and eavesdropping. The UE's failure to apply protection constitutes a security flaw, as an unprotected Deregistration Accept could be forged or manipulated by an attacker. 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 successful completion of 5G-AKA, establishing a security context between the UE and AMF. The UE then sent an uplink message containing both a Security Mode Complete and a Registration Request, indicating acceptance of the security parameters. Subsequently, the AMF responded with a Service Accept message, which was explicitly noted as protected (encrypted and integrity-protected) per 5G security requirements. The UE did not generate a response to the Service Accept, which aligns with standard behavior, as this message typically concludes the exchange without mandating further acknowledgment from the UE. Critically, after 5G-AKA and the Security Mode Command (not explicitly captured but implied by the UE's Security Mode Complete), all subsequent NAS messages must be protected under 3GPP standards (TS 33.501). The UE's Security Mode Complete (and bundled Registration Request) should have been protected, though the test summary does not explicitly verify this. However, given the completion of 5G-AKA and the absence of noted anomalies in the uplink, alongside the UE's adherence to procedural expectations (e.g., no response needed for Service Accept), the UE's actions appear compliant. The AMF's protected downlink further confirms network-side security activation, and no evidence suggests the UE bypassed protection requirements. Thus, the UE operated securely within the 5G framework. 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 successful completion of 5G-AKA, establishing a secure context for NAS communication. The UE sent a Registration Complete message, and the AMF responded with a Deregistration Request (UE-terminated), which was correctly protected with both integrity and ciphering (security header type 2) per 3GPP TS 24.501. The UE then sent a Deregistration Accept. However, the test summary and packet capture indicate that this Deregistration Accept message was transmitted without explicit mention of security protection (e.g., no security header type 2 indicated). According to 3GPP standards, once 5G-AKA is completed, all subsequent NAS messages—including Deregistration Accept—must be integrity-protected and ciphered to maintain confidentiality and prevent tampering, barring specific exceptions like initial registration or service reject with cause #31 (none of which apply here). The UE's failure to protect this response leaves it vulnerable to eavesdropping or manipulation, violating 3GPP security requirements. 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 UE sending a Registration Complete message, followed by the AMF responding with a protected Service Accept message after successful 5G-AKA authentication. Subsequently, the UE initiated a Deregistration Request (UE originating) without enabling NAS security protection. According to 3GPP standards (TS 33.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages—including deregistration requests—must be both integrity-protected and encrypted to prevent eavesdropping, tampering, or replay attacks. The UE's failure to protect this sensitive deregistration request, transmitted in plaintext (as implied by the lack of protection notation in the test summary and packet capture), violates 5G security requirements. This exposes the message to potential interception or manipulation, undermining confidentiality and authentication safeguards. 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 an unprotected Registration Complete message to the AMF, indicating the conclusion of initial NAS procedures. The AMF then responded with a Security Mode Command (SMC), which was integrity-protected using the new security context (security header type 3) and specified the integrity algorithm 128-5G-IA2 and null ciphering (5G-EA0). The UE, however, provided no response to this command. According to 3GPP 5G security standards (TS 33.501), after successful 5G-AKA authentication, the UE must validate the integrity of the SMC using the newly established keys and algorithms, activate the specified security context, and respond with a Security Mode Complete message to confirm synchronization. The UE's failure to respond violates this critical handshake, leaving the security context unconfirmed and subsequent communications vulnerable to downgrade attacks or misaligned security states. This omission breaks the mutual authentication and context activation process, undermining the security framework. 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 began with the successful completion of 5G-AKA, establishing a secure NAS context between the UE and AMF. Following this, the UE sent a Registration Complete message. The AMF then issued a protected Configuration Update Command (security header type 2, indicating integrity protection and ciphering), consistent with 3GPP TS 33.501 requirements for post-authentication messaging. The UE responded appropriately with a Configuration Update Complete message. Critically, after 5G-AKA, 3GPP mandates that all subsequent NAS messages—including UE-originated responses like Configuration Update Complete—must be both integrity-protected and ciphered (security header type 2) to prevent tampering or eavesdropping. The test summary explicitly confirms the AMF's downlink message was protected but does not specify the security header for the UE's uplink Configuration Update Complete. However, given that: - The security context was active, - The UE had just processed a protected command, - 3GPP TS 24.501 § 4.4.5 requires protected responses in this state, and - The test would likely highlight a deviation if the UE sent an unprotected message (as this is a security test focused on UE behavior), it is reasonable to infer the UE adhered to the standard by protecting its response. No vulnerability or non-compliance is indicated in the provided data. Secure

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 mutual authentication and security keys 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). The UE then responded with a Configuration Update Complete message. According to 3GPP TS 24.501, after 5G-AKA and upon receiving a protected NAS message (like the Configuration Update Command), the UE must protect all subsequent NAS messages, including responses like Configuration Update Complete, using both integrity protection and ciphering. The test summary explicitly noted the AMF's downlink message as protected but omitted any security indication for the UE's Configuration Update Complete, implying it was sent unprotected. This violates 5G security standards, as UEs must maintain protection once a security context is established and after receiving secured network commands. The UE's failure to protect this response exposes it to potential tampering or eavesdropping. 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 begins with the UE sending a Registration Complete message to the AMF. The AMF responds with a Security Mode Command, which is integrity-protected using the new security context (indicated by security header type 3) and specifies the ciphering (128-5G-EA2) and integrity (128-5G-IA2) algorithms, along with ABBA parameter 0272. According to 5G standards (3GPP TS 33.501), upon receiving this command, the UE must verify the message's integrity using the newly established K~AMF~ key (from the completed 5G-AKA) and respond with a Security Mode Complete message to confirm activation of the security context. However, the UE sends no response to the Security Mode Command. Instead, it initiates a new Service Request via an InitialUEMessage without completing the security setup. This Service Request is sent unprotected, as the security context remains unconfirmed, and the AMF rejects it due to inability to derive the UE identity—consistent with a lack of valid security context. By omitting the mandatory Security Mode Complete, the UE violates the 5G security protocol, which requires explicit confirmation before proceeding with subsequent protected communications. This failure leaves the UE vulnerable to security threats, such as bidding-down attacks or processing unauthorized commands, as the security context activation is incomplete. 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 sent an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Downlink NAS Transport carrying a Configuration Update Command, followed by another Downlink NAS Transport with a Deregistration Accept (UE terminated) message, which was protected using the established security context. The UE provided no response to the Deregistration Accept. According to 3GPP standards (TS 24.501), a Deregistration Accept is only valid as a network response to a UE-initiated deregistration request. Here, the UE did not initiate deregistration; its last uplink was a session request. The Deregistration Accept (UE terminated) is anomalous and unsolicited. A secure UE must ignore such unexpected messages after verifying integrity protection, as processing them could trigger erroneous deregistration. The UE's lack of response suggests it discarded the message after successful security verification (since the message was protected), avoiding inappropriate state changes. This aligns with standard security requirements for handling malformed or unsolicited NAS messages. Secure

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.	The interaction began with the UE completing 5G-AKA, establishing a secure context, and sending an Uplink NAS Transport containing Registration Complete and a PDU session establishment request. The AMF responded with a protected (integrity-protected and ciphered) Configuration Update Command, adhering to 5G security standards. Subsequently, the UE initiated deregistration by sending a Deregistration Request (UE originating) via Uplink NAS Transport. According to 3GPP TS 33.501, after 5G-AKA completion, all NAS messages—except specific exceptions like initial registration—must be protected to prevent tampering or eavesdropping. The Deregistration Request is not an exempted message and must be integrity-protected at minimum. The UE's failure to protect this request (as indicated by the absence of security-header notation in the test summary and packet capture) violates 3GPP mandates, leaving the message vulnerable to forgery or replay attacks. This oversight compromises session integrity and constitutes a security flaw. 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 (including Registration Complete and a PDU Session Establishment Request) after successful 5G-AKA authentication. The AMF responded with a protected Configuration Update Command and then a protected Deregistration Request (UE-terminated), which was integrity-protected and ciphered (security header type 2), as confirmed by the test summary. The UE replied with a Deregistration Accept message. According to 3GPP TS 33.501 and TS 24.501, once 5G-AKA completes and a security context is established, all subsequent NAS messages—including Deregistration Accept—must be both integrity-protected and ciphered to prevent tampering and eavesdropping. The test summary explicitly noted the AMF's Deregistration Request as protected but did not indicate equivalent protection for the UE's Deregistration Accept, and the packet capture lacked any mention of security headers or protection for this uplink message. Since the UE sent the Deregistration Accept without the required security measures despite an active security context, this violates 5G security standards. 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 UE sending a UL NAS Transport message (Registration Complete and PDU Session Establishment Request) after successful 5G-AKA authentication. The AMF responded with a Configuration Update Command, which was protected with both integrity and ciphering (security header type 2), as confirmed by the test summary. The UE processed this protected command and responded 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 to prevent tampering, and ciphering is required for confidentiality if supported by the UE's security capabilities. The UE correctly validated the AMF's protected Configuration Update Command—ensuring its authenticity and integrity—before responding. This adherence to mandatory protection mechanisms demonstrates that the UE enforced security policies as specified, rejecting any potential unprotected or altered commands. 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 a secure NAS context for integrity and encryption. The UE initiated communication by sending a protected UL NAS Transport (Registration Complete and 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) as mandated by 3GPP TS 33.501 after security context activation. The UE responded with a Configuration Update Complete message. Given that the security context was active (evidenced by the AMF's protected downlink message), 3GPP requires all subsequent NAS messages to be protected. The UE's Configuration Update Complete was sent as a UplinkNASTransport without any noted security failure or error, implying it adhered to the established security context. Since the test summary and packet capture lack indications of unprotected transmission or protocol violations, the UE's actions align with 5G security standards by maintaining protection throughout the exchange. 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 after the successful completion of 5G-AKA, establishing a security context for NAS communication. The UE initiated by sending an Uplink NAS Transport message, which included Registration Complete and a PDU Session Establishment Request. Subsequently, the AMF sent a Downlink NAS Transport message containing a Configuration Update Command, explicitly noted as protected with both integrity protection and ciphering (security header type 2). The UE responded with an Uplink NAS Transport message confirming Configuration Update Complete. According to 3GPP standards (TS 33.501), once 5G-AKA completes, all subsequent NAS messages must be integrity-protected and ciphered unless explicitly exempted (e.g., initial registration). The UE's acceptance and processing of the protected Configuration Update Command—verified by its valid integrity check and successful decryption—demonstrated adherence to security protocols. The UE correctly responded with Configuration Update Complete only after validating the protected command, confirming it enforced mandatory security requirements. There is no indication of the UE accepting unprotected sensitive messages or bypassing security checks. Thus, the UE operated securely within the 5G framework. 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 message (Registration Complete and PDU Session Establishment Request) after completing 5G-AKA authentication. The AMF responded with a Configuration Update Command and then a Security Mode Command (SMC), which was integrity-protected using the existing security context established during 5G-AKA. The SMC specified ciphering algorithm 5G-EA4 (undefined in 3GPP standards) and integrity algorithm 128-5G-IA2 (valid AES-based algorithm). The UE rejected the SMC with a Security Mode Reject (cause: "unspecified"). According to 3GPP TS 33.501, valid ciphering algorithms are 5G-EA0 to 5G-EA3 (assigned identifiers 0-3); 5G-EA4 (identifier 4) is reserved and not standardized. The UE correctly identified this invalid algorithm proposal, preventing potential security risks from non-standard encryption. Although the rejection cause was generic ("unspecified"), the UE adhered to security principles by refusing an undefined ciphering algorithm, maintaining compliance with 3GPP standards. 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 to initiate communication, followed by the AMF responding with a Security Mode Command protected with integrity (Security Header Type 3) but proposing null ciphering (5G-EA0) and 128-5G-IA2 for integrity. The UE rejected this command with a Security Mode Reject (cause: "unspecified"). Based on 3GPP standards (TS 33.501), the UE's rejection is **secure**. After successful 5G-AKA, the UE possesses keys to verify the AMF's integrity protection, confirming the command's authenticity. However, the AMF's proposal to use null ciphering (5G-EA0) violates 3GPP requirements, as null encryption is explicitly forbidden for user data and sensitive signaling outside specific exceptions (e.g., emergency services without authentication). By rejecting this insecure configuration—despite the integrity protection—the UE adheres to security principles by refusing to disable encryption, thus preventing potential eavesdropping or data exposure. The "unspecified" reject cause aligns with standard behavior when algorithm negotiation fails. 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 sending a Service Request (uplink) to the AMF, indicating a mobile-originated data request, following a completed 5G-AKA that established secure keys. The AMF responded with a protected Deregistration Accept (downlink) message, which was integrity-protected and encrypted per 5G security requirements, as confirmed by the "Protected" status. However, the UE exhibited no response to this message. According to 3GPP standards (TS 24.501), a Deregistration Accept (UE-terminated) is typically sent by the network during deregistration initiated by the AMF, and upon receiving such a protected message, the UE is required to process it, verify its integrity, and either comply with deregistration or react if verification fails. The UE's lack of response—despite successful 5G-AKA and the AMF's correctly protected message—suggests it failed to validate or acknowledge the deregistration command. This deviation indicates non-compliance with standard security procedures, as UEs must handle protected NAS messages appropriately to maintain session integrity and prevent potential exploits like forced deregistration without challenge. Insecure

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 sending a Service Request to the AMF after completing 5G-AKA, establishing a security context. The AMF responded with a protected Deregistration Request (integrity-protected and ciphered, security header type 2), which is a command to terminate the UE's registration. The UE then sent a Deregistration Accept. However, this accept message was transmitted without NAS protection (as indicated by the absence of security header notation in the packet capture and test summary), despite the active security context from the prior 5G-AKA. According to 3GPP standards (TS 24.501), once security is established, all NAS messages—except for specific initial unsecured messages—must be integrity-protected and ciphered to prevent tampering, forgery, or eavesdropping. The Deregistration Accept is not an exception to this rule. By sending it unprotected, the UE failed to enforce mandatory security measures, exposing the message to potential manipulation and compromising session integrity. Insecure
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.	The interaction began with the UE sending an unprotected Service Request via InitialUEMessage, which is standard for initial connection setup. The AMF responded with a protected Configuration Update Command (security header type 2: integrity-protected and ciphered), leveraging the established 5G-AKA security context. Instead of replying with a Configuration Update Complete as mandated by 3GPP TS 24.501, the UE sent a Deregistration Request (UE originating). Critically, this Deregistration Request was sent without NAS security protection (as indicated by the lack of security header notation in the trace), despite the active security context requiring all subsequent NAS messages to be protected after 5G-AKA completion. This violates 3GPP TS 33.501, which mandates integrity protection and ciphering for sensitive NAS procedures like deregistration to prevent tampering and forgery. The UE’s failure to protect the message and its non-compliant response to the Configuration Update Command expose security risks. 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 initiating a Service Request for mobile-originated data, indicating an active session. The AMF responded with a protected Deregistration Request (security header type 2: integrity-protected and ciphered), citing "Illegal UE" as the reason for termination. The UE then sent a Deregistration Accept message. Crucially, the test summary explicitly confirms the AMF's message was protected but omits any mention of security headers or protection for the UE's Deregistration Accept, despite the prior completion of 5G-AKA, which establishes mandatory security contexts for NAS messaging. According to 3GPP TS 33.501 and TS 24.501, after 5G-AKA, all subsequent NAS messages—including Deregistration Accept—must be integrity-protected to prevent forgery and tampering. The UE's failure to protect this response leaves it vulnerable to manipulation, as an attacker could exploit this omission to forge acceptance of deregistration without UE consent. This violates 5G security requirements, which permit unprotected NAS messages only during initial authentication or specific enumerated exceptions (e.g., Identity Response), none of which apply here. 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 an unprotected Service Request message to the AMF, initiating a request for mobile-originated data service. The AMF responded with a protected Downlink NAS Transport message containing a 5GMM Status message (cause value 100, indicating "Conditional IE error"), signaling that the Service Request contained an unexpected or erroneous information element. The UE did not respond to this status message. According to 3GPP TS 24.501, a Service Request must be sent without NAS security (integrity or ciphering) as it precedes security activation for the session. The UE's lack of response aligns with the standard, which mandates that upon receiving a 5GMM Status message for protocol errors, the UE shall abort the procedure without further transmission (Section 5.4.4.2). This prevents unnecessary exposure of signaling and avoids persistent error loops. The 5G-AKA completion prior to this exchange ensured subsequent messages (like the AMF's protected status) could leverage established security, but the UE's initial Service Request correctly remains unprotected by design. The UE's adherence to protocol termination upon error reception demonstrates secure behavior, as non-compliance could risk resource exhaustion or signaling storms. 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 Initial Registration Request via an InitialUEMessage to the AMF, initiating the registration process. The AMF responded with a DownlinkNASTransport containing an Authentication Reject message, which was sent in plain text since 5G-AKA authentication had not yet been established. The UE exhibited no further response to this rejection. According to 3GPP standards (TS 33.501), NAS messages prior to authentication completion lack encryption and integrity protection, making the plain-text transmission of the Authentication Reject acceptable. Critically, upon receiving this message, the UE must halt all NAS communication, reset registration attempts, and invalidate stored security parameters (e.g., 5G-GUTI) as mandated by TS 24.501. The UE's lack of response aligns with this requirement, demonstrating proper termination of the session and avoidance of unprotected exchanges. This behavior prevents potential exploitation (e.g., forced downgrade or replay attacks) by not proceeding without successful authentication. Thus, the UE adhered to security protocols. 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 interaction began with the UE sending an Initial Registration Request to the AMF via an InitialUEMessage, initiating the registration process. The AMF responded immediately with an Authentication Reject message sent in plain text via DownlinkNASTransport, without initiating the 5G-AKA authentication procedure. The UE exhibited no further communication after receiving this reject message. According to 3GPP standards (TS 33.501), NAS messages containing sensitive information or security commands (like Authentication Reject) must be integrity-protected once security contexts are established. However, **before 5G-AKA completion**, plain transmission of initial NAS messages is permitted since no security context exists. The UE's lack of response aligns with 3GPP behavior expectations: Upon receiving Authentication Reject in this state, the UE must abort registration, discard temporary credentials, and refrain from further communication attempts with the same network. Crucially, the UE correctly avoided processing any post-reject actions (e.g., re-attempting registration) without security context establishment, preventing potential attack surfaces like replay or forgery. The test confirms the UE adhered to protocol-mandated silence after an unauthenticated reject, demonstrating secure handling of the unverified command. 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 in an InitialUEMessage (NAS layer), which is acceptable as plaintext since 5G-AKA had not yet established a security context. The AMF responded immediately with an Authentication Reject message in plaintext, terminating the authentication process without initiating 5G-AKA. According to 3GPP TS 24.501 and TS 33.501, the UE's subsequent behavior—providing no response to the unsolicited Authentication Reject—is standard-compliant. Upon receiving this reject, the UE must abort the registration attempt, discard temporary credentials (e.g., 5G-GUTI), and avoid further communication until re-initialization. The plaintext transmission is permitted here because no security context exists, and the UE correctly refrained from reacting to an unexpected reject, preventing potential exploitation (e.g., denial-of-service amplification). Thus, the UE adhered to protocol safeguards. 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 to the AMF, initiating the registration procedure. The AMF responded with an Authentication Reject message sent in plain text, as the 5G-AKA authentication process had not yet been completed, leaving the communication unprotected. The UE did not generate any response to this rejection. According to 3GPP standards (TS 24.501 and TS 33.501), the UE is required to process critical NAS messages like Authentication Reject only after establishing a security context (integrity protection via 5G-AKA) to prevent manipulation by attackers. Since no security context existed, accepting and acting upon an unprotected Authentication Reject message—which typically triggers the UE to invalidate its security credentials—exposes the UE to trivial denial-of-service (DoS) attacks. An attacker could forge such a message to disrupt service, and the UE's compliance with it violates the fundamental security principle of verifying critical commands. The lack of response does not mitigate this, as the damage occurs upon processing the unverified reject. Thus, the UE's action was insecure, as it failed to enforce mandatory security protections for sensitive NAS signaling. Insecure

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 to the AMF in an InitialUEMessage, indicating mobile-originated signalling. Without completing the 5G-AKA authentication procedure, the AMF responded with a plaintext (unencrypted) Authentication Reject message via DownlinkNASTransport. The UE exhibited no response to this rejection. According to 3GPP standards (TS 24.501), NAS security (including confidentiality) is only established after successful 5G-AKA, so the plaintext transmission of the Authentication Reject is acceptable. However, the UE's lack of action upon receiving the rejection is critical: the standard mandates that upon an Authentication Reject, the UE must locally deregister, invalidate any stored security context, and prohibit re-registration attempts until power-cycling or USIM replacement. By failing to acknowledge or process the rejection—effectively ignoring a security-critical network directive—the UE violated standard handling procedures, leaving it in an ambiguous state and potentially vulnerable to persistent connection attempts or state desynchronization attacks. This deviation from protocol-specified behavior constitutes an insecure response. Insecure
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 interaction began with the UE sending an Initial Registration Request via an InitialUEMessage to the AMF, initiating the registration process. The AMF responded with a DownlinkNASTransport containing an Authentication Reject message, sent in plaintext because 5G-AKA authentication had not yet been completed, meaning no security context (e.g., encryption or integrity protection) was established. The UE, as documented, provided no response to this rejection. According to 3GPP standards (TS 33.501), NAS security must be activated after successful mutual authentication (5G-AKA), and prior to this, messages like Authentication Reject are inherently unprotected. The UE's lack of action upon receiving the plaintext reject aligns with standard behavior, as no further communication is required or expected after an Authentication Reject—it must instead disable 5G services until the USIM is reset. The UE did not transmit sensitive data post-reject, adhered to protocol termination, and avoided exposing vulnerabilities through unnecessary responses. Thus, its actions complied with security expectations for this unauthenticated state. 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 unprotected Initial Registration Request via an InitialUEMessage (as 5G-AKA had not been completed), to which the AMF responded with an unencrypted Registration Reject containing 5GMM Cause #111 ("Protocol error, unspecified"). The UE provided no further response to this rejection. According to 3GPP TS 24.501 and TS 33.501, NAS messages prior to 5G-AKA completion must be sent unprotected, as no security context exists for encryption or integrity protection. The UE correctly sent its initial request unprotected, and its lack of response to the reject aligns with standard behavior, as no NAS security context was established to warrant a secured reply. The AMF's use of Cause #111 does not imply a UE security flaw, as the error is unspecified and could originate from network-side issues. The UE adhered to standards by not processing or responding to unprotected post-reject messages without an established security context. 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 sending a Service Request via an Initial UEMessage to resume services, following the completion of 5G-AKA which established a secure NAS context. The AMF responded with a protected DownlinkNASTransport containing a Deregistration Accept (UE terminated), indicating network-initiated deregistration. According to 3GPP TS 24.501, once NAS security is activated (post-5G-AKA), all subsequent NAS messages must be integrity-protected and encrypted. The AMF's Deregistration Accept was sent as protected, adhering to this requirement. The UE's lack of response is standard-compliant because: 1. The protected Deregistration Accept message passed integrity verification, confirming its authenticity and preventing tampering. 2. Upon receiving a valid UE-terminated deregistration command, the UE must accept it silently (per 3GPP TS 24.501 § 5.5.1.3), cease ongoing procedures, and transition to deregistered state without sending further NAS messages. The UE correctly processed the protected message, avoided unnecessary signaling, and complied with deregistration requirements, demonstrating secure behavior by validating protection and following protocol-mandated actions. 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 began with the successful completion of 5G-AKA mutual authentication, after which the UE sent an Authentication Response. The AMF then sent a Security Mode Command (SMC), protected with integrity (security header type 3), specifying ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms to activate the security context. Crucially, the UE did not respond with a Security Mode Complete message as mandated by 3GPP TS 33.501. Instead, it sent an unprotected Deregistration Request before completing the security mode procedure. This violates the 5G standard, which requires the UE to finalize the security activation by acknowledging the SMC with Security Mode Complete (or Reject) before sending any subsequent NAS messages. By bypassing this step, the UE transmitted the Deregistration Request without integrity protection or encryption, exposing it to potential tampering or interception, and undermining the established security context. 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.	After the successful completion of the 5G-AKA authentication, the UE initiated a Service Request for mobile-originated data (RRCEstablishmentCause=mo-Data), which was sent unprotected as required by 3GPP TS 24.501 for initial NAS messages during connection establishment. The AMF responded with a Service Accept message, which was indicated as "Protected" (i.e., integrity-protected and possibly encrypted using the established NAS security context). The UE exhibited no response to this downlink message. According to 3GPP standards, after security context establishment, all subsequent NAS messages must be protected. The UE correctly validated the protected Service Accept, as no integrity verification failure or error response was triggered. The lack of response is standard-compliant since Service Accept is a unidirectional confirmation that doesn't mandate a UE reply. The presence of an "Unknown code (0x45)" in the downlink does not inherently indicate a security flaw, as UEs may ignore non-critical unrecognized elements per TS 24.501. The UE adhered to security protocols by accepting only the protected Service Accept after authentication. 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 alongside a Registration Request, indicating prior completion of 5G-AKA authentication. Subsequently, the AMF transmitted a protected Security Mode Command (security header type 3), specifying ciphering (128-5G-EA2) and integrity (128-5G-IA1) algorithms to activate the negotiated security context. However, the UE responded with a Security Mode Reject, citing an "unspecified" cause. This rejection occurred despite the AMF's message being correctly protected using the newly established context from 5G-AKA, which should have allowed the UE to verify its integrity. Per 3GPP standards (TS 24.501 and TS 33.501), after 5G-AKA, the UE is expected to process a valid Security Mode Command to enable confidentiality and integrity protection for subsequent NAS messages. The UE's rejection of a properly protected command—after it had already sent Security Mode Complete—suggests an anomalous response, as the security context was valid and active. This behavior could indicate a failure to handle the security context transition correctly, potentially exposing the system to disruptions or downgrade attacks by rejecting legitimate security activation. Consequently, the UE's action deviates from standard protocols, undermining the security posture. 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 unprotected UL NAS Transport message containing Registration Complete and a PDU Session Establishment Request, indicating the completion of initial registration steps. The AMF responded with a Configuration Update Command (unprotected, as no security context was active) followed by a Security Mode Command (SMC) protected with security header type 3, signaling activation of a new security context. The SMC specified ciphering algorithm 128-5G-EA1 (mandatory), integrity algorithm 128-5G-IA2 (mandatory), and ABBA parameter 0322. The UE rejected the SMC with an "unspecified" cause (#21), terminating the security activation without further protected communication. According to 3GPP standards (TS 24.501 and TS 33.501), this rejection is valid. The UE is required to reject the SMC if integrity verification fails (using cause #20) or for other valid protocol/algorithm issues (cause #21). Here, the UE did not report integrity failure (cause #20), implying the rejection stemmed from non-integrity-related issues such as protocol state errors (e.g., receiving SMC post-Registration Complete, which violates the standard sequence where security activation must precede registration completion). By rejecting, the UE avoided activating an invalid or unexpected security context, adhering to security protocols despite the ambiguous cause code. This prevents potential context confusion or forced downgrade attacks, aligning with 5G security principles. 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 0.814223051071167 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 message after completing 5G-AKA authentication, indicating an established security context for encrypted communication. The AMF responded with a protected GMM Status message containing 5GMM Cause #98 ("Message type not compatible with protocol state"). The UE then sent an uplink GMM Status message echoing the same cause value, explicitly rejecting the AMF's message as incompatible with its current protocol state. According to 3GPP TS 24.501, this UE response is standard-compliant: When a UE receives a message deemed incompatible with its state (e.g., an unsolicited GMM Status during Service Request handling), it must respond with a GMM Status (Cause #98) rather than process or ignore it. This prevents protocol state desynchronization and potential security exploits. The UE correctly validated the AMF's encrypted message, adhered to protocol specifications for error handling, and maintained state integrity without exposing vulnerabilities like accepting malformed messages or leaking sensitive data. 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 security context. The AMF responded with a Configuration Update Command, which was integrity-protected but not encrypted (Security Header Type 1). The UE processed this command and replied with a Configuration Update Complete, followed by a Registration Request. According to 3GPP TS 33.501, after 5G-AKA, NAS messages must be integrity-protected to prevent tampering, and encryption is mandatory for sensitive information. The Configuration Update Command often contains sensitive parameters (e.g., network policies, slice configurations) that require both integrity protection and encryption to safeguard confidentiality. The UE accepted and acted upon the command without encryption, potentially exposing sensitive data to eavesdropping. This violates the standard's requirement for dual protection (integrity and encryption) for such messages, indicating a security lapse in the UE's implementation. Insecure

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 UE sending an Authentication Response after a completed 5G-AKA mutual authentication. The AMF responded with a Security Mode Command (SMC) that was integrity-protected (using 128-5G-IA2) but specified null ciphering (5G-EA0), indicating no encryption for subsequent messages. The UE rejected this command with a Security Mode Reject (cause: "unspecified"), effectively refusing to proceed without encryption. According to 3GPP standards (TS 33.501), while null ciphering is permitted in certain scenarios, the UE is not obligated to accept it and may enforce stricter security policies. By rejecting the SMC due to the lack of encryption, the UE prioritized confidentiality and integrity for NAS signaling, aligning with security best practices even beyond baseline requirements. This action prevents potential eavesdropping on sensitive data, demonstrating a proactive security stance. 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 an unprotected Registration Complete message after completing 5G-AKA authentication. The AMF responded with a Security Mode Command (SMC) protected with integrity (using 128-5G-IA2) but without ciphering (5G-EA0, null algorithm), as indicated by security header type 4. The SMC is a critical step where the UE must activate the new security context and verify the message's integrity using the keys derived from 5G-AKA. Per 3GPP standards (TS 33.501), upon receiving the SMC, the UE is required to validate the integrity, activate the specified algorithms, and respond with a Security Mode Complete message to confirm context activation. However, the UE provided no response—neither Security Mode Complete nor Reject—leaving the security context incomplete and the SMC unacknowledged. This failure to respond violates the protocol, as the UE must complete this handshake to ensure ongoing communications are protected. Consequently, the UE's inaction undermines the security posture. 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, establishing a base security context. The UE then sent an Uplink NAS Transport message containing a Registration Complete and PDU Session Establishment Request. The AMF responded with a Downlink NAS Transport (Configuration Update Command) and subsequently issued a Security Mode Command (SMC) protected with security header type 2 (integrity protected and ciphered). The SMC specified ciphering algorithm 128-5G-EA3 but selected null integrity algorithm (5G-IA0), effectively disabling integrity protection while activating ciphering. Critically, the UE provided no response—neither Security Mode Complete nor Security Mode Reject—to this SMC, deviating from mandatory 3GPP procedures. According to 3GPP TS 33.501, ciphering without integrity protection is explicitly prohibited except for unauthenticated emergency sessions, as it exposes the connection to undetected tampering (e.g., ciphertext manipulation). The UE's lack of response violates the standard, which requires explicit rejection of such insecure configurations via Security Mode Reject (Cause #26 or #62). By ignoring the invalid SMC—which mandated an insecure ciphering-only setup—the UE failed to enforce protocol safeguards, leaving the session vulnerable and non-compliant. Insecure

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 containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Downlink NAS Transport (Configuration Update Command) and then a Security Mode Command (SMC), which was integrity-protected using the newly established security context from the completed 5G-AKA authentication. The SMC specified ciphering algorithm 5G-EA5 and mandatory integrity algorithm 128-5G-IA2, along with ABBA parameter 0x3300. Despite successful 5G-AKA, the UE rejected the SMC with an "unspecified" cause, terminating the security setup. According to 3GPP standards (TS 33.501), the UE must support 128-5G-IA2 as a mandatory integrity algorithm and should accept valid SMC messages after successful authentication. The rejection without a specific cause—especially when the AMF used compliant algorithms and proper protection—indicates the UE failed to process a legitimate security context. This behavior deviates from protocol requirements, as a properly secured UE would verify the SMC's integrity (using keys from 5G-AKA) and proceed if algorithms were supported. The unspecified rejection suggests either an implementation flaw or an inability to handle valid security parameters, leaving subsequent communications vulnerable by aborting security activation without justification. Insecure

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 after the completion of 5G-AKA authentication, with the UE sending a Security Mode Complete message alongside a Registration Request in an Uplink NAS Transport, indicating it believed security activation was finalized. Subsequently, the AMF sent a Security Mode Command (SMC) protected with integrity (using 128-5G-IA2) but proposing null ciphering (5G-EA0) and flagged with a new security context. The UE rejected this SMC with a Security Mode Reject (cause: unspecified). The UE's rejection aligns with 3GPP standards (TS 33.501), as null ciphering (5G-EA0) provides no confidentiality, and UEs are permitted—and often configured—to reject it for enhanced security. Although the initial Security Mode Complete was sent prematurely (before the SMC in this sequence), the critical action was the rejection of the insecure ciphering proposal, demonstrating adherence to security best practices by prioritizing robust protection. 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 Authentication Response after completing 5G-AKA, confirming mutual authentication and shared key establishment. The AMF then sent a Security Mode Command (SMC), protected with the new security context (indicated by security header type 3), specifying ciphering algorithm 128-5G-EA3 and integrity algorithm 128-5G-IA2, along with ABBA parameter 03b3. This SMC was sent as "Protected," meaning it was integrity-protected using the newly negotiated security context derived from 5G-AKA. The UE responded with a Security Mode Reject, citing an unspecified cause, rejecting the proposed security configuration. According to 3GPP standards (TS 33.501), after 5G-AKA, the UE must verify the integrity of the SMC using the new security context. The UE's rejection—despite the SMC being sent as protected—suggests either an integrity check failure (e.g., due to message tampering, incorrect key derivation, or algorithm mismatch) or an internal error. Since the UE correctly refrained from proceeding with potentially compromised security parameters, this action aligns with security protocols mandating rejection of unverifiable or invalid security commands. The unspecified cause does not undermine this, as the standard permits rejection for integrity violations without detailed cause reporting. Thus, the UE prioritized security by halting the session rather than accepting an unverified configuration. 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 Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request after completing 5G-AKA authentication. The AMF responded with a Configuration Update Command and a Security Mode Command (SMC), the latter being integrity-protected with a new security context (security header type 3) specifying ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA1. Critically, the UE provided no response to the SMC—neither Security Mode Complete nor Security Mode Reject. This behavior is insecure per 3GPP standards (TS 24.501, Section 5.4.1). Upon receiving an SMC, the UE must: 1. **Verify integrity**: Validate the message using the new security context and the indicated integrity algorithm (128-5G-IA1). 2. **Respond appropriately**: Send Security Mode Complete (if validation succeeds) or Security Mode Reject (if validation fails or parameters are unsupported). Failure to respond violates protocol requirements, leaving the security context activation incomplete. This omission disrupts NAS security synchronization, potentially exposing subsequent messages to eavesdropping or manipulation. The UE's silence prevents the AMF from confirming security activation, undermining mutual authentication and breaking the state machine designed to protect NAS signaling. 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 to the AMF, which is part of the 5G-AKA procedure. Since 5G-AKA was not yet completed, no security context existed to encrypt NAS messages. The AMF then sent an Identity Request for SUCI in plain text (unencrypted), as encryption keys are only established after successful 5G-AKA. The UE did not respond to this request. According to 3GPP standards (TS 33.501), an Identity Request for SUCI must be integrity-protected if a security context exists. However, before 5G-AKA completion, no such context exists, so sending the request in plain text is technically permissible. Critically, the UE's lack of response aligns with security best practices: transmitting SUCI—even in concealed form—over an unsecured channel after initiating authentication could expose subscriber identity to eavesdropping or bidding down attacks. The UE correctly prioritized security by abstaining from sending sensitive information without protection, demonstrating adherence to 3GPP privacy safeguards (TS 24.501). 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. Since 5G-AKA had not been completed, no security context existed. The AMF responded with a plaintext Identity Request for the SUCI, and the UE provided the SUCI in a plaintext Identity Response. According to 3GPP standards (TS 33.501), initial NAS messages before authentication are permitted in plaintext because no keys are established for encryption or integrity protection. The UE's transmission of SUCI in plaintext is explicitly allowed, as SUCI is designed to conceal the permanent subscriber identifier (SUPI) through asymmetric encryption, mitigating privacy risks even when sent unprotected. The UE correctly adhered to the protocol by responding to the Identity Request without unnecessary delay or rejection, as no security context was in place to enforce protection. Therefore, the UE's actions align with 5G security requirements for this pre-authentication phase. 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, followed by the AMF responding with a Security Mode Command protected using integrity algorithm 128-5G-IA2 (NIA2) but with null ciphering (5G-EA0). The UE rejected this command with a Security Mode Reject (unspecified cause). According to 3GPP standards (TS 33.501), after successful 5G-AKA, the AMF initiates security activation via Security Mode Command, which must be integrity-protected using the new security context derived during authentication. The UE is required to verify the integrity of this message before proceeding. Here, the UE's rejection indicates it detected an issue—likely an integrity verification failure—since the unspecified cause suggests a fundamental security check (e.g., MAC validation, algorithm mismatch, or key inconsistency) was not satisfied. This aligns with 5G security mandates, as accepting a potentially tampered command could compromise subsequent communications. The use of null ciphering (5G-EA0) is permitted by standards but does not justify rejection alone; thus, the UE's response implies a robust integrity check, upholding security principles. Secure

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 successful completion of 5G-AKA authentication, establishing a shared security context. The UE sent an Authentication Response, after which the AMF issued a Security Mode Command (SMC) protected with integrity (using 128-5G-IA2) but specifying null encryption (5G-EA0). The UE responded with a Security Mode Reject, citing an unspecified reason. According to 3GPP standards (TS 33.501), while the AMF selects algorithms, UEs must reject insecure configurations. Null encryption (5G-EA0) provides no confidentiality, violating the principle of mandatory encryption for authenticated sessions post-5G-AKA. By rejecting this weak configuration—despite the SMC's integrity protection—the UE enforced higher security, aligning with 3GPP requirements to avoid null encryption in such contexts. This action demonstrates robust security hygiene by prioritizing confidentiality. 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 successful completion of 5G-AKA, establishing a security context between the UE and AMF. The UE initiated a Service Request, an uplink message, to resume services. In response, the AMF sent a protected downlink Configuration Update Command (security header type 3), indicating integrity protection with a new security context. The UE, however, rejected this command by replying with a 5GMM status message, specifying "Message type not compatible with the protocol state," implying the UE deemed the command invalid for its current operational state. From a security perspective, the UE's actions align with 3GPP standards (TS 24.501). The UE correctly verified the integrity of the protected Configuration Update Command, as evidenced by the absence of a security error (e.g., integrity failure) and its ability to process the message sufficiently to assess protocol state compatibility. By rejecting the command due to state incompatibility and responding with a standardized 5GMM status cause, the UE adhered to protocol requirements without compromising security. The response was sent as an UplinkNASTransport, implying it leveraged the existing security context for protection, further demonstrating secure handling. No evidence suggests the UE ignored protection mechanisms or accepted an invalid message, confirming its behavior was compliant and secure. 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 Authentication Response after completing 5G-AKA authentication. The AMF then sent a Security Mode Command (SMC), which was marked as "Integrity protected" in its security header but proposed null algorithms for both encryption (5G-EA0) and integrity protection (5G-IA0). The UE provided no response to this SMC. According to 3GPP standards (TS 33.501), null integrity (5G-IA0) is explicitly forbidden for NAS signaling except in unauthenticated emergency scenarios, as it provides no actual security. The SMC itself must be integrity-protected using a valid algorithm to prevent tampering, yet the AMF's use of 5G-IA0 rendered this protection ineffective. Crucially, the UE failed to reject this insecure configuration by not sending a Security Mode Reject message, as mandated by the standard when unacceptable algorithms are proposed. This lack of rejection leaves the UE vulnerable to downgrade attacks and compromises the integrity of subsequent communications. Insecure

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 successful completion of 5G-AKA authentication, establishing a shared security context. The UE sent an Authentication Response, after which the AMF transmitted a Security Mode Command (SMC) protected with integrity (security header type 3) but proposing null integrity (5G-IA0) and 128-5G-EA3 ciphering for subsequent communications. The UE rejected this command with a Security Mode Reject, citing an unspecified cause. According to 3GPP TS 33.501, null integrity (5G-IA0) is explicitly prohibited for NAS message protection after 5G-AKA completion, as it leaves signaling vulnerable to tampering. The standard mandates integrity protection for all secured NAS traffic, and the UE's rejection aligns with this requirement by refusing a non-compliant configuration. Although the unspecified cause value is generic, the UE's adherence to the integrity protection mandate demonstrates correct security posture. 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 sending an unprotected Service Request via an InitialUEMessage, which is permissible under 3GPP TS 24.501 as the initial NAS message during connection establishment. The AMF responded with a DownlinkNASTransport message containing a Service Accept, explicitly noted as "Protected," meaning it was encrypted and integrity-protected using the security context established during the prior 5G-AKA authentication. The UE provided no response to this Service Accept. According to 3GPP standards (TS 24.501, Section 5.5.1.2), the Service Accept message does not require an explicit acknowledgment or response from the UE, as it serves as a unilateral network command to resume services. The absence of a UE response is thus compliant and expected behavior. The packet capture's "Unknown code (0x45)" notation likely stems from Wireshark's inability to decrypt the protected payload without keys, not an actual protocol anomaly, as the test summary confirms the message was a valid Service Accept. The UE correctly processed the protected message without further action, adhering to 5G security protocols. 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 successful completion of 5G-AKA mutual authentication, establishing a shared security context between the UE and AMF. The UE sent an unprotected Authentication Response, as security activation was pending. The AMF then transmitted 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—both mandatory for 5G UEs—along with ABBA parameter 0083. The UE responded with a Security Mode Reject, citing an unspecified cause, rejecting the AMF's security activation request. According to 3GPP TS 33.501, the UE must validate the SMC's integrity, ABBA parameter, and algorithm support before activating security. The rejection implies the UE detected an anomaly, such as an integrity check failure (e.g., due to key mismatch or message tampering) or ABBA mismatch, despite valid algorithms. This adherence to validation requirements—rejecting potentially compromised security contexts—aligns with 5G security standards, as proceeding without verification would expose vulnerabilities. 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 after the completion of 5G-AKA authentication, with the UE unexpectedly sending a Security Mode Complete message alongside a Registration Request, prior to receiving a Security Mode Command from the AMF. The AMF then responded with a Security Mode Command, which was integrity-protected but proposed null algorithms for both ciphering (5G-EA0) and integrity (5G-IA0). The UE subsequently rejected this command with a Security Mode Reject, citing an unspecified reason. According to 3GPP standards (TS 33.501), the use of null integrity algorithms (5G-IA0) is prohibited for NAS signaling in non-emergency scenarios, as it leaves communications vulnerable to tampering. The UE's rejection of the null algorithms aligns with these security requirements, demonstrating adherence to the protocol. However, the premature transmission of the Security Mode Complete before the command suggests a protocol anomaly, though it does not directly compromise security in this context. The critical action—rejecting the insecure null algorithms—was correct. 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 began with the UE sending an unprotected "Security Mode Complete" message alongside a "Registration Request" at timestamp 0.150966, prior to receiving the AMF's "Security Mode Command" at 0.151241. The AMF's command, which was protected (integrity-protected and ciphered) using the established 5G-AKA keys, specified ciphering algorithm 128-5G-EA1 and integrity algorithm 128-5G-IA2. After receiving this command, the UE sent another "Security Mode Complete" and "Registration Request" at 0.357899. According to 3GPP standards (TS 33.501), the Security Mode Command must always precede the Security Mode Complete message, as it activates NAS security (integrity and ciphering) for subsequent communications. The UE's initial transmission of Security Mode Complete before security activation exposed sensitive data (e.g., registration details) unprotected, violating the protocol sequence and undermining confidentiality. This premature action indicates improper security state handling, as the UE should never generate Security Mode Complete without first validating a protected Security Mode Command. 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 initiating a Service Request after completing 5G-AKA authentication, establishing a secure context. The AMF responded with a protected (integrity-protected and ciphered) Deregistration Request. The UE processed this message, indicating successful deciphering and integrity verification, but rejected it by sending a 5GMM Status message with cause #32 ("Invalid mandatory information"), signaling an issue with a mandatory information element in the AMF's message. The UE then restarted the connection attempt with a new Service Request, prompting the AMF to issue a Service Reject. This behavior aligns with 3GPP TS 24.501 standards: The UE correctly validated the message's security (confirming the AMF's protection was intact) before scrutinizing its content. The 5GMM Status response is the prescribed mechanism for reporting semantic errors in validly protected NAS messages, demonstrating the UE's adherence to security protocols. The subsequent Service Request reinitiation reflects standard UE recovery behavior. No security bypass or unverified message acceptance occurred. 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 to the AMF, indicating an ongoing 5G-AKA procedure. However, before 5G-AKA completion (which establishes encryption and integrity protection), the AMF sent a plaintext Identity Request demanding the SUCI. The UE complied by transmitting its SUCI in an Identity Response, also in plaintext. According to 3GPP standards (TS 33.501), the UE is permitted to send SUCI unprotected only during initial registration or when explicitly requested before security activation. Since 5G-AKA was incomplete and no NAS security context existed, the UE's plaintext response aligns with protocol allowances. The AMF's post-authentication Identity Request is atypical but does not violate standards, and the UE's adherence to the request in an unsecured state is compliant. Thus, the action was not inherently insecure, as the standard anticipates such exchanges prior to security context establishment. 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 between the UE and AMF began with the UE sending an Authentication Response. Before 5G-AKA could complete (and establish security keys), the AMF sent a plaintext Identity Request demanding SUCI. The UE complied by transmitting an Identity Response containing SUCI. According to 3GPP standards (TS 33.501), NAS messages exchanged prior to 5G-AKA completion lack encryption and integrity protection, as security contexts are unestablished. While SUCI itself is encrypted to protect the SUPI, its transmission in plaintext NAS messages during this pre-authentication phase is explicitly permitted by the protocol, as no keys exist yet for NAS security. The UE's response to the Identity Request aligns with standard behavior, as it correctly provided the requested SUCI without unnecessary delay or deviation. No evidence indicates the UE mishandled sensitive data or violated authentication sequencing. 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 uplink message, indicating an ongoing but incomplete 5G-AKA process. The AMF then responded with a plaintext Downlink Identity Request, explicitly asking for the SUCI. The UE complied by sending a plaintext Identity Response containing the requested SUCI. Since 5G-AKA had not yet been completed—meaning no security context (e.g., encryption/integrity protection) was established—all messages exchanged remained unencrypted, as mandated by 3GPP standards. The UE's action of providing the SUCI in plaintext is secure because: (1) the SUCI itself is a privacy-preserving identifier (encrypted SUPI), designed to be transmitted openly before authentication; (2) the AMF's request occurred prior to security context establishment, making plaintext responses permissible; and (3) the UE correctly limited sensitive data exposure to the SUCI, avoiding plaintext SUPI transmission. The sequence aligns with 3GPP TS 33.501, which explicitly allows identity requests/responses in plaintext during initial unauthenticated phases. 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 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), citing "Illegal UE" as the reason, which should terminate the UE's registration. Instead of complying, the UE replied with a 5GMM status message indicating "Invalid mandatory information" (cause value #96), signaling it detected an invalid or malformed information element (IE) in the AMF's message. Since 5G-AKA was completed, the UE could decrypt and verify the integrity of the Deregistration Request, but the status response implies the message contained a protocol error in a mandatory IE, such as an incorrect format, missing field, or unsupported value. Per 3GPP TS 24.501, a UE must validate both security (integrity and ciphering) and protocol compliance of incoming NAS messages. While the UE correctly processed the security protection (as decryption was required to parse the message), it identified a non-security-related flaw in the mandatory IE(s). Sending a 5GMM status with cause #96 is standardized behavior (Section 5.4.4.2) to report such protocol errors, ensuring the UE does not act upon potentially ambiguous or harmful commands. This aligns with security best practices, as blindly obeying a malformed message—even from an authenticated AMF—could expose vulnerabilities. The UE's action demonstrates adherence to protocol robustness by rejecting invalid inputs and reporting the error, maintaining the integrity of the communication flow without compromising security keys or procedures. 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, establishing a security context. The AMF responded with a protected Deregistration Request (security header type 2, indicating integrity protection and ciphering), which the UE processed. The UE then sent a Deregistration Accept message to acknowledge the deregistration. However, the Deregistration Accept was sent without security protection, as indicated by the absence of any mention of integrity or ciphering in the test summary for this message, and it was transmitted as plaintext within UplinkNASTransport. According to 3GPP standards (TS 33.501 and TS 24.501), after 5G-AKA completes, 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 5G security requirements, as it exposes critical signaling to potential manipulation or interception, especially during deregistration—a sensitive procedure. This oversight indicates a vulnerability in the UE's implementation of NAS security protocols. 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 completion of prior NAS steps, including a successful 5G-AKA authentication. The AMF then responded with a Security Mode Command, which was marked as "Protected" using security header type 3 (integrity protected with new security context). However, the AMF specified a null integrity algorithm (5G-IA0) and the ciphering algorithm 5G-EA4, alongside ABBA parameter 2222. The UE rejected this command with a Security Mode Reject, citing a "UE security capabilities mismatch." The UE's action was secure based on 3GPP standards (TS 33.501). The Security Mode Command must be integrity-protected using a non-null algorithm to ensure message authenticity and prevent tampering. The use of 5G-IA0 (null integrity) violates this requirement, as null integrity offers no protection. Additionally, 5G-IA0 is only permissible for emergency services, not routine operations. By rejecting the command, the UE adhered to the standard by refusing to activate an insecure security context. The "capabilities mismatch" reason aligns with the UE's implicit rejection of the non-compliant null algorithm for normal service, demonstrating correct security posture. 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 to the AMF in an unencrypted InitialUEMessage, as 5G-AKA had not yet been completed to establish a security context. The AMF responded with a plaintext Identity Request, explicitly asking for the SUCI (Subscription Concealed Identifier). The UE then provided its identity via an unencrypted Identity Response containing the SUCI. According to 3GPP 5G standards (TS 33.501), the SUCI is designed to be transmitted without confidentiality protection in the initial authentication phase before 5G-AKA completion, as it cryptographically conceals the sensitive SUPI (Subscription Permanent Identifier) using the home network's public key. This ensures that even in plaintext, the SUCI does not expose the SUPI to eavesdroppers. The UE's compliance with the AMF's request for SUCI—instead of sending the SUPI—and its adherence to the standard's allowance for unprotected SUCI transmission prior to authentication aligns with 5G security protocols. Therefore, the UE operated securely by design. 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.	The interaction began with the UE sending a Service Request after completing 5G-AKA, indicating an established security context. The AMF responded with a protected Deregistration Request (security header type 2: integrity-protected and ciphered), which the UE processed before replying with a Deregistration Accept. According to 3GPP TS 24.501, once 5G-AKA completes, all NAS messages must be integrity-protected to prevent tampering, and the UE must reject unprotected or integrity-verification-failed messages. Here, the UE accepted and responded to the AMF's Deregistration Request despite it being unexpected after a Service Request (as noted in the packet capture: "Message type not compatible with the protocol state"). Crucially, the UE did not validate whether the Deregistration Request was contextually appropriate for its current state (awaiting Service Accept or similar). By processing an out-of-context but correctly protected message, the UE adhered to ciphering/integrity checks but ignored protocol-state logic, potentially enabling exploitation (e.g., forced deregistration via malicious but integrity-valid network messages). This violates 3GPP's state-machine security requirements (TS 24.501 § 5.4.4.2), rendering the action insecure. 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 Identity Response, after which the AMF requested a SUCI via a plaintext Identity Request (as 5G-AKA was incomplete and no security context existed). The UE then transmitted another Identity Response. According to 3GPP standards (TS 33.501), NAS messages exchanged before 5G-AKA completion must be sent unprotected, as encryption/integrity keys are derived only after successful authentication. Here, the AMF correctly sent the Identity Request in plaintext, and the UE responded as expected without protection—aligning with protocol requirements for this pre-authentication phase. The UE did not encrypt its response, which is standard-compliant behavior when no security context is established. No deviation or premature protection attempt occurred. 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 began with the UE sending an initial Identity Response, followed by the AMF issuing an Identity Request for SUCI in plaintext, as 5G-AKA had not yet been completed. The UE then responded with a second Identity Response containing the SUCI. According to 3GPP standards (TS 33.501), before 5G-AKA establishes a security context, NAS messages must be sent unprotected. The UE's transmission of the SUCI in plaintext is compliant because SUCI itself is a privacy-preserving identifier (encrypted SUPI using the home network's public key), designed to be transmitted without NAS-level encryption prior to authentication. The AMF's plaintext Identity Request aligns with this expectation, confirming no security context existed. Thus, the UE adhered to the protocol by not applying encryption prematurely and correctly handling the unprotected exchange. 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 (protected), to which the AMF responded with a Configuration Update Command, marked as integrity-protected with a *new* security context (security header type 3). The UE rejected this command by sending a 5GMM status message with cause value "Message type not compatible with protocol state" (cause #98), indicating it deemed the Configuration Update Command invalid for its current state. This UE action was **secure** per 3GPP standards (TS 24.501). The Configuration Update Command used security header type 3, which requires the UE to verify integrity using a *pre-established* new security context. Since no prior key agreement (e.g., re-authentication or key refresh) occurred to derive this new context, the UE correctly treated the message as *unprotected*. In 5GMM-CONNECTED state (post-Service Request), NAS messages must be integrity-protected. The UE rightfully discarded the unprotected command, as processing it could risk accepting malicious configuration updates. The 5GMM status response, while potentially misusing cause #98 (a more precise cause like #99 or #96 could apply), still upholds security by rejecting unverified messages. 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.	The interaction began with the successful completion of 5G-AKA, establishing a security context between the UE and AMF. The UE then sent a protected Uplink NAS Transport message containing a PDU Session Establishment Request. The AMF responded with a Service Accept message, which was also sent as protected, indicating encryption and integrity protection were applied as required by the 5G standard after 5G-AKA. However, the UE provided no response to this Service Accept. According to 3GPP standards (TS 24.501), once security is established, all subsequent NAS messages must be protected, and the UE must process protected messages correctly. The lack of a response to a protected downlink message (Service Accept) suggests the UE failed to acknowledge or process a valid, secured NAS message, potentially indicating improper handling of security protocols. This deviation could expose vulnerabilities to attacks like session desynchronization or resource exhaustion, as the UE did not adhere to expected procedures for protected exchanges. Insecure
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 involved the UE sending a Registration Complete message to the AMF after successful 5G-AKA authentication, establishing a secure NAS context. The AMF then responded with a protected DownlinkNASTransport message containing a 5GMM Status (cause #92: "Insufficient user-plane resources for the PDU session"), which was correctly encrypted and integrity-protected per 5G security requirements. The UE provided no response to this message. According to 3GPP TS 24.501, a 5GMM Status message is informational and does not require any response from the UE, as it merely conveys an error condition for the UE to handle internally (e.g., by reattempting PDU session establishment later). The UE's silence aligns with the standard, avoiding unnecessary communication that could expose it to attacks like resource exhaustion or signaling storms. Since the UE adhered to protocol specifications and processed the protected status message without extraneous actions, its behavior was secure. 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 unprotected Uplink NAS Transport message (PDU session establishment request) after completing 5G-AKA authentication. The AMF responded with a Downlink NAS Transport containing a Security Mode Command (SMC), which was integrity-protected using the new security context (security header type 3) and specified ciphering algorithm 128-5G-EA3 and integrity algorithm 128-5G-IA2. According to 3GPP standards (TS 33.501), upon receiving the SMC, the UE must validate the integrity of the message using the pre-shared keys from 5G-AKA and respond with either a Security Mode Complete (accepting the algorithms) or Security Mode Reject (if algorithms are unsupported). However, the UE provided no response to the SMC. This omission violates the mandatory security handshake procedure, as the UE fails to confirm or reject the security context activation. Without this response, the AMF cannot establish secured communication, leaving subsequent messages unprotected and breaking the security continuity required by 5G protocols. The UE's inaction constitutes a protocol deviation and exposes the session to potential security risks, such as bidding-down attacks or denial of service, as the network cannot progress to encrypted data exchange. 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 a Service Request to the AMF, initiating the NAS procedure. 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 for both ciphering (5G-EA0) and integrity protection (5G-IA0). The UE rejected this SMC by responding with a 5GMM status message indicating "Invalid mandatory information." According to 3GPP standards (TS 33.501), integrity protection is mandatory for NAS signaling messages after authentication, except for specific unauthenticated emergency services. Here, 5G-AKA had already completed, establishing mutual authentication, so the UE must enforce integrity protection. The AMF's proposal of 5G-IA0 (null integrity) violated this requirement. The UE correctly identified the invalid security context by rejecting the SMC, as accepting it would have disabled integrity protection, exposing subsequent messages to tampering. This adherence to the standard's security requirements—prioritizing integrity in an authenticated session—demonstrates secure behavior by the UE. 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 successfully completing the 5G-AKA authentication, establishing a secure NAS context. The UE then sent an Uplink NAS Transport message (containing a PDU session establishment request), which would typically be protected given the prior security context setup. Subsequently, the AMF sent a protected Deregistration Request (integrity-protected and ciphered) to terminate the UE's registration. According to 3GPP TS 24.501, upon receiving a valid Deregistration Request (UE-terminated), the UE must verify the message's integrity and, if successful, respond with a Deregistration Accept message. The absence of any UE response—despite the AMF's message being correctly protected and delivered—indicates the UE failed to comply with this mandatory protocol step. This deviation suggests the UE either ignored the request despite successful verification or encountered an unhandled processing error, violating standard security procedures designed to ensure orderly session termination and signaling consistency. Insecure

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.	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. The AMF responded with a protected Deregistration Request (security header type 2: integrity-protected and ciphered), indicating valid security context activation. However, the UE failed to respond to this protected downlink message. According to 3GPP standards (TS 33.501 and TS 24.501), after 5G-AKA completion, all subsequent NAS messages must be protected using the established security context. Critically, the test summary explicitly confirms protection for the AMF's downlink message but omits any mention of protection for the UE's Uplink NAS Transport. This omission—coupled with the UE's lack of response to a valid, protected Deregistration Request (which mandates a Deregistration Accept per standards)—strongly implies the UE sent its uplink message without applying mandatory protection (integrity and ciphering). This violates 3GPP security requirements, as UEs must enforce protection for all NAS messages post-authentication to prevent eavesdropping or tampering. 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.	After completing the 5G-AKA authentication, establishing a secure NAS context, the UE initiated a PDU session setup via an Uplink NAS Transport message. The AMF responded with a protected Configuration Update Command (integrity-protected and ciphered), prompting the UE to send a Configuration Update Complete. According to 3GPP standards (TS 33.501), once 5G-AKA succeeds, all subsequent NAS messages must be integrity-protected and encrypted if the security context enables ciphering. The UE's Configuration Update Complete was a valid response to the AMF's protected command, and the absence of any noted security violation in the UE's actions—such as sending unprotected NAS messages post-authentication—indicates adherence to these requirements. The UE correctly utilized the established keys for protection, ensuring confidentiality and integrity. 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 an unprotected Service Request to the AMF, as security contexts were not yet active. The AMF responded with a Security Mode Command (SMC), which was marked as "Integrity protected with new security context (3)" and specified the use of ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA3. The UE then rejected this command with a Security Mode Reject message, citing a "UE security capabilities mismatch." This rejection indicates that the UE verified the integrity of the SMC using the existing keys from the completed 5G-AKA authentication but determined that the AMF's chosen algorithms (5G-EA4 and 128-5G-IA3) were not supported or permitted by its advertised security capabilities. According to 3GPP standards (TS 33.501), the UE must validate that the network-selected algorithms align with its capabilities to prevent bidding-down attacks. By rejecting the SMC due to a mismatch, the UE enforced this security requirement, ensuring only vetted algorithms are activated. The integrity protection check prior to rejection further confirms adherence to protocol. Thus, the UE's actions were compliant and security-focused. 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) (Restricted service area) 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 UE sending a Registration Complete message after completing 5G-AKA authentication, establishing a secure NAS context. The AMF responded with a protected Deregistration Request (security header type 2: integrity-protected and ciphered), initiating UE-terminated deregistration. The UE acknowledged this by sending a Deregistration Accept. According to 3GPP standards (TS 33.501), once 5G-AKA is complete, all subsequent NAS messages—including deregistration signaling—must be integrity-protected to prevent tampering, and ciphering is required if confidentiality is enabled (as indicated by the AMF's protected message). The UE's Deregistration Accept, sent after security context activation, would be non-compliant and insecure if transmitted unprotected (e.g., without integrity protection), as it could be forged or manipulated by an attacker. However, the test summary does not explicitly state the security status of this uplink message, creating ambiguity. Since the UE is expected to adhere to the security context established by 5G-AKA—and the test design focused on UE behavior without flagging protection failures—the absence of noted vulnerabilities implies standard-compliant protection. Thus, the UE's actions align with 5G security requirements. Secure

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 with the successful completion of 5G-AKA, establishing a secure context between the UE and AMF. The UE then sent a UL NAS TRANSPORT containing a PDU session establishment request. The AMF responded with a protected Configuration Update Command (security header type 3), which mandates integrity protection and encryption under the newly established security context. Instead of processing this valid command—which is permissible in the UE's REGISTERED state per 3GPP TS 24.501—the UE rejected it with an unprotected 5GMM status message indicating "Message type not compatible with the protocol state." This rejection is non-compliant, as the Configuration Update Command is allowed during ongoing procedures like PDU session establishment. Crucially, the UE's 5GMM status response lacked integrity protection and encryption, violating 3GPP TS 33.501, which requires all NAS messages post-5G-AKA to be protected when a security context is active. This omission exposes the UE to forgery or manipulation attacks, undermining NAS security. Insecure
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 with the UE sending a Uplink NAS Transport containing a PDU Session Establishment Request after successful 5G-AKA authentication. The AMF responded with a protected Downlink NAS Transport carrying a 5GMM Status message (Cause #98: "Message type not compatible with the protocol state"), indicating the UE's request was invalid in the current protocol context. Instead of handling this error as specified in 3GPP TS 24.501, the UE improperly sent another Uplink NAS Transport containing a 5GMM Status message with the same cause value. This response violates the 5GMM protocol in three critical ways: First, 5GMM Status messages must never be encapsulated within Uplink/Downlink NAS Transport messages (reserved for session management). Second, the UE should have treated Cause #98 as a fatal error, halted ongoing procedures, and potentially initiated re-registration rather than echoing the status. Third, reusing the NAS Transport container for a management message demonstrates improper message formatting. By deviating from the standard protocol state machine and message structure, the UE exposed an implementation flaw that could be exploited to induce undefined states or bypass security controls, as its non-compliant response might leak information about its internal state or fail to properly reset the security context. 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 sending a Registration Complete message, followed immediately by a Deregistration Request (UE originating) in the same UplinkNASTransport. The AMF, after acknowledging the uplink, responded with a protected DownlinkNASTransport containing a 5GMM Status message (Cause #101: "Message not compatible with the protocol state"), indicating the UE's combined messages violated the expected protocol sequence. The UE provided no response to this status message. According to 3GPP TS 24.501, after successful 5G-AKA, all NAS messages must be integrity-protected and encrypted. The AMF correctly protected its downlink message, adhering to security protocols. However, the UE's transmission of a Deregistration Request immediately after Registration Complete is abnormal, as the standard expects the UE to await network commands (e.g., Configuration Update) post-registration. This sequence likely triggered Cause #101, as deregistration is not permitted mid-registration without prior context. Crucially, the UE's lack of response aligns with 3GPP standards: GMM Status messages (especially for protocol errors) do not require acknowledgments or follow-ups (clause 5.4.4.3). Instead, the UE should internally handle the error (e.g., resetting the GMM state). While the UE's initial message bundling was non-compliant, its subsequent silence was protocol-compliant and avoided further unprotected exchanges. Thus, the core security posture (encryption, integrity, and error handling) remained intact. 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, initiating the establishment of a secure connection after 5G-AKA authentication was completed. The AMF responded with a Security Mode Command (SMC) protected using the existing security context (security header type 3), specifying the ciphering algorithm 5G-EA5 and the integrity algorithm 5G-IA0 (null integrity). The UE rejected this command with a Security Mode Reject, citing a "UE security capabilities mismatch." This rejection occurred because the AMF selected 5G-IA0 for integrity protection, which is explicitly prohibited for NAS signaling messages in 5G by 3GPP TS 33.501 (Section 6.4). The standard mandates that integrity protection is compulsory for NAS messages after initial authentication, and null integrity (5G-IA0) is only permitted for unauthenticated emergency services. The UE's rejection aligns with these requirements, as supporting null integrity would violate 5G security principles by leaving signaling vulnerable to tampering. By refusing the insecure configuration, the UE upheld the integrity protection mandate, demonstrating adherence to 3GPP security standards. 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 an unprotected Service Request after completing 5G-AKA. The AMF responded with a Security Mode Command, which was integrity-protected using the established security context, specifying 5G-EA5 for ciphering and 128-5G-IA2 for integrity. The UE rejected this command with a Security Mode Reject, citing a "UE security capabilities mismatch," indicating the selected algorithms were not supported per its advertised capabilities during registration. According to 3GPP standards (TS 33.501), the UE must verify the integrity of the Security Mode Command and ensure the chosen algorithms align with its provided security capabilities. By rejecting the command due to unsupported algorithms—rather than accepting them or failing to verify integrity—the UE adhered to security protocols. This prevents potential vulnerabilities, such as forced usage of unsecured or compromised algorithms. The UE correctly prioritized security context enforcement over network directives, demonstrating compliant and secure behavior. 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 newly established security context (security header type 3) and specified ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms. The UE rejected the SMC with an "unspecified" reject cause. According to 3GPP TS 33.501, after 5G-AKA, the UE must verify the integrity of the SMC using the K~AMF~ key derived during authentication. If verification fails—due to key mismatch, algorithm mismatch, or integrity check failure—the standard mandates rejection to prevent security context activation under potentially compromised conditions. Here, the UE's rejection indicates it detected an inconsistency (e.g., failed integrity check or unsupported algorithms), adhering to security protocols by halting further communication under an unverified context. This aligns with 3GPP requirements to mitigate risks like man-in-the-middle attacks. Secure
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 secure context between the UE and AMF. The UE then sent an Uplink NAS Transport message containing a PDU session establishment request. Subsequently, the AMF responded with a protected Downlink NAS Transport message (security header type 2: integrity-protected and ciphered), specifically a Configuration Update Command. The UE acknowledged this with an Uplink NAS Transport message carrying a Configuration Update Complete. Crucially, the UE's Configuration Update Complete message was not indicated to be protected (no security header type specified in the capture or summary), despite 3GPP TS 33.501 mandating that all NAS messages after 5G-AKA must be integrity-protected at minimum to prevent tampering and spoofing. By sending this critical response unprotected, the UE violated 5G security standards, exposing the communication to potential manipulation or replay 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 a Service Request to the AMF, initiating the procedure. The AMF responded with a Security Mode Command (SMC) that was integrity-protected using the new security context established during the prior 5G-AKA authentication. The SMC specified the ciphering algorithm 5G-EA4 (ZUC-based) and integrity algorithm 128-5G-IA3 (ZUC-based), along with ABBA parameter 0000. Instead of accepting the SMC and deriving the new keys (as required by 3GPP TS 33.501 and TS 24.501) or sending a standard Security Mode Reject message if the algorithms were unsupported, the UE responded with a 5GMM status message indicating "Invalid mandatory information." This cause typically denotes a protocol error, such as a missing or malformed mandatory information element in the SMC. However, the UE's failure to properly handle the SMC—either by completing the security setup or rejecting it explicitly—deviates from 5G standards. The use of a generic status message instead of the mandated Security Mode Reject suggests non-compliant behavior, potentially leaving the security context unresolved and exposing the session to risks like downgrade attacks or state synchronization failures. The UE should have validated the SMC's integrity (given it was protected), processed the algorithms, and adhered to protocol-specific rejection mechanisms if issues arose. Its response indicates insecure implementation per 3GPP specifications. Insecure

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 UL NAS Transport (PDU session establishment request) after completing 5G-AKA, establishing a shared key. The AMF responded with a Security Mode Command (SMC) protected with the initial security context (integrity-protected), proposing new algorithms (128-5G-EA2 for ciphering, 128-5G-IA2 for integrity) and ABBA parameter 00d2. The UE rejected this with a Security Mode Reject (cause: "unspecified"). According to 3GPP standards, after 5G-AKA, the SMC must be integrity-protected using the initial K_AMF-derived keys, and the UE must verify this protection before accepting new security parameters. The rejection—despite the AMF using standardized mandatory algorithms and proper protection—suggests the UE detected an anomaly, possibly in integrity verification, ABBA handling, or internal state consistency. By rejecting the SMC, the UE avoided activating a potentially compromised security context, prioritizing integrity validation over forced progression. This aligns with 3GPP security principles (TS 33.501), which mandate rigorous checks before context activation. 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 unprotected UL NAS TRANSPORT message containing a PDU session establishment request. The AMF responded with a Security Mode Command (SMC) protected with the new security context (security header type 4), specifying ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA1. This SMC message was integrity-protected and ciphered using keys derived from the completed 5G-AKA authentication. According to 3GPP TS 24.501 and TS 33.501, upon receiving a protected SMC, the UE must: (1) verify the message integrity, (2) validate the selected algorithms against its capabilities, (3) activate the new security context, and (4) respond with a Security Mode Complete message (protected with the new context). The UE's failure to send any response violates this protocol. This omission leaves the security context activation unconfirmed, prevents the AMF from progressing securely, and could indicate an inability to process the SMC correctly (e.g., decryption or integrity check failure). Since the standard mandates a response to complete the security handshake, the UE's inaction constitutes a protocol breach and exposes the session to risks like bidding-down attacks or stagnation. 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 unprotected UL NAS TRANSPORT (PDU session establishment request), as indicated by the absence of security header notation in the packet capture and test summary. The AMF responded with a protected Configuration Update Command (security header type 2: integrity-protected and ciphered), adhering to 5G security requirements. The UE then replied with a Configuration Update Complete message, which was also sent without security protection, as no security header was mentioned in the test summary or packet capture for this or the initial uplink message. According to 3GPP standards (TS 33.501), once 5G-AKA completes and a security context is established, all subsequent NAS messages—including uplink transmissions—must be integrity-protected to prevent tampering, with ciphering applied where confidentiality is required. The UE's failure to apply integrity protection to its uplink messages (UL NAS TRANSPORT and Configuration Update Complete) violates this mandate, exposing the communication to potential manipulation or replay attacks. 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 UL NAS TRANSPORT message containing a PDU session establishment request. The AMF responded with a Security Mode Command (SMC) protected under a new security context (security header type 3), specifying integrity algorithm 128-5G-IA1 and null ciphering (5G-EA0), along with ABBA parameter "1111". The UE rejected this command with a Security Mode Reject message, citing an unspecified cause (interpreted as 3GPP cause #96, "Invalid mandatory information"). This rejection aligns with 5G security standards (3GPP TS 33.501 and 24.501) as the UE likely detected an integrity verification failure or invalid ABBA parameter during SMC processing. The SMC message was the first integrity-protected downlink message post-authentication, requiring the UE to validate its integrity using the newly established K~AMF~ key. An incorrect ABBA (which must match the UE's stored value from 5G-AKA to prevent bidding-down attacks) or a mismatched integrity calculation would constitute "invalid mandatory information," justifying cause #96. The UE's refusal to proceed without successful verification demonstrates adherence to security protocols, as accepting an unverified or tampered SMC could compromise subsequent communications. 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 began with the UE sending a Registration Complete message to the AMF, confirming successful 5G-AKA authentication and establishing a secure NAS context. Subsequently, the AMF sent a protected Deregistration Accept message (indicating UE-terminated deregistration) to the UE. This downlink message was integrity-protected and encrypted per the active security context, as confirmed by the "Protected" status and the prior completion of 5G-AKA. The UE provided no response to this message. According to 3GPP TS 24.501, upon receiving a protected Deregistration Accept for UE-terminated deregistration, the UE must silently deregister, release resources, and transition to the DEREGISTERED state without transmitting further NAS messages. The absence of a response aligns precisely with this requirement, demonstrating proper handling of the deregistration command without unnecessary communication that could expose vulnerabilities. The UE correctly trusted the integrity-protected downlink message and adhered to protocol-mandated behavior, maintaining session security. 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 as part of the 5G-AKA procedure. However, before authentication could complete, the AMF responded with a Service Reject message containing 5GMM Cause #111 ("Protocol error, unspecified"), sent in plaintext since no security context was established. The UE then ceased communication, providing no further response. According to 3GPP standards (TS 24.501 and TS 33.501), NAS messages prior to 5G-AKA completion must remain unencrypted, as cryptographic keys are not yet available. The UE's lack of response to the Service Reject aligns with protocol expectations—where Cause #111 indicates an unrecoverable error—by terminating the session without exposing additional vulnerabilities or processing potentially malicious payloads. This behavior prevents unnecessary resource consumption and avoids potential exploitation of unauthenticated states, adhering to security best practices for handling protocol errors during initial authentication. 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 UE initiated the registration procedure by sending an unprotected Registration Request message to the AMF, as 5G-AKA authentication had not yet been completed, leaving NAS communications unencrypted. The AMF responded with an unprotected Service Reject message containing 5GMM cause value #9 ("UE identity cannot be derived by the network"), indicating the network failed to identify or authenticate the UE. Per 3GPP TS 24.501, the UE correctly terminated the registration attempt upon receiving this reject cause without further communication, as no security context existed to protect subsequent messages. Since the UE did not transmit sensitive data (e.g., SUPI) in plaintext beyond the initial request and adhered to protocol termination requirements, its actions align with 5G security standards for unauthenticated states. The absence of unnecessary retransmissions or exposure of credentials mitigates risks inherent in unprotected NAS signaling. Secure

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 unprotected Identity Response to the AMF. The AMF then responded with a Security Mode Command (SMC) marked as "Integrity protected with new security context," specifying ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA1, despite the 5G-AKA authentication not being completed. The UE rejected this command with a Security Mode Reject (cause: unspecified). According to 3GPP standards (TS 33.501), NAS security context establishment via SMC must occur **after** successful 5G-AKA authentication, which generates the root key (K~AMF~) necessary for integrity protection. The AMF's transmission of an "integrity-protected" SMC without prior authentication violates this sequence, as no valid keys exist for integrity verification. The UE correctly identified this anomaly: accepting an unprotected SMC would expose it to downgrade attacks or forced security context activation without authentication. By rejecting the command, the UE adhered to the standard's security hierarchy, preventing unauthorized context establishment. 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 between the UE and AMF occurred before 5G-AKA authentication was completed, as explicitly stated. The UE first sent an Identity Response, followed by the AMF sending a plaintext Identity Request (requesting SUCI). The UE then responded with another Identity Response containing the SUCI. According to 3GPP standards (TS 33.501), NAS messages exchanged before authentication must not be encrypted, as no security context exists. The use of SUCI—a privacy-preserving identifier encrypted with the home network's public key—is specifically designed for unprotected transmission in this pre-authentication phase. The UE correctly avoided sending sensitive data (like SUPI) in plaintext and adhered to the protocol by transmitting SUCI without encryption. No deviation from the standard was observed in the UE's behavior. 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 initial Registration Request via an InitialUEMessage, which is unprotected as 5G-AKA had not yet been initiated. The AMF responded with an Authentication Reject message sent in plaintext, as no security context existed for encryption. The UE exhibited no further communication after receiving this reject. According to 3GPP standards (TS 33.501 and TS 24.501), initial NAS messages prior to authentication are inherently unprotected, and an Authentication Reject terminates the registration procedure without requiring a UE response. The UE's silence aligns with protocol expectations, as responding to an unprotected reject could expose vulnerabilities (e.g., to bidding-down attacks). By refraining from further action, the UE avoided processing unauthenticated commands and maintained a deregistered state until potential re-attempts under controlled conditions. This behavior adheres to security best practices for handling unverified rejections in the pre-authentication phase. 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 a successful 5G-AKA authentication. The AMF then sent a protected Deregistration Request (UE-terminated), which was integrity-protected and ciphered (security header type 2) in accordance with 5G security standards. The UE responded with a Deregistration Accept. However, the test summary and packet capture do not establish that the UE protected this Deregistration Accept message with integrity or ciphering. According to 3GPP standards (TS 33.501), after 5G-AKA completion, all subsequent NAS messages—except initial Registration Requests and Identity Responses—must be integrity-protected to prevent tampering and ensure authenticity. The Deregistration Accept is not an exempted message and must be protected. The UE's failure to apply integrity protection to this message violates 5G security requirements, leaving it vulnerable to attacks such as replay or injection. 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 via an unprotected UplinkNASTransport message, which is permissible at this stage as 5G-AKA authentication had not yet been completed, and initial NAS messages may be sent unsecured. The AMF then responded with a DownlinkNASTransport message carrying a Deregistration Accept (UE terminated), sent in plain text without encryption or integrity protection. The UE exhibited no response to this message. According to 3GPP standards (TS 24.501 and TS 33.501), after initiating NAS signaling, critical procedural messages like Deregistration Accept require security context activation via 5G-AKA to ensure confidentiality and integrity. Since 5G-AKA was incomplete, the AMF's transmission of Deregistration Accept unprotected violates the protocol, which mandates that such commands only be sent after security establishment. The UE's lack of response aligns with standard behavior, as processing an unprotected, security-sensitive command could expose it to spoofing or forced deregistration attacks. Thus, while the UE acted securely by ignoring the invalid message, the overall scenario highlights an AMF deviation from 5G security protocols. Insecure
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 replied with a plain (unencrypted) Authentication Request containing invalid parameters: a RAND value of all zeros and an AUTN value of all zeros, along with other elements like ABBA and ngKSI. The UE, upon receiving this request, responded with a 5GMM Status message indicating "Invalid mandatory information" (cause #96 per 3GPP TS 24.501), rejecting the authentication attempt. According to 3GPP standards (TS 33.501 and TS 24.501), the AUTN is critical for network authentication and must be validated by the UE. An all-zero AUTN fails structural and cryptographic validation, as it cannot contain a valid MAC or SQN. The standard mandates that such failures should trigger an Authentication Failure message with specific causes like "MAC failure" or "Synch failure." Instead, the UE used a generic 5GMM Status message, which is non-compliant for this scenario. This deviation obscures the root cause from the network and violates protocol specifications, potentially hindering security diagnostics. Insecure

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 successful 5G-AKA authentication. The AMF then sent a Security Mode Command, which was integrity-protected (security header type 3) but proposed null ciphering (5G-EA0) and integrity algorithm 128-5G-IA2, along with ABBA parameter 3100. The UE rejected this command with a Security Mode Reject (cause: "unspecified"), indicating it refused to establish the security context as configured. According to 3GPP standards (TS 33.501), while null ciphering (5G-EA0) is permitted in limited scenarios (e.g., emergency services), UEs should reject it for normal operations to enforce confidentiality. The UE’s rejection aligns with security best practices by preventing unencrypted communication, which could expose sensitive data. The "unspecified" cause, while vague, does not invalidate the security merit of rejecting null ciphering. Thus, the UE prioritized confidentiality as mandated by 5G security principles. 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, followed by the AMF sending a plaintext Authentication Request containing RAND (all 0x35), AUTN (all 0x35), ABBA (0x3131), and ngKSI parameters. The UE responded with an Authentication Failure message, explicitly stating "Non-5G authentication unacceptable." This rejection occurred because the UE detected that the provided AUTN—which was structured as a 16-byte value identical to EPS (4G) authentication tokens—lacked the 5G-specific extensions mandated by 3GPP TS 33.501. Specifically, 5G-AKA requires AUTN to include additional fields like the 5G-HN public key identifier or SUPI concealment metadata, ensuring network authenticity and alignment with 5G security policies. By rejecting the non-compliant AUTN, the UE correctly adhered to 3GPP standards (TS 24.501 Sect. 5.4.1.3), preventing potential security risks such as bidding-down attacks or processing of unverified network credentials. The plaintext transmission was expected, as 5G-AKA must complete before encryption activation. Thus, the UE's action proactively enforced 5G security requirements. 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 NAS communication by sending an unencrypted Initial Registration Request (as expected before 5G-AKA completion). The AMF responded with an unencrypted Registration Reject containing 5GMM Cause #26 ("Insufficient resources"), to which the UE correctly provided no response. According to 3GPP TS 24.501, upon receiving a Registration Reject—especially with non-security-related cause codes like #26—the UE must: (1) halt further registration attempts toward the rejected PLMN, (2) transition to a limited-service state, and (3) refrain from sending any NAS response unless explicitly required (e.g., for emergency services). The UE's silence here aligns with standard protocol behavior, as no response is mandated or expected for Registration Reject messages. Since the UE complied with termination procedures without exposing additional vulnerabilities (e.g., ignoring the reject or retrying prematurely), its actions maintained protocol integrity despite the unsecured reject message, which was unavoidable pre-authentication. 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 message to the AMF in plain text, as the 5G-AKA authentication had not yet been completed, meaning no security context was established. The AMF responded with a Service Reject message (also in plain text) containing 5GMM Cause #99 ("semantically incorrect message"), indicating a protocol-level error in the UE's previous communication. The UE did not respond further, which aligns with standard behavior when receiving a Service Reject that terminates the session. From a security perspective, the UE's actions were **secure** according to 3GPP standards (TS 33.501 and TS 24.501). Before 5G-AKA completion, NAS messages must remain unencrypted because keys for confidentiality and integrity protection are derived during authentication. The UE correctly sent its Identity Response in plain text and abstained from unnecessary further communication after the Service Reject, avoiding any premature or non-compliant encryption attempts. The cause code #99 suggests a semantic error (e.g., malformed information element), but this relates to functional correctness, not a security violation. The UE adhered to the protocol's security state by not encrypting messages pre-authentication and handling the reject appropriately. 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 replied with a plain-text Authentication Request containing a RAND (3535...35) and AUTN (3535...35), both set to artificial constant values. The UE rejected this request with an Authentication Failure message, explicitly stating "Non-5G authentication unacceptable." This response aligns with 3GPP TS 33.501 and TS 24.501, where the UE must verify the AUTN's validity and the 5G-specific AMF bit (indicating 5G context). The AUTN's constant value (without the mandatory 5G bit set) would fail this check, as it cannot be validated as a genuine 5G authentication token. By rejecting the improperly formatted AUTN—which could indicate a downgrade attack or network spoofing—the UE correctly enforced 5G security protocols, preventing potential unauthorized access. Its adherence to the standard safeguards against accepting non-compliant or legacy (e.g., 4G) authentication attempts. 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 part of the NAS registration procedure. Before 5G-AKA authentication could be completed, the AMF responded with a Service Reject message containing 5GMM Cause #3 ("Illegal UE"), sent in plaintext since no security context existed. The UE exhibited no further communication after this rejection. According to 3GPP standards (TS 24.501), NAS messages prior to 5G-AKA completion are inherently unprotected, and the plaintext transmission of the Service Reject by the AMF is standard-compliant in this unauthenticated state. The UE's lack of response aligns with protocol expectations, as Service Reject terminates the registration attempt without requiring acknowledgment. Crucially, the UE did not proceed with any security-sensitive actions (e.g., transmitting user data or reattempting registration without cause analysis) after the rejection, demonstrating adherence to security protocols by halting further unprotected communication. 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 "Integrity protected with new security context" (security header type 3), but specified null algorithms (5G-EA0 for ciphering and 5G-IA0 for integrity) despite 5G-AKA authentication not being completed. The UE rejected this command with a Security Mode Reject (cause: unspecified), refusing to proceed. According to 3GPP standards (TS 33.501), NAS security must not be activated with null algorithms after initial registration, as this leaves signaling unprotected against tampering or eavesdropping. The AMF's SMC—claiming protection while mandating null algorithms—contradicts security requirements, as null algorithms provide no protection. The UE correctly identified this invalid state by rejecting the command, preventing the establishment of an insecure connection that would violate 5G's mandatory encryption and integrity policies for post-registration NAS messages. This adherence to protocol safeguards against potential downgrade attacks or forced insecurity. 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 Identity Response to the AMF. The AMF then responded with a Security Mode Command (SMC), which was marked as "Integrity protected with new security context" and included ABBA parameter 3000, null ciphering (5G-EA0), and integrity algorithm 128-5G-IA3. Crucially, the 5G-AKA authentication had not been completed at this stage, meaning no shared security keys were established between the UE and AMF. The UE rejected the SMC with a Security Mode Reject (cause: "unspecified") because it received a protected NAS message requiring integrity verification without having the necessary keys derived from a prior successful authentication. According to 3GPP standards (TS 33.501), NAS security (including SMC processing) must only occur after 5G-AKA completes to ensure keys are available for message validation. Accepting or processing a protected SMC without authentication would violate the security hierarchy, exposing the UE to potential forgery attacks. The UE's rejection aligns with this requirement by refusing to proceed without verified keys, demonstrating correct security posture. 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 between the UE and AMF began with the UE sending an unsolicited Authentication Response message (without prior receipt of an Authentication Request from the AMF). The AMF then responded with a DownlinkNASTransport containing an Authentication Request, which included the RAND, AUTN, and security parameters (ngKSI), and was explicitly sent in plaintext since 5G-AKA had not yet been completed. The UE subsequently sent another Authentication Response, likely in reply to this request. According to 3GPP standards (TS 33.501), NAS messages like Authentication Request/Response must be sent unprotected (plaintext) before 5G-AKA establishes a security context, as encryption/integrity keys are derived only after successful authentication. However, the UE's initial transmission of an Authentication Response without a triggering Authentication Request violates the protocol sequence, which mandates that the network (AMF) must initiate authentication by sending the request first. This unsolicited response indicates improper state handling by the UE, potentially exposing authentication-related data prematurely and deviating from standard security procedures. 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) (Unknown) 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 successful completion of 5G-AKA, establishing a secure NAS context. The UE sent a Registration Complete message, followed by the AMF transmitting a protected Deregistration Request (security header type 2, indicating integrity protection and ciphering). The UE responded with a Deregistration Accept. According to 3GPP standards (TS 33.501), once 5G-AKA completes, all subsequent NAS messages must be integrity-protected and ciphered by both the UE and network. The AMF's Deregistration Request was correctly protected, as confirmed in the test summary. For the UE's Deregistration Accept, the test summary explicitly notes the UE "provided" the message but does not specify its security status. However, 3GPP mandates that after 5G-AKA, UEs must protect all NAS messages (including Deregistration Accept) unless explicitly exempted (e.g., during initial unsecured procedures). No exemption applies here, and the UE's failure to protect this message would violate 3GPP requirements. Since the test summary omits security details for the UE's Deregistration Accept—while explicitly confirming protection for the AMF's message—it implies the UE sent it unprotected, constituting a security lapse. Insecure

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 an Authentication Request containing a RAND value and an all-zero AUTN (Authentication Token), sent unencrypted as plain NAS text since 5G-AKA had not yet been completed. The UE rejected this message with a 5GMM Status message indicating "Invalid mandatory information" (cause #96), specifically targeting the invalid AUTN. According to 3GPP TS 24.501, the AUTN is a mandatory information element that must contain a valid network authentication signature generated by the home network. An all-zero AUTN is syntactically invalid and fails to provide legitimate network authentication credentials. The UE correctly identified this anomaly and aborted the procedure, as accepting such an AUTN would compromise network authentication and expose the UE to spoofing attacks. This behavior aligns with 5G security standards by preventing authentication with an unverified network. 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 ngKSI parameters) sent in plain text, as 5G-AKA had not yet been completed to establish a security context. Instead of replying with an Authentication Response to continue the authentication process, the UE sent a Deregistration Request (UE originating) while still in an unauthenticated state. According to 3GPP standards (TS 33.501), NAS messages exchanged before 5G-AKA completion lack integrity protection and encryption, making them vulnerable to tampering or interception. The UE's transmission of a sensitive service-termination message (Deregistration Request) without waiting for security context establishment violates 5G security principles, which require critical procedures like deregistration to be protected after authentication. This premature action exposes the deregistration request to potential manipulation or replay attacks, as it was sent in plain text before cryptographic keys were derived. 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 UplinkNASTransport, indicating its attempt to complete the 5G-AKA authentication procedure. The AMF then responded with an Authentication Reject message in DownlinkNASTransport, transmitted in plain text because the 5G-AKA had not yet been completed, leaving the communication unprotected. The UE exhibited no further response after receiving the reject. According to 3GPP standards (TS 33.501 and TS 24.501), NAS messages prior to 5G-AKA completion lack encryption and integrity protection, making plain-text transmission expected for non-secured messages like Authentication Reject. Critically, the UE's lack of action upon receiving the reject aligns with protocol requirements: Upon authentication rejection, the UE must deregister locally, cease communication attempts for the current PLMN, and avoid transmitting sensitive data or responses that could expose vulnerabilities. By silently handling the rejection internally—without initiating new messages, retries, or security compromises—the UE adhered to security protocols, mitigating risks like credential leakage or forced re-authentication attacks. Thus, its behavior was compliant and secure. 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 to the AMF, followed by the AMF responding with a plain-text Authentication Request containing RAND, AUTN, ABBA, and security context parameters. The AUTN structure (AMF field `3000` hex) explicitly indicated a 5G authentication request, as the most significant bit (bit 15) was set to 0 per 3GPP TS 33.501. However, the UE rejected this request with an Authentication Failure message, citing "Non-5G authentication unacceptable" (cause #22 from TS 24.501). This cause is reserved for scenarios where the UE receives a non-5G method (e.g., EPS AKA) and refuses fallback. Since the AUTN's AMF field unambiguously signaled 5G authentication, the UE misinterpreted a valid 5G-AKA request as non-5G. This deviation from the 3GPP standard—where UEs must correctly process AUTN per the separation bit—constitutes an implementation flaw. Such misclassification could enable denial-of-service attacks by tricking the UE into rejecting legitimate 5G networks, undermining service availability and compliance. Insecure
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 successful completion of 5G-AKA, establishing a secure context. The UE sent a Registration Complete message to the AMF, confirming its registration. Subsequently, the AMF sent a Deregistration Request (UE-terminated) to the UE, which was correctly protected with both integrity protection and ciphering (security header type 2) in accordance with 5G security standards (3GPP TS 33.501). However, the UE failed to respond to this request. According to 3GPP TS 24.501, upon receiving a valid UE-terminated Deregistration Request, the UE must send a Deregistration Accept message to acknowledge the deregistration. The absence of this mandatory response violates the protocol, indicating improper handling of the deregistration procedure. This omission leaves the deregistration process incomplete and undermines the state synchronization between the UE and network, exposing a failure to comply with standard security protocols. 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 UE sending a Registration Complete message after successful 5G-AKA authentication, establishing a secure NAS signaling connection. The AMF then sent a Configuration Update Command, which was protected with both integrity protection 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. Crucially, the UE's response was sent only after receiving a properly protected downlink message (Configuration Update Command), and the UE correctly generated the expected response, confirming it validated the message's integrity and deciphered it using the established security context. This aligns with 3GPP mandates that after 5G-AKA completion, all subsequent NAS messages (except specific unprotected exceptions like initial registration or authentication) must be integrity-protected and ciphered. Since the UE processed the protected command and responded appropriately—without any indication of accepting unprotected sensitive commands or mishandling keys—its actions adhered to security protocols. The lack of anomalous behavior (e.g., responding to unprotected or malformed commands) further supports 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 initial Security Mode Complete message alongside a Registration Request, prior to receiving any Security Mode Command from the AMF. Subsequently, the AMF sent a Security Mode Command (protected with integrity using algorithm 128-5G-IA2 and no encryption via 5G-EA0) to activate the new security context. The UE then sent a second Security Mode Complete message in response. According to 3GPP standards (TS 24.501 and TS 33.501), the Security Mode Complete message must only be sent by the UE as a direct response to a valid, integrity-protected Security Mode Command from the network. Transmitting Security Mode Complete before receiving and verifying this command violates the protocol sequence, as it assumes security context activation prematurely. This deviation risks processing unprotected or maliciously injected NAS messages, undermining the mutual authentication and integrity protection established during 5G-AKA. The UE’s premature transmission exposes it to potential replay or manipulation attacks, indicating non-compliant behavior. 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, establishing mutual authentication and security keys. The UE then sent a Security Mode Complete message, confirming activation of the negotiated security algorithms for NAS protection. Subsequently, the AMF transmitted a protected Deregistration Accept message (indicating UE-terminated deregistration), which was encrypted and integrity-protected using the established security context. The UE provided no response to this message, consistent with 3GPP TS 24.501 standards, as Deregistration Accept is a network-initiated procedure that does not require UE acknowledgment or further action. Critically, the UE adhered to security protocols by ensuring all post-authentication uplink messages (Security Mode Complete) were protected before transmission. The AMF's protected downlink message aligned with 5G security requirements, and the UE's lack of response was compliant and expected, avoiding unnecessary exposure. The UE maintained confidentiality and integrity protections throughout, with no deviation from the mandated flow. 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 UE successfully completing 5G-AKA and sending a Security Mode Complete message to the AMF, confirming activation of the new security context. The AMF then sent a Configuration Update Command, which was integrity-protected using the newly established security context (security header type 3). The UE, upon receiving this command, performed an integrity check (which passed, as no integrity failure was indicated) but determined that the Configuration Update Command was received in an incompatible protocol state—specifically, during an ongoing registration procedure where such a command is not expected post–Security Mode Complete but before registration finalization. Consequently, the UE responded with a 5GMM status message (cause value #98: "Message type not compatible with protocol state"), as mandated by 3GPP TS 24.501. This behavior demonstrates that the UE properly validated message integrity and enforced protocol state consistency, rejecting the out-of-sequence command without processing it. The response aligns with 3GPP security requirements, as the UE prioritized state-machine correctness over executing a potentially disruptive command in an invalid context. 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 UE sending a Security Mode Complete message, confirming the successful establishment of security contexts following 5G-AKA authentication. The AMF then responded with a protected Deregistration Request (security header type 2: integrity-protected and ciphered), initiating a UE-terminated deregistration. The UE acknowledged this with a Deregistration Accept message. According to 3GPP standards (TS 33.501 and TS 24.501), after Security Mode Complete is sent, all subsequent NAS messages—including Deregistration Accept—**must** be integrity-protected at confirmation, and ciphered if confidentiality is enabled. The packet capture explicitly notes the AMF's Deregistration Request as protected but omits any security header indication for the UE's Deregistration Accept. Given that the test summary emphasizes security validation and would highlight protection if present, this omission implies the UE sent the Deregistration Accept **unprotected**. This violates 3GPP mandates to protect NAS messages post-security setup, exposing the message to tampering or forgery. 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 prematurely sending a Security Mode Complete message alongside a Registration Request, without having received a Security Mode Command from the AMF first. Subsequently, the AMF transmitted a protected Security Mode Command specifying ciphering algorithm 5G-EA7 and integrity algorithm 128-5G-IA2. The UE then sent another Security Mode Complete after this command. According to 3GPP standards (TS 33.501 and TS 24.501), the Security Mode Command must initiate the security activation procedure, with the UE only sending Security Mode Complete in response after validating the command's integrity and parameters. The UE's initial transmission of Security Mode Complete prior to receiving the command violates this sequence, as it attempts to confirm security activation before the network has issued the relevant parameters or instructions. This deviation bypasses critical security validations, including algorithm negotiation and replay attack protection (via ABBA), and could indicate improper handling of the security context. Such behavior exposes the system to potential bidding-down attacks or unauthorized context activation, undermining the protocol's security framework. 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 mutual authentication and security keys. The UE then sent a Security Mode Complete message, confirming activation of security contexts. Subsequently, the AMF sent a protected Deregistration Request (integrity-protected and ciphered, security header type 2), indicating a network-initiated deregistration. The UE responded with a Deregistration Accept message. According to 3GPP standards (TS 33.501), after Security Mode Complete, all NAS messages—including Deregistration Accept—must be integrity-protected and ciphered to prevent forgery or eavesdropping. However, the test summary explicitly noted the AMF's Deregistration Request as protected but omitted any security indication for the UE's Deregistration Accept. Given that the test focused on UE actions and the summary highlighted protection only for the AMF's message, it implies the UE sent the Deregistration Accept without applying mandatory security measures. This violates 3GPP requirements, as post-security-activation messages must remain protected until context release. 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 InitialUEMessage containing a Registration Request to the AMF, indicating a request for network registration. The AMF responded with a DownlinkNASTransport message containing an Identity Request for the GUTI, which was sent in plaintext as the 5G-AKA authentication procedure had not yet been completed. The UE provided no response to this Identity Request. According to 3GPP standards (TS 33.501 and TS 24.501), the GUTI is a privacy-sensitive identifier that must only be transmitted after the establishment of a secure NAS context through 5G-AKA. Since the AMF's request was unencrypted and lacked integrity protection, the UE correctly refrained from disclosing its GUTI to prevent potential tracking or privacy breaches. This aligns with security requirements mandating that sensitive identities must not be exposed before authentication and key agreement finalize. The UE's non-response demonstrates adherence to 5G security protocols by avoiding transmission of protected data in an insecure state. Secure

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 5G-AKA authentication had not yet been completed. The AMF responded with a Configuration Update Command (CUC) marked as "Protected" in the DownlinkNASTransport message, though the security header was noted as "Unknown". The UE provided no response to this message. According to 3GPP standards (TS 33.501 and TS 24.501), NAS message protection (integrity and ciphering) requires a valid 5G security context established via 5G-AKA and Security Mode Command (SMC) procedures. Since 5G-AKA was incomplete, the UE lacked the necessary keys to verify or process protected NAS messages. The standard mandates that a UE must discard such protected messages received without an active security context to prevent processing potentially malicious or malformed commands. By not responding, the UE adhered to this security requirement, avoiding potential exploitation (e.g., forced configuration changes or bidding-down attacks). Thus, the UE's inaction aligns with 3GPP security protocols. 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) marked as "Integrity protected with new security context" (security header type 3), but specified a null integrity algorithm (5G-IA0) and a non-null ciphering algorithm (128-5G-EA3). Crucially, 5G-AKA authentication had not been completed, meaning no valid security context existed for protection. The UE rejected this message with a 5GMM status indicating "Invalid mandatory information." According to 3GPP standards (TS 33.501 and TS 24.501), the SMC must be integrity-protected using a non-null algorithm (not IA0) to ensure message authenticity and prevent downgrade attacks. The AMF's use of IA0 for "protected" SMC violates this requirement, as IA0 provides no integrity. The UE correctly identified this inconsistency, as accepting an SMC with null integrity would expose it to tampering or forgery. By rejecting the flawed SMC, the UE adhered to security protocols, demonstrating robust implementation against invalid security parameter combinations. 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 Initial Registration Request via an InitialUEMessage, which was unprotected, as expected at this stage since 5G-AKA authentication had not yet been completed. The AMF then responded with a DownlinkNASTransport containing a Configuration Update Command, which was marked as protected (security header type 2, indicating integrity protection and ciphering). However, since 5G-AKA had not been performed, no valid security context (K~AMF~, derived keys) existed between the UE and AMF. According to 3GPP TS 33.501, NAS security (integrity and ciphering) must only be applied *after* successful 5G-AKA establishes a mutual security context. The UE correctly ignored the protected Configuration Update Command, as it could not verify the integrity or decipher the message without valid keys. This aligns with 3GPP standards, which mandate that UEs must reject protected NAS messages received prior to security context establishment to prevent processing potentially malicious or forged commands. The UE's lack of response demonstrates adherence to security protocols by avoiding engagement with unsolicited protected messages in an unauthenticated state. Secure
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 UE initiated communication by sending an unprotected Initial Registration Request, as expected without an established security context. The AMF then responded with a protected Deregistration Accept message without completing the mandatory 5G-AKA authentication procedure. According to 3GPP standards (TS 33.501), NAS message protection requires prior successful 5G-AKA to establish cryptographic keys. Since 5G-AKA was not performed, the UE had no valid security context to decrypt or verify the integrity of the protected message. The UE's lack of response demonstrates it correctly ignored the illegitimate protected message, as processing it without authentication could expose vulnerabilities like accepting forged network commands. This adherence to security protocols—rejecting unprotected processing of protected messages—aligns with 3GPP requirements. 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" (security header type 3), yet 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 cause. According to 3GPP standards (TS 33.501), null algorithms (5G-EA0/IA0) are explicitly prohibited for protected NAS messages once security activation is initiated. The SMC's use of security header type 3 while selecting null algorithms creates an invalid contradiction, as this header requires non-null integrity protection. The UE correctly identified this violation, as accepting null algorithms in a "protected" context would expose subsequent communications to tampering or eavesdropping. By rejecting the flawed SMC, the UE adhered to 5G security principles, preventing an insecure configuration that bypassed essential protections. 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 for the first NAS message prior to authentication. Before 5G-AKA could be completed to establish a security context, the AMF responded with a Deregistration Request message that was marked as "Integrity protected and ciphered" (security header type 2). Crucially, the UE did not respond to this downlink message. According to 3GPP standards (TS 33.501), NAS security (integrity protection and ciphering) must only be applied *after* successful 5G-AKA authentication and key derivation. Since 5G-AKA was incomplete, the UE lacked the necessary keys to verify or decrypt the protected Deregistration Request. By ignoring this unsolicited protected message—which could not be validated without an established security context—the UE correctly adhered to security protocols. This prevents processing potentially malicious or forged commands during the vulnerable pre-authentication phase, aligning with 3GPP's mandate that protected NAS messages require a valid security context. 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 transmitting an unprotected (plain) Identity Request for the IMEISV, as the 5G-AKA authentication had not yet been completed. The UE provided no response to this request. According to 3GPP standards (TS 33.501), the IMEISV is sensitive information that must only be transmitted after a security context is established (i.e., post-5G-AKA), ensuring encryption and integrity protection. Since the AMF's request was sent in plaintext without an active security context, the UE's lack of response aligns with security requirements by avoiding the exposure of the IMEISV in an unprotected manner. This prevents potential eavesdropping or manipulation by attackers during the vulnerable pre-authentication phase. Although a compliant UE might ideally respond with a protected "no identity" or error indication after security activation, the absence of a response here prioritizes confidentiality over protocol responsiveness, adhering to the core security principle of safeguarding sensitive data. 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 (containing likely the SUCI or another requested identity) via an unprotected UplinkNASTransport message, as 5G-AKA had not yet been completed to establish a security context. The AMF responded with a DownlinkNASTransport message carrying a 5GMM Status (Cause #13: "Roaming not allowed in this tracking area"), explicitly sent in plaintext without encryption or integrity protection. The UE provided no response to this message. According to 3GPP standards (TS 33.501), NAS messages exchanged before 5G-AKA completion—including Identity Request/Response—may legitimately be sent unprotected, as no security context exists. However, the 5GMM Status message is a post-initialization control message that typically requires integrity protection once security procedures are initiated, as it can terminate sessions or alter UE behavior (e.g., rejecting registration). Cause #13 specifically impacts mobility decisions, making it a potential vector for denial-of-service attacks if accepted without verification. While the standard permits unprotected messaging *before* 5G-AKA, the UE's silent acceptance of an unprotected 5GMM Status—without challenging the lack of security or ignoring it due to missing integrity—demonstrates non-compliance with 3GPP security principles (TS 24.501, § 4.4.4). A secure UE should either discard such messages or trigger recovery procedures when receiving unverified control commands after initiating registration. Here, the UE implicitly trusted an unprotected directive, exposing it to spoofed network attacks. Insecure

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 to the AMF in plaintext, which is acceptable as no security context existed at this initial stage. The AMF then responded with a Configuration Update Command, also sent as a plain NAS message (security header type 0), despite the absence of a completed 5G-AKA authentication procedure. The UE did not respond to this command. According to 3GPP standards (TS 24.501 and TS 33.501), after initial registration steps but before 5G-AKA completion, only a limited set of NAS messages (e.g., Authentication Request, Identity Request, Security Mode Command) are permitted in plaintext. The Configuration Update Command is not among these allowed messages and must be integrity-protected once security contexts are initiated. By accepting and processing an unprotected Configuration Update Command—or failing to explicitly reject it—the UE violated 3GPP security requirements. The standard mandates that UEs discard such unsecured, non-permitted messages and may trigger recovery procedures (e.g., re-registration). The UE's lack of response here suggests it silently processed the command or ignored a security violation, both of which undermine trust in the UE's security posture. This behavior exposes the UE to potential man-in-the-middle attacks, such as malicious configuration updates. Insecure
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 5G-AKA authentication had not yet been completed. The AMF then responded with a Deregistration Accept message marked as "Protected," despite the absence of an established security context. Crucially, the UE exhibited no response to this protected downlink message. According to 3GPP standards (TS 33.501), NAS messages requiring protection (integrity and/or confidentiality) must not be processed before 5G-AKA successfully establishes security keys. The UE should have rejected the protected Deregistration Accept by either ignoring it (triggering AMF recovery procedures) or responding with a Security Mode Reject (5GMM cause #96 "invalid mandatory information"), as processing protected messages without keys undermines security assumptions. The UE's lack of action—failing to challenge or reject the improperly protected message—demonstrates non-compliant behavior, leaving it vulnerable to maliciously crafted protected messages that could induce undefined states or denial-of-service. Insecure

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 Identity Response to the AMF, which is a standard unprotected message during initial NAS procedures. The AMF then responded with a Service Accept message marked as "Protected," indicating it was encrypted and integrity-protected. However, the 5G-AKA authentication procedure had not been completed at this stage, meaning no security context (including ciphering/integrity keys) was established between the UE and AMF. According to 3GPP standards (TS 33.501), NAS protection must only be applied *after* successful 5G-AKA, as the keys derived during authentication enable secure communication. The UE's lack of response to the protected Service Accept message demonstrates it correctly rejected this improperly protected message, as it lacked the security context to decrypt or validate it. This aligns with 3GPP requirements, which mandate that UEs must ignore or reject protected NAS messages received before security setup completion to prevent processing potentially malicious or malformed data. 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, as 5G-AKA had not yet been completed to establish a security context. Subsequently, the AMF sent a Deregistration Request message protected with both integrity and ciphering (security header type 2), despite the absence of a valid security context. The UE did not respond to this protected downlink message. According to 3GPP standards (TS 33.501), NAS security (integrity and ciphering) is only applicable after successful 5G-AKA authentication, which establishes the necessary keys. Sending a protected message without this context violates the protocol, as the UE cannot validate or process it securely. The UE's lack of response aligns with the standard's security expectations, as processing such a message would risk accepting malicious or unverified commands. Thus, the UE correctly ignored the anomalous protected message, demonstrating secure behavior by adhering to protocol requirements. 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, as 5G-AKA authentication had not yet been completed. The AMF then sent a Security Mode Command (SMC) marked as "Integrity protected with new security context," specifying ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA1. Crucially, the SMC was sent *before* 5G-AKA authentication finalized, meaning no valid security context existed between the UE and AMF at this stage. The UE correctly rejected the SMC with a "Security mode rejected, unspecified" response, as 3GPP TS 33.501 mandates that NAS security (initiated via SMC) must only occur *after* successful 5G-AKA authentication establishes shared keys. By rejecting the premature SMC, the UE prevented potential security context activation without authentication, adhering to 5G standards that prioritize authentication-before-security-establishment to mitigate man-in-the-middle and replay attacks. 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 plaintext, as 5G-AKA authentication had not been completed. The AMF responded with a Security Mode Command (SMC), also sent in plaintext, specifying the ciphering algorithm 128-5G-EA2 for encryption but selecting the null integrity algorithm (5G-IA0), which provides no integrity protection. Despite the incomplete authentication and absence of established security keys, the UE did not reject the invalid SMC. Instead, it proceeded to send a Deregistration Request in plaintext, ignoring the SMC's encryption directive. According to 3GPP standards (TS 33.501), the UE must reject an SMC that mandates null integrity protection (as integrity is mandatory for secured NAS messages) and should never process security commands without a valid security context from completed 5G-AKA. By accepting the SMC with 5G-IA0 and transmitting sensitive messages without encryption or integrity checks, the UE violated core 5G security protocols. 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 began with the UE sending an Authentication Response as part of the 5G-AKA procedure, which was not yet completed. Immediately afterward, the AMF sent a Configuration Update Command (CUC) protected with integrity security (security header type 1). Crucially, the 5G-AKA process—which establishes the shared security context (K~AMF~) needed to validate such protected messages—had not concluded, as the Security Mode Command (SMC) step to activate ciphering and integrity protection was skipped. According to 3GPP TS 33.501 and TS 24.501, a UE without an active security context must reject protected NAS messages like the CUC by responding with a Security Mode Reject (cause #96, "invalid mandatory information") to prevent processing unverified commands. Here, the UE provided no response, failing to enforce this security requirement. This omission could allow malicious network elements to inject unauthorized configuration changes without detection, violating 3GPP's mutual authentication and message protection principles. Insecure

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 5G-AKA procedure, which was not yet completed. The AMF responded with a plain-text (unencrypted) Identity Request for the UE's IMEISV—a permanent equipment identifier. The UE did not respond to this request. According to 3GPP standards (TS 33.501), permanent identifiers like IMEISV must only be transmitted after NAS security is established via successful 5G-AKA, ensuring confidentiality and integrity. Since 5G-AKA was incomplete and the AMF's request lacked NAS security protections (encryption/integrity), the UE correctly refrained from disclosing its IMEISV. This adherence to protocol prevents potential tracking or eavesdropping attacks. 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 as part of the 5G-AKA procedure, which had not yet been completed. The AMF then sent a Service Accept message marked as "Protected," indicating it was encrypted and integrity-protected. Subsequently, the UE sent a Deregistration Request (UE originating) without any indication of protection. According to 3GPP standards (TS 33.501), NAS messages must only be protected *after* 5G-AKA successfully completes and security contexts are established via the Security Mode Command (SMC) procedure. Here, the AMF sent a protected Service Accept prematurely—before 5G-AKA finalized and without initiating SMC—which violates the protocol. Crucially, the UE accepted this protected message without a valid security context and proceeded to send a Deregistration Request in plaintext. This indicates the UE failed to enforce mandatory security checks: it should have rejected the protected Service Accept (as no security context existed) and initiated recovery actions, such as local deregistration or restarting authentication. By processing the protected message and continuing communication insecurely, the UE exposed itself to potential manipulation (e.g., accepting forged network commands), undermining mutual authentication and confidentiality guarantees. 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 to the AMF as part of the 5G-AKA procedure. However, before 5G-AKA could complete and establish a security context for encrypted NAS communication, the AMF responded with an unencrypted (plain) GMM Status message containing 5GMM Cause 26 ("Non-5G authentication unacceptable"). This cause indicates the network rejected the UE's authentication method, likely due to the use of non-5G credentials (e.g., EPS-AKA in a 5G standalone context). Critically, the UE provided no response to this plain-text GMM Status message. According to 3GPP standards (TS 24.501 and TS 33.501), NAS messages must be integrity-protected and encrypted once security is activated via the Security Mode Command (SMC). However, **before 5G-AKA completion and SMC exchange, messages are inherently unprotected**, and the UE is not obligated to respond to unauthenticated commands that could be maliciously injected. By ignoring the plain-text GMM Status message—which lacked cryptographic integrity checks—the UE avoided processing an unverified network instruction. Responding could have exposed vulnerabilities (e.g., revealing UE state or accepting rogue commands), whereas silence aligns with security best practices for unsecured phases. The UE's non-response demonstrates adherence to zero-trust principles during pre-security-context establishment, mitigating potential exploitation. 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 established a security context. Immediately after, the AMF sent a Deregistration Request message protected with both integrity protection and ciphering (security header type 2). According to 3GPP standards (TS 33.501), a UE must not process or respond to integrity-protected NAS messages before successfully completing 5G-AKA and validating the message's integrity with a fresh security context. Since 5G-AKA was incomplete, the UE lacked the necessary keys to verify the message's authenticity. The UE's lack of response indicates it discarded the message as required by the standard, avoiding potential processing of unverified commands. This aligns with security protocols designed to prevent attacks exploiting premature protected messages. 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.	After completing the 5G-AKA authentication, the UE sent a **Security Mode Complete** message (indicating activation of NAS security context), followed by an AMF **Identity Request** for IMEISV sent in plaintext. The UE provided no response. According to 3GPP 5G standards (TS 33.501), once the security context is established via Security Mode Command/Complete, all subsequent NAS messages—including Identity Request—**must** be integrity-protected and encrypted to prevent eavesdropping or manipulation. The UE's lack of response to this unprotected request aligns with standard security requirements: UEs must reject/ignore unsecured NAS messages after security activation to avoid potential exploits (e.g., fake requests or privacy leaks). Thus, the UE correctly enforced security protocols by discarding the plaintext demand. 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 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 (integrity protection and encryption) for subsequent communications. Following this, the AMF transmitted an Identity Request for the GUTI, but sent this message unprotected (in plaintext). The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once NAS security is activated via Security Mode Complete, all subsequent NAS messages—both uplink and downlink—must be protected. The UE is required to discard any unprotected NAS messages received after security activation, as they violate security protocols and may indicate manipulation. By ignoring the unprotected Identity Request, the UE adhered to this mandate, preventing potential exploitation of unprotected communications. 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 UE successfully completing 5G-AKA and sending a Security Mode Complete message, confirming the activation of NAS security (integrity protection and encryption). The AMF then responded with an unprotected Service Reject message (5GMM Cause #111: "Protocol error, unspecified"), violating 3GPP TS 24.501, which mandates that after security context establishment, all subsequent NAS messages—except specific exceptions like Authentication Requests—must be integrity-protected and encrypted. Despite this breach, the UE processed the unprotected Service Reject and initiated a Deregistration Request (UE originating). According to 3GPP standards, the UE should discard any NAS message lacking integrity protection once security is activated, as it cannot verify the message's authenticity or guard against tampering. By acting upon the unsecured Service Reject instead of ignoring it, the UE exposed itself to potential downgrade attacks or malicious network impersonation, undermining the security framework. Insecure
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 activation of the security context after 5G-AKA completion. The AMF then sent an Authentication Request in plain text (unencrypted and unprotected). According to 3GPP standards (TS 33.501), once the security context is established via Security Mode Complete, all subsequent NAS messages must be protected with integrity and encryption. The UE correctly ignored the unprotected Authentication Request, as processing it would violate mandatory security requirements and expose the system to potential downgrade attacks or malicious injections. By not responding, the UE adhered to protocol mandates that prioritize rejecting unprotected communications after security activation, thereby maintaining the integrity of the session. 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 AMF. The UE then sent a Security Mode Complete message, confirming activation of NAS security (integrity protection and encryption) as mandated by 3GPP TS 33.501. Subsequently, the AMF sent a Service Accept message in plaintext (unencrypted and without integrity protection). The UE exhibited no response to this message. According to 5G standards, after security activation, all NAS messages—including Service Accept—must be encrypted and integrity-protected to prevent eavesdropping and tampering. The UE's lack of response aligns with security requirements, as processing or acknowledging an unprotected post-security-activation message could expose vulnerabilities. By ignoring the plaintext Service Accept, the UE avoided potential security risks like accepting forged network instructions, demonstrating adherence to 3GPP safeguards. Secure
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 successfully completing 5G-AKA authentication and sending a Registration Complete message to the AMF, indicating the establishment of a secure NAS security context as per 3GPP standards. The AMF then responded with an Identity Request for SUCI, explicitly sent in plaintext without encryption or integrity protection. The UE correctly provided no response to this request. According to 3GPP TS 33.501, after security context establishment (confirmed by 5G-AKA completion), all subsequent NAS messages—including Identity Request—**must** be integrity-protected and ciphering-enabled to prevent eavesdropping or manipulation. The UE's silence aligns with standard-mandated behavior: rejecting unprotected NAS messages post-authentication to avoid potential security exploits (e.g., false credential harvesting). This non-response upholds confidentiality and protocol integrity requirements. Secure

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 process. Subsequently, the AMF sent an Authentication Request containing RAND, AUTN, and security parameters (ngKSI) in plaintext, as no security context was active at this stage. Critically, the UE did not respond to this request. According to 3GPP standards (TS 33.501), after Registration Complete is sent, the UE should have an established security context from prior 5G-AKA completion, and all subsequent NAS messages must be integrity-protected and encrypted. The AMF's plaintext Authentication Request post-registration violates this requirement, as it should only initiate authentication during initial registration setup—not after its completion. The UE's lack of response aligns with standard security protocols: it correctly discarded the unprotected, out-of-sequence message, avoiding processing potentially malicious or replayed authentication challenges. This behavior prevents security context disruption and upholds NAS layer protection mandates. 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.	The interaction began with the UE completing 5G-AKA and sending a Registration Complete message, confirming mutual authentication and establishing a secure NAS context. The AMF then sent an Identity Request for SUCI in plaintext (unencrypted). Crucially, after security activation via 5G-AKA, 3GPP standards (TS 33.501) mandate that all subsequent NAS messages must be integrity-protected and encrypted to prevent eavesdropping or manipulation. Instead of ignoring this unprotected request—as required by the standard—the UE processed it and responded with a Deregistration Request (UE originating). By acting upon an unsecured command, the UE violated 5G security protocols, which prohibit processing unprotected NAS messages post-authentication. This exposes a vulnerability where an attacker could inject plaintext requests to trigger unexpected actions like deregistration, potentially disrupting service or enabling denial-of-service attacks. Insecure

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 security context between the UE and AMF. The UE sent a protected Registration Complete message, as expected after authentication. Subsequently, the AMF transmitted a Configuration Update Command as a plain (unprotected) NAS message, indicated by the security header type "0". Per 3GPP TS 24.501, once a NAS security context exists (post-5G-AKA), the UE must reject all unprotected NAS messages except specific exceptions like Authentication Request or Identity Request. The Configuration Update Command is not among these exceptions. However, instead of discarding the unprotected message or initiating a security recovery procedure, the UE responded with a Deregistration Request (UE originating). This action indicates the UE processed the unprotected command, violating 3GPP security requirements (Section 4.4.4.3), which mandate ignoring such messages to prevent manipulation by attackers. By acting upon an unverified plaintext command, the UE exposed itself to potential spoofing attacks (e.g., forced deregistration), undermining NAS security principles. 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 NAS security context, and sending a UL NAS Transport (including a Registration Complete and PDU Session Establishment Request). The AMF responded with two consecutive Downlink NAS Transport messages carrying a Configuration Update Command, both sent as plain text (security header type 0), despite the existing security context. Subsequently, the UE initiated deregistration by sending a UL NAS Transport containing a Deregistration Request (UE originating). According to 3GPP standards (TS 24.501), once NAS security is established via 5G-AKA, all subsequent NAS messages—including Deregistration Requests—must be integrity-protected and encrypted, with only narrow exceptions (e.g., specific authentication or security mode messages). The Configuration Update Command is permitted in plain text only if limited to network name updates; however, the UE must still enforce security for its own transmissions. Here, the UE sent a sensitive Deregistration Request (exposing identifiers like SUPI/5G-GUTI) without applying NAS security, violating 3GPP mandates. This lapse could enable eavesdropping or impersonation attacks, indicating non-compliance with 5G security protocols. 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, including Registration Complete and a PDU Session Establishment Request, indicating it considered the registration procedure complete. The AMF then responded with a Configuration Update Command and an Authentication Request, the latter containing RAND, AUTN, and ABBA parameters for 5G-AKA authentication, sent in plain text. According to 3GPP standards (TS 33.501), initial authentication messages like Authentication Request may be sent unprotected before security activation. However, the UE had already sent Registration Complete, implying it had progressed beyond initial registration and likely established a security context. After receiving the Authentication Request, the UE provided no response—neither an Authentication Response nor an Authentication Failure message. This violates 3GPP TS 24.501, which mandates that UEs must process authentication requests and reply appropriately, even during re-authentication scenarios. The lack of response leaves the network without confirmation of UE legitimacy or failure reasons, potentially allowing session hijacking or desynchronization attacks. Thus, the UE's failure to respond constitutes a protocol deviation and undermines the security integrity of the session. 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 NAS context. The UE then sent a protected UL NAS Transport message containing multiple requests (Registration Complete, PDU Session Establishment, and Deregistration). The AMF responded with an unprotected Service Reject message (5GMM Cause 111: "Protocol error, unspecified"), violating the 3GPP security requirement (TS 24.501, Section 4.4.4) that mandates all NAS messages after 5G-AKA must be integrity-protected and encrypted. The UE took no action upon receiving this unprotected message, failing to detect or respond to the security violation. According to 3GPP standards, the UE should have discarded the unprotected Service Reject and potentially initiated recovery procedures (e.g., re-registration) to mitigate potential attacks like downgrade or manipulation. The UE's passive acceptance of an unprotected message post-authentication constitutes a security flaw, as it undermines the confidentiality and integrity safeguards enforced by the 5G security architecture. Insecure

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 message containing Registration Complete and a PDU Session Establishment Request, indicating the completion of initial registration and an attempt to establish a session. Subsequently, the AMF sent a Configuration Update Command followed by an Authentication Request in plaintext (unencrypted), which included RAND and AUTN parameters for re-authentication. Notably, this occurred after the initial 5G-AKA was marked as completed, and the UE had already established a security context. The UE responded with a Deregistration Request (UE originating) instead of the expected Authentication Response or Authentication Failure message. According to 3GPP standards (TS 33.501), after security context establishment, unprotected NAS messages like the Authentication Request are permissible only when initiating a new authentication procedure. However, the UE should process such requests by verifying the AUTN and responding appropriately (e.g., with Authentication Response or Failure). Deregistration as a reaction to a valid re-authentication attempt deviates from protocol requirements, indicating improper handling that could facilitate denial-of-service attacks by forcing unnecessary deregistration upon receiving forged or unexpected authentication requests. 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 UE sending a UL NAS Transport (Registration Complete and PDU Session Establishment Request) after completing 5G-AKA, which establishes a security context for encrypted/integrity-protected NAS messaging. The AMF responded with a plaintext (unencrypted) Identity Request for the UE's IMEI. Instead of ignoring this unprotected request—as mandated by 3GPP TS 33.501 (Section 6.4) for security-sensitive commands after authentication—the UE sent a Deregistration Request. This action deviates from the standard, which requires UEs to reject unsecured Identity Requests to prevent potential identity harvesting by attackers. The UE's non-compliant response indicates it processed an unprotected security command, violating 3GPP safeguards. Insecure
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 sending an Uplink NAS Transport message, including Registration Complete and a PDU Session Establishment Request, following a completed 5G-AKA authentication. The AMF responded with two downlink messages: first, a Configuration Update Command (acknowledgment details noted), and then a Registration Reject with 5GMM Cause #62 ("No network slices available"), explicitly sent in plaintext without encryption or integrity protection. The UE exhibited no response to these messages. According to 3GPP standards (TS 24.501, TS 33.501), after successful 5G-AKA, all subsequent NAS messages—including reject messages like Registration Reject—must be confidentiality and integrity protected using the established security context. The AMF's transmission of a critical service-denial message (Registration Reject) in plaintext violates this requirement, as it exposes the UE to forgery or manipulation by attackers. Crucially, the UE's lack of reaction—failing to discard the unprotected message, trigger a security error, or initiate recovery procedures—demonstrates non-compliance with 3GPP's security mandates. This inaction implies acceptance of an illegitimate plaintext command, undermining the confidentiality and integrity safeguards enforced by 5G-AKA. Insecure

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.	The interaction began with the UE sending an unprotected UL NAS Transport (PDU session establishment request) after completing 5G-AKA. The AMF responded with an unprotected Security Mode Command (SMC), specifying ciphering (5G-EA6) and integrity (128-5G-IA1) algorithms. Instead of replying with a **Security Mode Complete** message—which should be the first integrity-protected and ciphering-enabled response per 3GPP TS 24.501—the UE sent an unprotected Deregistration Request without activating security. This violates the 5G security protocol, which mandates that after receiving the SMC, the UE must activate NAS security and confirm it via a protected Security Mode Complete. By sending a sensitive deregistration request in plaintext without completing this step, the UE exposed itself to tampering or spoofing attacks, as the message lacks integrity protection and confidentiality. 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 an Uplink NAS Transport message after completing 5G-AKA authentication, which establishes a security context for encrypted/integrity-protected communication. The AMF then responded with two downlink messages: a Configuration Update Command and an Identity Request for the IMEISV. Critically, the Identity Request was sent in plaintext (unencrypted), violating the 5G security standard (3GPP TS 33.501), which mandates that all NAS messages must be integrity-protected and encrypted after 5G-AKA completion to prevent eavesdropping or manipulation. The UE correctly ignored the Identity Request, as processing unsecured post-authentication messages would expose it to attacks like impersonation or data leakage. This aligns with 3GPP requirements that UEs reject unprotected NAS commands once a security context is active. The UE's non-response demonstrates adherence to security protocols by refusing to engage with non-compliant network instructions. 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 a completed 5G-AKA authentication, establishing a secure NAS context. The UE then sent a Service Request (uplink), expecting encrypted/integrity-protected messaging per 3GPP TS 24.501. However, the AMF responded with a Deregistration Accept message (downlink) sent in plaintext without encryption or integrity protection. Critically, the UE exhibited no response to this unsecured message. According to 3GPP standards (TS 33.501, Section 6.4), after 5G-AKA completion, all NAS messages—except specific initial procedures—must be confidentiality and integrity protected. The Deregistration Accept falls outside these exceptions and must be secured. The UE's failure to reject or challenge this unprotected message violates core 5G security principles, as it could allow threat actors to inject forged deregistration commands, disrupt sessions, or force re-authentication. Insecure
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 via an InitialUEMessage in plain text, as NAS security had not yet been activated post-5G-AKA. The AMF responded with a Security Mode Command (also sent in plain text, as required by the 3GPP standard for this initial security activation step), specifying the 5G-EA6 ciphering algorithm and 128-5G-IA2 integrity algorithm for subsequent protected communications. However, the UE failed to respond to this command—neither acknowledging acceptance (via Security Mode Complete) nor rejecting it (via Security Mode Reject). According to 3GPP TS 24.501 and TS 33.501, upon receiving a Security Mode Command, the UE must validate the proposed algorithms and respond to activate NAS security; silence violates protocol. This inaction leaves the security context unestablished, meaning subsequent messages remain unprotected and vulnerable to interception or manipulation. The UE's failure to engage in this critical handshake undermines the security framework. Insecure

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 an unprotected Service Request via an InitialUEMessage to the AMF, which is standard behavior since no security context existed at this initial stage. The AMF responded with an Authentication Request containing RAND and AUTN for 5G-AKA initiation, sent in plaintext as required by 3GPP, given the absence of an established security context. However, the UE failed to respond to this challenge, deviating from the 5G standard (3GPP TS 33.501), which mandates that the UE must process the AUTN and reply with either an Authentication Response (if valid) or an Authentication Failure message (e.g., for MAC/synchronization errors). This lack of response leaves the network in an ambiguous state, potentially masking security issues like authentication failures or attacks, and violates protocol expectations for handling authentication challenges. Consequently, the UE's inaction is non-compliant and insecure. 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 initiate communication. The AMF responded with a plain-text Authentication Request containing RAND, AUTN, and ngKSI=4 (indicating a native security context). Instead of processing the authentication challenge, the UE immediately replied with an Authentication Failure message, explicitly citing "ngKSI already in use" as the cause. This indicates the UE detected that the ngKSI value 4 was already associated with an active security context on the device. According to 3GPP standards (TS 33.501), reusing an ngKSI for a new authentication attempt while an existing context is still valid constitutes a security risk, as it could enable context confusion or replay attacks. The UE's rejection of the request aligns precisely with mandated behavior defined in section 6.1.3, which requires UEs to terminate the procedure and report "ngKSI already in use" in such scenarios. By doing so, the UE prevented potential security context overriding or key reuse vulnerabilities. The response was appropriate given the plain-text delivery of the request (as 5G-AKA wasn't yet complete, encryption wasn't required), and the UE adhered to protocol-specified failure handling without exposing sensitive data. 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.	The interaction began with the UE sending a Service Request to the AMF after 5G-AKA completion, which established a security context. The Service Request, as per 5G standards, is permitted to be sent without encryption but must include integrity protection to prevent tampering. Subsequently, the AMF responded with an Identity Request for the TMSI, explicitly sent in plaintext without encryption or integrity protection. The UE did not respond to this request. According to 3GPP standards (e.g., TS 33.501), once 5G-AKA is complete and a security context is active, all NAS messages—except specific exceptions like the initial Service Request—must be both integrity-protected and encrypted. The Identity Request does not qualify as an exception, as it may contain sensitive information or directives requiring confidentiality and authenticity. By ignoring the unprotected Identity Request, the UE correctly adhered to security protocols, avoiding potential exposure to eavesdropping, spoofing, or manipulation of identity-related data. This behavior aligns with 3GPP mandates that devices must reject unsecured NAS messages after security activation to maintain session integrity. 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 after 5G-AKA authentication had been completed, establishing a security context. The AMF responded with a Configuration Update Command message, which was marked as "Protected" in the test summary but carried an "Unknown" security header. Critically, the UE provided no response to this message. According to 3GPP standards (TS 24.501 and TS 33.501), after successful 5G-AKA, all subsequent NAS messages—including Configuration Update Command—must be integrity-protected and may be encrypted. The UE is required to validate the security header and integrity of such messages. An "Unknown" security header suggests potential misalignment or improper protection (e.g., incorrect security context, missing integrity protection, or malformed formatting). The UE's lack of response—neither acknowledging the message nor triggering a security recovery procedure (e.g., re-authentication or registration)—indicates it failed to enforce mandatory security checks. This omission violates 3GPP requirements, as a properly secured UE must reject unprotected or integrity-check-failing messages and initiate countermeasures to maintain security continuity. Insecure
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 began with the UE initiating a Service Request after completing the 5G-AKA procedure, which should have established a valid NAS security context for encrypted and integrity-protected communication. However, the AMF responded with an Authentication Reject message sent in plaintext (unencrypted and without integrity protection). According to 3GPP standards (TS 24.501, clause 4.4.4.3 and 5.4.1.2), the Authentication Reject is explicitly permitted to be sent unprotected, even after security context establishment, as it invalidates the security context and forces the UE to transition to a deregistered state. The UE's lack of response aligns with the standard, as no reply is mandated upon receiving this message. The UE is expected to locally delete stored security keys (e.g., K~AMF~), 5G-GUTI, and related parameters without further action. Since the UE adhered to this protocol—accepting the unprotected reject only for this specific message type and silently terminating the session—its behavior complies with 3GPP security provisions. Secure

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 via an InitialUEMessage (unprotected, as RRC security was not yet active). After 5G-AKA completion—which establishes mutual authentication and NAS security keys—the AMF responded with an unprotected (plain) Identity Request message demanding SUCI. The UE complied by sending an Identity Response. According to 3GPP TS 33.501, after successful 5G-AKA, all NAS messages **must** be integrity-protected and encrypted to prevent eavesdropping or manipulation, barring explicitly allowed exceptions (e.g., initial Registration Request). The Identity Request is not an exempted message in this context, as security context already existed. The UE's failure to reject the unprotected Identity Request—instead processing it and responding—violates the standard. This exposes the UE to risks like malicious network impersonation or privacy leaks (e.g., forcing unnecessary SUCI disclosure). Thus, the UE acted insecurely by not enforcing mandatory NAS protection post-authentication. 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 communication by sending a Service Request to the AMF after completing 5G-AKA, which establishes a security context. The AMF responded with a Configuration Update Command, which was indicated as "Protected" in the test summary, implying it should have been integrity-protected and encrypted per 5G standards (3GPP TS 24.501). However, the UE failed to respond to this command—neither acknowledging it with a Configuration Update Complete nor initiating recovery procedures (e.g., re-authentication) despite the security context being active. According to 3GPP, a UE must either process valid protected NAS messages (responding appropriately) or, if integrity checks fail, trigger countermeasures like re-registration to maintain security continuity. The UE's lack of any reaction—ignoring the command without rejection or recovery efforts—deviates from protocol requirements, leaving the session unacknowledged and potentially exposing the system to unaddressed security risks (e.g., accepting malformed updates or stalling security synchronization). This non-compliant behavior indicates a failure to enforce mandatory security validation and response mechanisms. Insecure

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) (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, which is standard before security establishment. However, before completing the 5G-AKA authentication procedure—a prerequisite for deriving security keys—the AMF sent a Deregistration Request (UE-terminated) that was marked as "Protected" (security header type 2, indicating integrity protection and ciphering). Since 5G-AKA had not been finalized, the UE lacked the necessary keys to verify the message's integrity or decrypt its content. Per 3GPP TS 33.501, a UE must reject protected NAS messages received without an established security context, as they cannot be authenticated. The UE's lack of response aligns with this requirement, as processing an unverifiable protected message could expose it to spoofing or forced deregistration attacks. By ignoring the message, the UE adhered to security protocols, preventing potential exploitation. 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 successful completion of 5G-AKA authentication, establishing shared keys for security. The UE then sent a Security Mode Complete message, confirming activation of NAS security (encryption and integrity protection) as required after 5G-AKA. Subsequently, the AMF sent an Identity Request for the GUTI in plaintext (unencrypted and unprotected). The UE provided no response 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 negotiated security context. The UE correctly ignored the unprotected Identity Request, as accepting or processing it would violate security protocols by exposing sensitive data or enabling downgrade attacks. This adherence to discarding unsecured post-authentication messages aligns with 5G security requirements. 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.	The interaction began with the UE sending a Security Mode Complete message, confirming successful activation of security context after 5G-AKA authentication. Subsequently, the AMF transmitted an Identity Request (for IMEISV) in plaintext, without encryption or integrity protection. According to 3GPP 5G standards (TS 33.501), once NAS security is established—indicated by the Security Mode Complete—all subsequent NAS messages must be integrity-protected and encrypted if confidentiality is negotiated. The UE's lack of response to this unprotected Identity Request aligns with security requirements: accepting or processing an unsecured post-authentication message would violate core security principles, as it could enable spoofing or information leakage. By discarding the unauthenticated request, the UE correctly enforced security protocols, preventing potential exploitation by rogue network elements. 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 the security context following 5G-AKA authentication. Subsequently, the AMF transmitted an Identity Request (for SUCI) in plaintext, without encryption or integrity protection. The UE provided no response to this request. According to 3GPP standards (TS 33.501), once NAS security is activated (after Security Mode Complete), all subsequent NAS messages—including downlink messages like Identity Request—must be integrity-protected and encrypted if confidentiality is required. The UE's receipt of an unprotected message after security activation violates this requirement, as unprotected messages are vulnerable to tampering and forgery. The standard mandates that UEs must discard such unprotected messages to prevent security downgrade attacks. By ignoring the plaintext Identity Request, the UE correctly adhered to security protocols, avoiding potential exploitation through unverified commands. 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 completing the 5G-AKA authentication and sending a Security Mode Complete message to the AMF, confirming the activation of the negotiated security context for NAS communication. Subsequently, the AMF transmitted an Identity Request for the UE's IMEI in plaintext (unencrypted and unprotected). The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once the Security Mode Complete is sent, the UE has activated its security context, and all subsequent NAS messages must be integrity-protected and encrypted unless explicitly exempt (e.g., specific mobility management messages during initial registration). The Identity Request for IMEI is not among these exemptions after security activation. The UE correctly identified the unprotected request as non-compliant with the established security context and discarded it, avoiding potential exposure of sensitive identity data (IMEI) in plaintext. By ignoring the request, the UE adhered to security protocols that mandate rejection of unprotected messages post-security activation, preventing man-in-the-middle or information-leakage attacks. This behavior aligns with 3GPP requirements for discarding non-compliant messages without response (e.g., to avoid signaling storms or side-channel leaks), thus maintaining confidentiality and protocol integrity. 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.	After the completion of 5G-AKA, which establishes a security context, the UE sent a Security Mode Complete message (indicating successful activation of security algorithms) followed by a Registration Request. The AMF responded with an Identity Request for SUCI, sent in plaintext without encryption or integrity protection. According to 3GPP TS 24.501, once NAS security is activated (post-Security Mode Complete), the UE must reject any unprotected NAS messages except specific exceptions like Service Reject or Authentication Reject. The Identity Request is not among these exceptions. The UE correctly ignored this unprotected request, as processing it could expose sensitive data or enable downgrade attacks. This adherence to security policies—rejecting non-compliant messages—aligns with 5G standards. 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.	After completing the 5G-AKA authentication and security mode procedure, the UE sent a **Security Mode Complete** message (indicating successful activation of security contexts) followed immediately by a **Registration Request**. The AMF responded with an **Identity Request** for the UE's GUTI, transmitted in **plain text** without encryption or integrity protection. The UE provided **no response** to this request. According to 3GPP standards (TS 33.501), once 5G-AKA and the Security Mode Command procedure are completed, all subsequent NAS messages—including Identity Requests—**must be encrypted and integrity-protected** using the established security context. The Identity Request is not among the few exceptions (e.g., initial service requests) permitted in plain text post-security activation. By ignoring the unprotected Identity Request, the UE correctly adhered to 3GPP security requirements, as processing such a message could expose it to eavesdropping, spoofing, or identity-harvesting attacks. The lack of response demonstrates the UE's compliance with mandatory security enforcement. 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.	The interaction began with the UE successfully completing the 5G-AKA authentication, establishing a security context. The UE then sent a Security Mode Complete message, confirming the activation of NAS security (integrity protection and encryption) as per the negotiated security algorithms. Subsequently, the AMF sent an Identity Request for the IMEISV 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 via the Security Mode Command procedure, all subsequent NAS messages must be integrity-protected and encrypted if confidentiality is enabled. The UE is mandated to discard any unprotected NAS messages received after security activation to prevent potential attacks, such as downgrade or injection attempts. By ignoring the unprotected Identity Request, the UE adhered to this requirement, demonstrating correct security behavior. 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 successfully completing 5G-AKA, establishing a security context, and sending a Registration Complete message. 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 and TS 24.501), once 5G-AKA is completed and a security context is active, all NAS messages—including Identity Request—must be integrity-protected and encrypted to prevent eavesdropping, tampering, or replay attacks. The AMF's transmission of a post-authentication Identity Request in plaintext violates this requirement. The UE's lack of response aligns with security protocols, as it should reject unprotected messages after security context establishment. This behavior prevents potential exploitation (e.g., forced re-identification via spoofed requests) and upholds the standard's confidentiality and integrity mandates. 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.	The interaction began with the UE successfully completing 5G-AKA authentication and sending a Registration Complete message to the AMF. The AMF then responded with an Identity Request message, explicitly requesting the SUCI identity, which was transmitted in plain text without encryption or integrity protection. Crucially, the UE provided no response to this request. According to 3GPP security standards (TS 33.501), after 5G-AKA completion, all subsequent Non-Access Stratum (NAS) messages must be confidentiality and integrity protected using the established security context. The AMF's transmission of the Identity Request in plain text violates this requirement, as post-authentication messages must be secured. The UE's lack of response aligns with 3GPP specifications, which mandate that UEs must ignore or reject unprotected NAS messages once a security context is active, preventing potential exploits like manipulation or eavesdropping. By refusing to process the unprotected request, the UE adhered to security protocols. 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 after the successful completion of 5G-AKA, establishing a secure context between the UE and AMF. The UE sent an encrypted Registration Complete message, as required post-authentication. However, the AMF then transmitted an Identity Request for SUCI in plaintext (unencrypted) at 2.019s and again at 3.000s. The UE did not respond to these requests. According to 3GPP standards (TS 33.501), once 5G-AKA completes and a security context is established, 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 security requirements, as processing an unprotected Identity Request after authentication would violate 3GPP mandates (Section 6.4). The UE correctly ignored the non-compliant messages, avoiding potential exposure of sensitive identity information. 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, establishing a security context, and sending a protected Registration Complete message to the AMF. The AMF then responded with an Identity Request message, explicitly asking for the UE's SUCI (Subscription Concealed Identifier), but transmitted this message in plaintext without encryption or integrity protection. Despite this request, the UE provided no response. According to 3GPP standards (TS 33.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages—including Identity Requests—must be confidentiality and integrity protected to prevent eavesdropping, tampering, or identity compromise. The UE's failure to respond aligns with security requirements, as processing an unprotected message after security activation could expose sensitive information (like SUCI) and violate protocol mandates. By ignoring the unprotected request, the UE avoided potential security risks such as identity leakage or man-in-the-middle attacks, demonstrating adherence to 5G security protocols. 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 involved the UE sending a Registration Complete message (protected, as 5G-AKA was completed) followed by a PDU session establishment request. Subsequently, the AMF sent an unprotected Identity Request for SUCI. According to 3GPP standards (TS 33.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages—including those from the network—must be integrity-protected and encrypted to prevent eavesdropping and tampering. The UE's failure to respond to the unprotected Identity Request aligns with 5G security requirements: UEs must discard any non-integrity-protected NAS messages received after security activation, as they could be malicious injections. By ignoring this plaintext request, the UE correctly prioritized security enforcement over compliance, avoiding potential exploitation of unprotected communication. 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 completing the 5G-AKA authentication, establishing a secure context, and sending a Registration Complete message (which should be protected per the security context). Immediately after, the AMF sent an Identity Request for SUCI in plaintext (unencrypted and without 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 secure NAS context is established, all subsequent NAS messages—including post-registration commands like Identity Request—must be confidentiality and integrity protected to prevent eavesdropping, tampering, and privacy breaches. The UE's lack of response to the unprotected Identity Request aligns with these requirements, as processing or responding to an unprotected message after security activation would violate security protocols and expose the UE to risks like identity tracking or replay attacks. By ignoring the request, the UE correctly enforced security policies, demonstrating adherence to 5G standards. 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.	The interaction began with the UE completing 5G-AKA authentication, establishing a secure NAS context. The UE then sent a Registration Complete message to the AMF. Subsequently, the AMF transmitted an Identity Request (plaintext, unprotected) for the UE's TMSI. The UE did not respond to this request. According to 3GPP standards (TS 33.501), after 5G-AKA completion, all NAS messages must be integrity-protected to prevent forgery or tampering. Encryption is optional but integrity protection is mandatory. The AMF's Identity Request, sent unprotected, violates this requirement. The UE's lack of response aligns with security protocols, as it should discard unprotected messages once a security context is active. Ignoring such requests mitigates risks like location tracking or denial-of-service via forged commands. Thus, the UE's action was correct and adherent to 5G security principles. 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.	After completing the 5G-AKA authentication procedure, which establishes a secure NAS context, the UE initiated a PDU session setup via an UL NAS TRANSPORT message. The AMF responded with an Identity Request for the IMEISV, transmitted in plaintext without encryption or integrity protection. Per 3GPP TS 33.501 and TS 24.501, once 5G-AKA completes and a security context is active (as confirmed here), all subsequent NAS messages—including Identity Requests—**must** be confidentiality-protected and integrity-protected to mitigate eavesdropping, spoofing, and privacy breaches. The UE correctly discarded the unprotected Identity Request by not responding, adhering to the standard's security requirements. This behavior prevents potential exploitation of unsecured identity disclosures and maintains protocol compliance. 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 with the successful completion of 5G-AKA, establishing a secure context between the UE and AMF. The UE then initiated a PDU session setup via an Uplink NAS Transport message. Subsequently, the AMF sent an Identity Request demanding the SUCI, but transmitted this message in plaintext without leveraging the established security context (integrity protection or encryption). The UE did not respond to this request. According to 3GPP standards (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages—including Identity Requests—must be integrity-protected and encrypted to prevent eavesdropping or manipulation. The UE's failure to respond aligns with the standard's security requirements, as it correctly rejected an unprotected message that should have been secured, thereby avoiding potential exposure of sensitive identity information (SUCI/SUPI) or acceptance of unauthorized commands. This behavior demonstrates adherence to 5G security protocols. 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 successful completion of 5G-AKA, establishing a mutual security context between the UE and AMF. The UE initiated communication by sending an encrypted Uplink NAS Transport message containing a PDU session establishment request, adhering to 5G security protocols. Subsequently, the AMF sent an Identity Request for the TMSI identity in plaintext (unencrypted and without 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, all NAS messages must be confidentiality and integrity protected to prevent eavesdropping and tampering. The Identity Request, while not containing highly sensitive data itself, is subject to these mandatory security protections after security context establishment. The UE's lack of response demonstrates compliance with the standard, as processing an unprotected NAS message would violate security requirements. By discarding the unsecured request, the UE avoided potential risks like message injection or manipulation, maintaining protocol integrity. 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.	After completing the 5G-AKA authentication, the UE sent a UL NAS Transport (including Registration Complete and PDU Session Establishment Request). The AMF responded with a Configuration Update Command and an Identity Request for the IMEISV, both sent as plain/unprotected downlink NAS messages. Since 5G-AKA had already established a security context (requiring subsequent NAS messages to be encrypted and integrity-protected per 3GPP TS 33.501), the UE correctly ignored the unprotected Identity Request. The standard mandates that UEs discard non-integrity-protected NAS messages after security activation to prevent manipulation by attackers. By not responding, the UE adhered to security protocols, avoiding potential exploitation (e.g., spoofed identity requests). The Configuration Update Command's plaintext delivery further violates security norms but does not alter the UE's correct handling of the Identity Request. 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 sending an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request, following the completion of 5G-AKA, which establishes a secure NAS signaling context. Subsequently, the AMF sent two downlink messages: a Configuration Update Command (whose protection status is unspecified) and an Identity Request for SUCI, explicitly noted as sent "Plain" (unencrypted and without integrity protection). The UE provided no response to the Identity Request. According to 3GPP standards (TS 33.501), after 5G-AKA completion, all NAS messages—except specific exceptions like initial Identity Requests during initial registration—must be confidentiality and integrity protected. The Identity Request here occurred post-authentication and post-Registration Complete, meaning the secure context was active. An unprotected Identity Request at this stage is non-compliant, as it risks interception or forgery. The UE's lack of response aligns with security requirements: rejecting unprotected commands post-authentication prevents potential exploits (e.g., false identity requests). Thus, the UE correctly prioritized security by ignoring the unsecured message. 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 after the successful completion of 5G-AKA, which establishes a security context between the UE and AMF. The UE sent an encrypted UL NAS TRANSPORT containing Registration Complete and PDU Session Establishment Request. Subsequently, the AMF sent two downlink messages: first a Configuration Update Command (protection status unspecified), followed by an Identity Request explicitly sent in plaintext (unencrypted and unprotected), demanding the UE's IMEISV. The UE did not respond to the Identity Request. According to 3GPP 5G security standards (TS 33.501), once 5G-AKA completes and a security context is established, all NAS messages **must** be integrity-protected and encrypted to prevent eavesdropping or manipulation. The AMF's plaintext Identity Request violates this requirement, as sensitive identity requests (like IMEISV) must be sent securely after authentication. The UE correctly ignored this unprotected request, adhering to the standard's mandate to reject unsecured NAS messages post-security-context establishment. This prevents potential attacks where an adversary could harvest identity data via unprotected downlink messages. 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.	After the successful completion of the 5G-AKA authentication, which establishes a secure context for NAS communication, the UE sent an Uplink NAS Transport message containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Downlink NAS Transport message containing an Identity Request for the TMSI, sent in plaintext without encryption or integrity protection. The UE did not respond to this request. According to 3GPP security standards (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages must be confidentiality and integrity protected to prevent eavesdropping and tampering. The AMF's transmission of the Identity Request in plaintext violates this requirement, as sensitive identity requests must be secured after authentication. The UE’s lack of response aligns with the standard’s security protocols, as it should reject unprotected NAS messages after security context establishment to avoid potential attacks like identity harvesting or manipulation. 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.	After completing the 5G-AKA authentication, which establishes mutual authentication and security keys for encryption/integrity protection, the UE sent a protected UL NAS Transport (PDU session establishment request). The AMF responded with an Identity Request message (requesting TMSI) sent in plaintext without encryption or integrity protection. The UE correctly ignored this request, as no response was observed. According to 3GPP standards (TS 33.501, TS 24.501), after 5G-AKA completion, all subsequent NAS messages—including Identity Request—must be integrity-protected to prevent tampering and spoofing. The AMF's plaintext transmission violates this requirement, as Identity Request is not among the few exceptions (e.g., authentication messages) allowed without protection. The UE's silent discard of the unprotected message aligns with 3GPP-mandated behavior (Section 4.4.4.2), mitigating potential replay or manipulation attacks. Thus, the UE adhered to security protocols. 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 successful completion of 5G-AKA, establishing a mutual authentication and security context between the UE and AMF. The UE then initiated a PDU session establishment via an Uplink NAS Transport message. Subsequently, the AMF sent an Identity Request message in plaintext (unencrypted and without integrity protection), explicitly requesting the UE's TMSI. The UE provided no response to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA completes and a security context is established, **all subsequent NAS messages must be confidentiality- and integrity-protected**, with extremely limited exceptions. An Identity Request falls under this mandatory protection requirement when security context exists, as it could expose sensitive subscriber identifiers (like TMSI) to eavesdropping or manipulation. The UE's lack of response aligns precisely with 3GPP mandates: upon receiving an unprotected NAS message post-security-context establishment, the UE must discard the message and may terminate the connection to prevent potential attacks (e.g., identity harvesting or downgrade attempts). By ignoring the unsecured Identity Request, the UE adhered to protocol-specified security measures, demonstrating robust compliance. Secure

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 initiating a Service Request via an InitialUEMessage after completing 5G-AKA authentication. The AMF responded with a Service Accept message, which was transmitted in plaintext (unencrypted and without integrity protection) as indicated in the test summary and packet capture. According to 3GPP standards (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages—including Service Accept—must be confidentiality-protected (encrypted) and integrity-protected to safeguard against eavesdropping and tampering. The UE's lack of response to this unprotected Service Accept message demonstrates that it processed the message despite the absence of mandatory security mechanisms. This violates 3GPP security requirements, which mandate that UEs must reject unsecured NAS messages after security context establishment. By accepting the plaintext message without protest or error indication, the UE failed to enforce critical security protocols, exposing the communication to potential attacks such as interception or manipulation. 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 a Service Request after completing 5G-AKA authentication, which established a security context. The AMF responded with a Service Accept message sent in plaintext (unprotected). According to 3GPP standards (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages—including Service Accept—must be integrity-protected and encrypted using the negotiated security context to prevent eavesdropping, tampering, or replay attacks. The UE's failure to reject or respond to this unprotected Service Accept message violates this requirement, as it should have detected the absence of security and initiated countermeasures (e.g., aborting the session or triggering re-authentication). This omission indicates the UE did not enforce mandatory post-authentication security protocols. 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 sending a Service Request (uplink) after completing 5G-AKA, indicating an established security context. The AMF responded with a Service Reject (downlink) sent in plaintext (unencrypted and unprotected), including 5GMM cause #9 ("UE identity cannot be derived by the network"). The UE did not respond to this message. According to 3GPP standards (TS 24.501 and TS 33.501), once 5G-AKA completes, all subsequent NAS messages—except specific initial unauthenticated procedures—must be integrity-protected and encrypted to prevent downgrade attacks and eavesdropping. The Service Reject is not an exempted message, and its transmission in plaintext violates this requirement. The UE's failure to respond or reject this unprotected message—such as by initiating a re-registration or resetting the security context—constitutes a security lapse. It indicates the UE did not enforce mandatory post-authentication message protection, leaving it vulnerable to man-in-the-middle attacks where an adversary could forge unprotected reject messages to disrupt service. 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 with the UE sending a Service Request (encrypted, as 5G-AKA was completed) to initiate communication. The AMF responded with an unencrypted Service Reject containing 5GMM Cause #9 ("UE identity cannot be derived by the network"), indicating the AMF failed to identify the UE using its temporary identifier. The UE correctly provided no response to this reject. According to 3GPP TS 24.501, Cause #9 explicitly permits the AMF to send Service Reject unprotected since the security context cannot be established without UE identification. The UE's silence aligns with standard expectations: it must treat the current cell as unsuitable, discard the invalid temporary identity, and initiate recovery (e.g., re-registration) instead of reacting to the unprotected message. This prevents potential security risks like processing malformed or malicious unsecured downlink messages. The UE adhered to protocol by terminating the session securely upon receiving the standardized cause value. Secure

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 completing 5G-AKA authentication, which establishes a security context for encrypted and integrity-protected NAS communication. However, the UE transmitted this Service Request in plaintext, without any security protection. The AMF responded with a Service Reject message (also sent in plaintext) containing 5GMM Cause #111 ("Protocol error, unspecified"), to which the UE offered no further response. This behavior is **insecure** under 3GPP standards (TS 24.501). After successful 5G-AKA, all subsequent NAS messages—including Service Requests—must be integrity-protected and encrypted using the established security context to prevent eavesdropping, tampering, and replay attacks. The UE's transmission of a sensitive Service Request in plaintext violates this fundamental security requirement, exposing critical signaling data. Additionally, the UE's lack of reaction to the AMF's unsecured Service Reject (which itself should have been protected per standards) further demonstrates non-compliant handling of security protocols. 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 to the AMF after completing 5G-AKA authentication, which establishes a NAS security context. The AMF responded with a Service Reject message containing 5GMM Cause #21 ("Synch failure"), indicating a potential sequence number desynchronization. Crucially, the AMF sent this rejection in plaintext without encryption or integrity protection, despite the existing security context mandating protected NAS messaging post-authentication. The UE exhibited no response to this unprotected rejection. Based on 3GPP standards (TS 24.501), this UE behavior is **insecure**. After successful 5G-AKA, all subsequent NAS messages must be confidentiality and integrity protected, except for specific unprotected exchanges like initial registration. The Service Reject falls under protected messaging requirements. The UE should have: 1. Detected the lack of security protection on the Service Reject. 2. Discarded the message as invalid per §4.4.4.3 of TS 24.501. 3. Initiated recovery actions (e.g., local release or re-registration) as specified for security context mismatches in §5.5.1.2. The UE's failure to recognize the unprotected message—particularly one indicating a critical security issue like synchronization failure—and its subsequent inaction violate 5G security protocols, leaving it vulnerable to downgrade attacks or desynchronization exploits. Insecure

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 after the completion of 5G-AKA, with the UE sending an unprotected UL NAS TRANSPORT message containing a Registration Complete and PDU Session Establishment Request. The AMF responded with a Configuration Update Command (unprotected, as security was not yet activated) and then sent a Security Mode Command (SMC) marked as "Protected" in the test summary, using integrity algorithm 128-5G-IA2 and ciphering algorithm 5G-EA6. Critically, the UE provided no response to the SMC. According to 3GPP standards (TS 33.501), the SMC must be integrity-protected but **not ciphered** at this stage, as ciphering activation depends on the SMC procedure itself. The test summary ambiguously describes the SMC as "Protected" without clarifying whether ciphering was applied, but the UE's lack of response aligns with standard behavior if the AMF improperly ciphered the SMC: A compliant UE must reject or ignore non-conforming messages that violate the security state machine (e.g., ciphering before SMC completion). Since the UE did not proceed with security activation upon receiving an improperly secured SMC (likely due to ciphering being prematurely applied by the test AMF), it adhered to 5G security protocols by not engaging further. Secure

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 unprotected UL NAS TRANSPORT message after completing 5G-AKA, which is standard as security activation had not yet been initiated. The AMF responded with a Configuration Update Command (unprotected) and a Security Mode Command (SMC) marked as "Protected." However, the SMC specified null algorithms—5G-EA0 for ciphering and 5G-IA0 for integrity—which provide no actual security. Crucially, the UE did not respond to the SMC. According to 3GPP standards (TS 33.501), null integrity (5G-IA0) is prohibited for non-emergency sessions, and the SMC itself must be integrity-protected to prevent tampering. By discarding the invalid SMC (as it claimed protection but used null integrity, violating the standard), the UE avoided activating an insecure security context. This silent discard aligns with protocol requirements to ignore non-conformant messages, demonstrating secure behavior. Secure
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 sending a Service Request after completing 5G-AKA authentication, establishing a security context. The AMF responded with a Configuration Update Command sent as a plain (unprotected) NAS message, indicated by the security header type "Plain NAS message (0)". The UE provided no response to this message. According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA is completed and a security context is active, all subsequent NAS messages—including Configuration Update Command—must be integrity-protected to prevent tampering and ensure authenticity. The UE's failure to respond to an unprotected Configuration Update Command aligns with the standard's requirement to discard such messages and initiate re-authentication or recovery procedures. However, the absence of any observed recovery action (e.g., re-registration or security mode renegotiation) indicates the UE did not enforce the mandated security protocols, leaving it vulnerable to potential downgrade attacks or exploitation via unverified commands. Insecure

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 to the AMF after completing 5G-AKA authentication. The AMF then responded with a Security Mode Command (SMC) message, sent as plain text (security header type 0), specifying ciphering algorithm 5G-EA4 and integrity algorithm 5G-IA5. According to 3GPP TS 33.501, the SMC must always be sent unprotected to initiate security activation, as no security context exists yet. The UE's role was to validate the SMC (including algorithm acceptance and ABBA parameter consistency), activate the security context immediately after processing the SMC, and respond with a Security Mode Complete message—protected with the newly activated integrity and ciphering. However, the UE provided no response, failing to send this mandatory confirmation. This omission indicates the UE did not activate the security context, leaving subsequent messages unencrypted and unverified, violating the standard's requirement to establish secured communication post-SMC. The lack of response also prevents the AMF from confirming successful security activation, breaking the protocol flow. 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 UL NAS TRANSPORT message containing a Registration Complete and a PDU Session Establishment Request. Subsequently, the AMF sent a Downlink NAS TRANSPORT with a Configuration Update Command, followed by a Security Mode Command (SMC) in plaintext, specifying ciphering algorithm 5G-EA6 and integrity algorithm 5G-IA5. The UE did not respond to the SMC. According to 3GPP standards (TS 33.501), after 5G-AKA completion, NAS security must be activated via the SMC procedure before transmitting sensitive messages like PDU Session Establishment Requests. Here, the UE transmitted this unprotected request prematurely, prior to SMC completion. Moreover, the UE's failure to respond to the SMC prevented security context activation, leaving subsequent communications unsecured. This violates 5G security protocols, which mandate that session management messages be integrity-protected and that UEs must complete the security handshake to enable encryption. 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.	After successfully completing the 5G-AKA authentication, the UE initiated communication by sending a protected Service Request to the AMF. The AMF responded with an Authentication Reject message sent in plaintext, without encryption or integrity protection, despite the established security context from the prior 5G-AKA. According to 3GPP standards (TS 24.501 and TS 33.501), once 5G-AKA completes, all subsequent NAS messages—including Authentication Reject—must be confidentiality and integrity protected using the derived security keys. The UE exhibited secure behavior by not processing or responding to the unprotected Authentication Reject message. This aligns with 3GPP requirements, which mandate that UEs discard unprotected NAS messages after security context establishment to prevent exploitation (e.g., forced deregistration attacks). The absence of UE action confirms it ignored the non-compliant message, preserving its security state. 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 initiating a Service Request via an uplink NAS message, following a completed 5G-AKA procedure that established a valid security context. The AMF responded with a downlink Authentication Reject message sent in plaintext (unencrypted and without integrity protection). Crucially, the UE exhibited no detectable reaction to this unsecured rejection, such as initiating a local release, resetting the connection, or triggering re-authentication. This behavior is insecure under 3GPP 5G security standards (TS 33.501), which mandate that all NAS messages after a successful 5G-AKA must be confidentiality and integrity protected using the negotiated keys. The UE's failure to detect or respond to the unprotected critical message—which could indicate an adversary injecting forged rejections—violates fundamental security requirements by accepting an unauthorized, unsecured command without challenge or protective action. 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 that had not yet established a security context. The AMF then sent an Identity Request in plaintext (unencrypted and unprotected), asking for the UE's TMSI. The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), prior to completing 5G-AKA, NAS messages lack integrity protection and encryption, making them vulnerable. The standard explicitly mandates that UEs must not disclose sensitive identities like TMSI in response to unprotected requests, as this could expose user identifiers to eavesdropping or spoofing attacks. Instead, the UE should either ignore the request, respond with a "no identity" indicator, or defer the response until security is established. While the UE's non-response avoids leaking the TMSI—aligning with the security principle of not exposing identifiers unprotected—it represents a protocol deviation, as the standard expects a formal Identity Response (e.g., with "no identity") for compliance. Nevertheless, the core security objective of preventing unprotected identity disclosure was upheld, as the UE refrained from transmitting the TMSI in plaintext. Thus, the action prioritizes confidentiality over procedural adherence, mitigating immediate risks. 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 ongoing but incomplete 5G-AKA process. The AMF then sent an Identity Request for the UE's IMEISV (a permanent equipment identifier) in plain text, as no security context had been established. 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 a security context is established, ensuring confidentiality and integrity protection. Since the 5G-AKA was incomplete and the AMF's request lacked encryption or integrity protection, the UE's refusal to disclose the IMEISV aligns with security requirements. This prevents potential eavesdropping or manipulation of unprotected identity data, adhering to 5G security protocols. 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, confirming mutual authentication. The AMF then sent a Security Mode Command (SMC) in plain text, as standardized, specifying ciphering (5G-EA4) and integrity (128-5G-IA2) algorithms for subsequent protected communications. Per 3GPP TS 24.501 and TS 33.501, upon receiving the SMC, the UE must first respond with a **Security Mode Complete** message—protected using the newly negotiated algorithms—to acknowledge security activation before sending any other NAS messages. However, the UE ignored this requirement and immediately sent a Deregistration Request without activating security. This request was transmitted unprotected, as evidenced by the absence of a security header and the lack of prior Security Mode Complete. By bypassing the mandatory security activation step and transmitting a sensitive message (deregistration) in plaintext, the UE violated 5G security protocols, leaving the message vulnerable to interception or manipulation. 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 between the UE and AMF 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) to activate security algorithms for subsequent communications. This SMC was marked as "Protected" and specified the ciphering algorithm 5G-EA5 for encryption but used the null integrity algorithm (5G-IA0), meaning no integrity protection was applied. Crucially, the UE provided no response to this SMC. According to 3GPP standards (TS 33.501), the SMC message must always be integrity-protected to prevent tampering, as it establishes the security context for future messages. The use of 5G-IA0 for integrity violates this requirement, leaving the SMC vulnerable to manipulation (e.g., algorithm downgrade attacks). The UE's failure to reject the SMC—by not sending a Security Mode Reject message—indicates it accepted an insecure configuration, disregarding the mandate for integrity protection during security setup. This non-compliant behavior undermines the security framework of 5G. 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 to the AMF, followed by the AMF sending an Identity Request for the TMSI in plain text, as 5G-AKA authentication had not yet been completed. The UE did not respond to this request. According to 3GPP standards (TS 33.501), initial NAS messages before 5G-AKA completion are permitted in plain text, as no security context exists for encryption. The Identity Request for TMSI—a temporary, non-sensitive identifier—does not inherently violate security protocols when sent unprotected at this stage. However, the UE's lack of response deviates from standard behavior, which mandates compliance with network requests during registration. While this non-response might indicate a protocol conformance issue, it does not constitute a *security* vulnerability: the UE avoided transmitting sensitive data (e.g., SUPI/IMSI) in plain text and did not expose credentials or keys. The silence prevented potential attack surfaces like manipulation or replay, though it could disrupt service. Thus, the core security principles of confidentiality and integrity were maintained, as no sensitive information was compromised. Secure

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 (downlink) for the IMEISV identity, as 5G-AKA authentication had not yet been completed. The UE did not provide the requested IMEISV. According to 3GPP standards (TS 33.501), sensitive identities like IMEISV must only be transmitted after a secure NAS context is established through successful 5G-AKA, ensuring encryption and integrity protection. Since the AMF's request was sent in plaintext—consistent with the pre-authentication phase—the UE's refusal to respond aligns with security requirements. Providing IMEISV unprotected would risk exposing device-specific data to eavesdropping or spoofing. Thus, the UE's non-response demonstrates adherence to 5G security protocols by safeguarding sensitive information until authentication completes. 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 complete the 5G-AKA procedure, confirming mutual authentication. The AMF then responded with a Security Mode Command (SMC) to activate NAS security, specifying the ciphering (128-5G-EA3) and integrity (128-5G-IA1) algorithms. Critically, this SMC was transmitted as a plaintext NAS message (security header type 0), without integrity protection or encryption. The UE did not generate any response to this command. According to 3GPP standards (TS 33.501 and TS 24.501), the SMC must always be integrity-protected, as it is the first message post-authentication that establishes security parameters. An unprotected SMC is vulnerable to tampering (e.g., algorithm downgrade attacks) and must be rejected by the UE. The standard mandates that the UE should respond with a Security Mode Reject message (NAS cause #96: "Invalid mandatory information") when receiving an unprotected SMC. The UE's lack of response constitutes non-compliance, as it fails to explicitly reject the insecure command or initiate recovery actions, leaving the session in an ambiguous state and violating security protocols. Insecure

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 between the UE and AMF began with the UE sending an uplink message containing a Security Mode Complete, Registration Request, and other control data, followed by the AMF sending a downlink Security Mode Command message, which was marked as "Protected" and included specified ciphering (5G-EA7) and integrity (128-5G-IA2) algorithms. Critically, this sequence violates the 5G security protocol mandated by 3GPP (TS 33.501), which requires the AMF to initiate security activation by sending a Security Mode Command *before* the UE responds with a Security Mode Complete. Here, the UE sent Security Mode Complete *without* having received the Security Mode Command first, indicating it prematurely treated security activation as complete. This deviation suggests the UE ignored the protocol's state machine, potentially accepting unprotected or improperly secured messages. Furthermore, the UE provided no response to the AMF's subsequent Security Mode Command, compounding the irregularity. Such behavior undermines the mutual authentication and negotiated security context establishment defined by 5G standards, exposing the UE to risks like command injection or security context bypass. 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 after completing 5G-AKA, indicating successful mutual authentication and key derivation. The AMF then sent a Security Mode Command (SMC) to activate NAS security, specifying ciphering algorithm 128-5G-EA1, integrity algorithm 128-5G-IA2, and ABBA parameter 03f3. This SMC was marked as "Protected," implying it was integrity-protected using the established K_{NASint} key and the new integrity algorithm (128-5G-IA2) as mandated by 3GPP TS 33.501. The UE, however, provided no response to the SMC. According to 3GPP TS 24.501, a UE must silently discard any SMC that fails integrity verification—a critical security measure to prevent processing tampered or malicious commands. The absence of a response indicates the UE detected an integrity failure (e.g., due to mismatched keys, incorrect ABBA, or algorithm mismatch) and adhered to the standard by not proceeding. This behavior aligns with security protocols, as responding to an unverified SMC could expose vulnerabilities. The UE's silent discard action demonstrates robust security compliance. 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 successful 5G-AKA, confirming mutual authentication and key establishment. The AMF then sent a Security Mode Command (SMC) in plaintext (without integrity protection or encryption) to activate NAS security, specifying ciphering (128-5G-EA1) and integrity (128-5G-IA1) algorithms. The UE provided no response to this SMC. According to 3GPP standards (TS 33.501, sections 6.7 and 8.2.2.1), the SMC must be integrity-protected to prevent tampering with security parameters (e.g., algorithm selection or ABBA values), as it is the first step in enabling secured communication. Transmitting it unprotected exposes the system to downgrade attacks or malicious modifications. The UE's lack of response indicates it rejected the SMC due to the absence of integrity protection, aligning with standard-mandated behavior to ignore unprotected SMCs. This ensures the UE does not proceed with an insecure security context, upholding the protocol's security requirements. Secure

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, which is typically a response to a Security Mode Command, before receiving any such command from the AMF. Subsequently, the AMF sent a Security Mode Command as a plain (unprotected) NAS message, specifying null ciphering (5G-EA0) and integrity algorithm 128-5G-IA2. Critically, this command lacked integrity protection (security header type 0), violating the 3GPP standard (TS 33.501 and TS 24.501), which mandates that Security Mode Command messages must be integrity-protected to prevent tampering and ensure authenticity. The UE failed to respond to this unprotected command, deviating from standard requirements where the UE must reject such messages with a Security Mode Reject (e.g., cause #96 "invalid mandatory information") and terminate the session. This non-response, coupled with the premature Security Mode Complete, demonstrates non-compliance with 5G security protocols, leaving the UE vulnerable to attacks like bidding-down or malicious command injection. 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.	In the observed interaction, the UE transmitted an Authentication Response to the AMF, but the 5G-AKA procedure remained incomplete, meaning no security context (integrity protection or encryption) was established. Subsequently, the AMF sent a plaintext Identity Request demanding the UE's IMEISV—a sensitive device identifier. Critically, the UE provided no response to this request. According to 3GPP 5G security standards (TS 33.501), sensitive identities like IMEISV must never be transmitted unprotected. Since the 5G-AKA had not yet secured the NAS layer, the UE correctly refrained from disclosing the IMEISV in plaintext, adhering to the requirement that such data only be shared after security activation. This non-compliance with an insecure request aligns with protocol mandates to prevent identity exposure during initial authentication. 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, which is part of the 5G-AKA procedure to establish a secure context. Before 5G-AKA completion, the AMF sent an Identity Request (for TMSI) in plain text, as indicated in the packet capture. According to 3GPP standards (TS 33.501), once the Authentication Response is sent, the UE must enforce security activation for subsequent NAS messages. This means any message after the Authentication Response should be protected (encrypted and integrity-protected) using the newly derived security keys. The AMF's plain-text Identity Request violates this requirement, as it occurred post-Authentication Response without security activation. The UE correctly identified this deviation by providing no response, adhering to the standard's mandate to reject unsecured communications after security context initiation. This prevents potential eavesdropping or manipulation of sensitive requests like identity queries. The UE's non-response demonstrates compliance with 5G security protocols. 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 via UplinkNASTransport, acknowledging the ongoing 5G-AKA process. Before authentication could complete, the AMF sent a DownlinkNASTransport containing an Identity Request for the UE's IMEISV in plaintext (unprotected). The UE provided no response to this request. According to 3GPP standards (TS 33.501), after initiating authentication (via Authentication Response), the UE must only process subsequent NAS messages that are integrity-protected using a valid 5G NAS security context—which is established only upon successful 5G-AKA completion. Since the Identity Request was sent unprotected mid-authentication, the UE correctly ignored it to prevent exposing sensitive identity data (IMEISV) without cryptographic safeguards. This adherence to protocol, prioritizing security over network demands, constitutes secure behavior. 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 successful completion of 5G-AKA mutual authentication, after which the UE sent an unprotected Authentication Response. The AMF then transmitted a Security Mode Command (SMC), which was marked as "Protected" and specified the ciphering algorithm (128-5G-EA2) and integrity algorithm (128-5G-IA3), along with ABBA parameter "1111". According to 3GPP TS 33.501, the SMC must be integrity-protected to authenticate the network and establish secure communication. Upon receiving the SMC, the UE was required to verify its integrity, validate the algorithms, and respond with either a Security Mode Complete (if accepted) or Security Mode Reject (if invalid or unsupported). However, the UE provided no response, as confirmed by the packet capture and test summary. This failure to engage with the SMC violates the 5G security protocol, which mandates a UE response to complete or reject the security context setup. Without this response, the security context remains unconfirmed, leaving subsequent communications vulnerable to downgrade attacks or manipulation, as the UE did not enforce the required security handshake. 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.	After successfully completing 5G-AKA authentication, establishing a security context between the UE and AMF, the UE initiated a Service Request (which should have been integrity-protected and encrypted per 3GPP standards). The AMF responded with a Configuration Update Command sent as a plaintext NAS message (security header type 0), lacking both encryption and integrity protection. According to 3GPP TS 33.501, all NAS messages after 5G-AKA must be protected using the established security context to prevent tampering and eavesdropping. The UE correctly identified this violation by discarding the unprotected message and providing no response, as processing such messages would compromise security. This adherence to protocol requirements—rejecting unsecured commands despite potential network-triggered actions—demonstrates robust security hygiene. Secure

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, likely in response to an initial unprotected Identity Request from the AMF for a subscription identifier like SUCI/SUPI. Subsequently, the AMF sent another unprotected Identity Request—this time for the IMEISV (equipment identifier)—before 5G-AKA authentication completed. The UE did not respond to this second request. According to 3GPP TS 24.501, after the initial unprotected Identity Request during registration, the UE must only respond to subsequent Identity Requests if they are integrity-protected. Since 5G-AKA had not yet established a security context, the AMF's IMEISV request lacked integrity protection. The UE's refusal to comply aligns with the standard, preventing potential exposure of sensitive identifiers (IMEISV) to unauthenticated or malicious networks and mitigating tracking risks. This behavior demonstrates adherence to 5G security protocols, which mandate protection for non-initial identity exchanges. 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, followed by the AMF sending a subsequent Identity Request in plain text (unencrypted) asking for the TMSI identity. Since 5G-AKA had not been completed at this stage, no security context was established, meaning NAS messaging lacked encryption and integrity protection as per 3GPP standards (TS 33.501). The UE did not respond to the Identity Request for TMSI. This inaction aligns with 3GPP security requirements, which mandate that after initial registration, requests for sensitive identities like TMSI must be integrity-protected to prevent tracking and spoofing attacks. Sending TMSI in plaintext would expose the UE to privacy breaches and location tracking. By withholding the response, the UE correctly prioritized security, adhering to the protocol’s safeguards for unprotected NAS messaging phases. Secure

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 for the UE's IMEISV, as 5G-AKA had not yet been completed to establish encryption and integrity protection. The UE did not respond to this request. According to 3GPP standards (TS 33.501 and TS 24.501), sensitive identifiers like IMEISV must not be transmitted without NAS security (integrity protection and encryption), which requires successful 5G-AKA authentication. Since 5G-AKA was incomplete, the UE correctly refrained from sending the IMEISV to prevent potential tracking or spoofing by untrusted entities. However, the standard mandates that the UE must respond to an Identity Request with an Identity Response message, even if it cannot provide the requested identity (e.g., by setting the identity type to "no identity"). The UE's failure to send any response constitutes a protocol violation, but this does not compromise security, as the critical requirement—protecting the IMEISV—was upheld. The absence of a response avoids exposing the IMEISV and does not indicate a security flaw in the UE's handling of sensitive data. 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 to the AMF, indicating its intent to resume services after the prior completion of 5G-AKA authentication. The AMF then responded with an Identity Request for the UE's GUTI, explicitly sent as a plain/unprotected NAS message. The UE did not provide any response to this request. According to 3GPP security standards (TS 33.501), after successful 5G-AKA, all subsequent NAS messages—including Identity Request—must be integrity-protected and encrypted using the established security context. The UE, recognizing that the unprotected Identity Request violated this requirement, correctly ignored it, as processing such a message would expose it to potential tampering or spoofing attacks. By rejecting the non-compliant message, the UE adhered to 5G security protocols. 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.	The interaction began with the successful completion of 5G-AKA authentication, establishing a security context for encrypted and integrity-protected NAS communication as mandated by 3GPP standards (TS 33.501). The UE then initiated a PDU session request via an Uplink NAS Transport message. In response, the AMF sent a Service Accept message, but critically, this downlink message was transmitted in plaintext without encryption. The UE exhibited no response to this unencrypted message. According to 3GPP, once 5G-AKA completes, all subsequent NAS messages—including Service Accept—must be confidentiality-protected to prevent eavesdropping and tampering. The UE's failure to reject or challenge the plaintext Service Accept (e.g., by initiating a recovery procedure or ignoring the message) violates this requirement. This inaction implies acceptance of an insecure transmission, exposing the UE to potential man-in-the-middle attacks or data interception. 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.	After the completion of the 5G-AKA authentication, which establishes a secure NAS context, the UE initiated communication by sending a Service Request (encrypted, as required post-authentication). The AMF responded with an Identity Request for the IMEI, but transmitted this message in plaintext without encryption or integrity protection. The UE correctly recognized the AMF's message as non-compliant with 3GPP security standards (TS 33.501), which mandate that all NAS messages after 5G-AKA must be confidentiality and integrity protected to prevent eavesdropping and tampering. Consequently, the UE discarded the unprotected Identity Request and sent no response, adhering to the protocol's security requirements by rejecting improperly secured traffic. This behavior aligns with 5G security specifications, as accepting or processing plaintext NAS messages post-authentication would expose the UE to potential attacks like information leakage or spoofing. 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 after the successful completion of 5G-AKA, establishing a NAS security context. The UE sent a Registration Complete message, which should be integrity-protected and encrypted per 3GPP TS 24.501. The AMF then responded with a DownlinkNASTransport containing a plaintext (unencrypted) 5GMM Status message with cause #97 ("Message type non-existent or not implemented"). The UE took no action in response. According to 3GPP standards (TS 24.501 § 4.4.4.3 and § 5.4.1), once a NAS security context is active (post-5G-AKA), all NAS messages—except specific exceptions like authentication requests—must be integrity-protected and encrypted. The 5GMM Status message does not qualify as an exception. The UE correctly ignored the unprotected message, as processing it would violate security protocols by risking exploitation of unverified or malicious content. This adherence to discarding non-compliant messages aligns with standard security requirements. 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.	After completing the 5G-AKA authentication, the UE sent a Registration Complete message to the AMF, indicating successful registration. The AMF then responded with an Identity Request for the SUCI, 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 is completed, all subsequent NAS messages must be confidentiality and integrity protected using the established security context. The UE's failure to respond to an unprotected Identity Request aligns with security requirements, as processing such a message could expose vulnerabilities to eavesdropping or tampering. By ignoring the non-compliant request, the UE adhered to protocol mandates that prioritize rejecting unprotected communications post-authentication. Insecure

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.	After completing the 5G-AKA authentication, the UE sent a **Registration Complete** message (integrity-protected and ciphered), confirming a secure NAS context. The AMF then sent a **Deregistration Request** downlink message **in plaintext** (without integrity protection or encryption), violating the 3GPP security standard (TS 33.501), which mandates that all NAS messages after 5G-AKA must be integrity-protected to prevent tampering and ensure authenticity. The UE discarded this unsecured request, as required by the standard, and instead initiated a new **UE-originating Deregistration Request** uplink message. This uplink message was correctly sent with security (implied by the completed 5G-AKA context), demonstrating that the UE adhered to security protocols by rejecting the insecure downlink message and handling deregistration via a protected uplink procedure. The UE’s actions align with 3GPP guidelines, which specify that unsecured NAS messages must be discarded, and subsequent protected actions may be taken. 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 completing the 5G-AKA authentication, establishing a secure NAS context, the UE sent an UplinkNASTransport message (PDU session establishment request), which should have been encrypted and integrity-protected per 3GPP standards. The AMF responded with a DownlinkNASTransport containing a 5GMM status message (cause #99: "Information element non-existent or not implemented"), sent in plaintext without encryption or integrity protection. The UE provided no response to this unprotected message. According to 3GPP TS 24.501, once a security context is established, all subsequent NAS messages—except specific exceptions like initial authentication or null-protected registration—must be protected. The 5GMM status message does not qualify as an exception. The UE's failure to respond aligns with security requirements, as processing or acknowledging an unprotected message could expose vulnerabilities. By discarding the message silently, the UE avoided potential security risks like malicious injection or manipulation, demonstrating adherence to 3GPP protocols. Secure

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.	After completing 5G-AKA (establishing a secure context), the UE sent a Registration Complete message, which should have been encrypted per 3GPP standards (TS 24.501, 4.4.5). The AMF then responded with a plaintext GMM Status message (Cause #101: "Message not compatible with the protocol state"), violating the requirement to protect NAS messages post-authentication. The UE, instead of discarding this non-compliant plaintext message as mandated by the standard, processed it and initiated a Deregistration Request. This action demonstrates that the UE failed to enforce security policies by: (1) accepting and acting upon an unprotected NAS message despite an active security context, and (2) potentially exposing sensitive information (e.g., UE identity) in the Deregistration Request if transmitted without encryption—though encryption status of this specific message isn't explicitly confirmed, the UE's prior acceptance of plaintext undermines the security posture. **Insecure**
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 sending an unprotected Service Request to the AMF. After 5G-AKA completion, the AMF responded with a Security Mode Command (SMC) marked as "Protected," specifying ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and including ABBA parameter 0101. The UE failed to respond with either Security Mode Complete or Reject, violating 3GPP TS 24.501 §4.4.6 and §8.2.6.1. Post-AKA, the SMC must be integrity-protected (not encrypted) using the established K~AMF~, allowing the UE to verify it before activating new security. The UE's lack of response indicates it either ignored the SMC, failed integrity verification, or encountered an internal error—all deviations from protocol. This omission prevents security activation, leaving subsequent messages unprotected and undermining mutual authentication. 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 to the AMF, indicating a request for service initiation. The AMF responded with a Security Mode Command (SMC) to activate NAS security. However, the AMF transmitted this SMC as a plaintext message (Security Header: 0), with null ciphering (5G-EA0) and integrity protection algorithm 128-5G-IA2. Critically, the SMC lacked integrity protection and encryption, violating the 3GPP 5G security standard (TS 33.501). After 5G-AKA completion, all NAS messages—including the SMC—must be integrity-protected to prevent tampering and ensure authenticity. The UE's lack of response to this unprotected SMC indicates it failed to reject the insecure command, as required by the standard. This omission leaves the UE vulnerable to man-in-the-middle attacks, such as security algorithm downgrade or malicious SMC injection, since the UE did not enforce mandatory integrity verification. 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.	The interaction began with the successful completion of 5G-AKA, establishing mutual authentication and security context between the UE and AMF. The UE then sent an Uplink NAS Transport message (encapsulating a PDU session establishment request), which should have been encrypted and integrity-protected per 3GPP TS 24.501 standards, given the active security context. The AMF responded with an unprotected (plain) Registration Reject message containing 5GMM cause #74 ("Temporarily not authorized for this SNPN"). The UE exhibited no response to this message. According to 3GPP standards (TS 24.501 § 4.4.4, § 5.4.1.2), once 5G-AKA completes, all subsequent NAS messages—including reject messages—**must** be confidentiality and integrity-protected to prevent downgrade attacks, spoofing, or information leakage. The AMF's transmission of the Registration Reject in plaintext violates this requirement. The UE’s lack of response aligns with standard-compliant behavior: Upon receiving an unprotected NAS message after security activation (excluding specific exceptions like authentication requests), the UE must discard the message and refrain from processing or acknowledging it (TS 24.501 § 5.4.1.2). This prevents potential exploitation of unprotected interactions. Thus, the UE correctly identified the protocol violation and adhered to security protocols by ignoring the invalid message. Secure

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.	The interaction began with the UE successfully completing 5G-AKA authentication, establishing a secure NAS context. The UE then sent an Uplink NAS Transport containing Registration Complete and a PDU Session Establishment Request. The AMF responded with a Downlink NAS Transport carrying a Registration Reject message (5GMM Cause #6: Illegal ME), transmitted in plaintext without encryption or integrity protection. Crucially, the UE exhibited no response to this unprotected rejection message. According to 3GPP standards (TS 24.501 and TS 33.501), once 5G-AKA completes, all subsequent NAS messages—including Registration Reject—must be confidentiality and integrity protected to prevent tampering or interception. The UE's failure to respond aligns with protocol requirements: upon receiving an unprotected NAS message post-authentication, the UE must discard it without processing (TS 24.501 §4.4.4.3) and locally handle the security violation (e.g., releasing the connection, transitioning to DEREGISTERED state). By ignoring the unsecured reject message and avoiding further action, the UE correctly identified the security breach and mitigated potential exploitation, adhering to 5G security mandates. 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 RAND, AUTN, ABBA, and ngKSI=5 (Native security context). Instead of processing the authentication challenge, the UE immediately replied with an Authentication Failure message, explicitly citing "ngKSI already in use" as the reason. This indicates the UE detected that the ngKSI value (5) provided by the AMF was already associated with an active security context on the UE side, per 3GPP TS 33.501 Section 6.1.2.2, which prohibits ngKSI reuse for distinct security contexts. By rejecting the request and explicitly signaling the ngKSI conflict without attempting authentication, the UE adhered to 5G security standards. This prevents potential context confusion attacks where an adversary might force key reuse or compromise session integrity. The plaintext transmission was unavoidable here since no security context was active yet, but the UE's validation of ngKSI uniqueness aligns with protocol requirements to mitigate key-related threats. 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 sending a UL NAS TRANSPORT message containing a PDU session establishment request, indicating that the 5G-AKA authentication had previously completed successfully. This completion should have established a NAS security context for encrypted and integrity-protected communication. However, the AMF responded with an unprotected (plain) Authentication Reject message, which the UE ignored, providing no further response. According to 3GPP standards (TS 33.501), once a NAS security context is established after 5G-AKA, the UE must reject all unprotected NAS messages—except for specific initial procedures like Authentication Request or Identity Request. The Authentication Reject is not exempt from this protection requirement when a security context exists, as it is only permitted without protection during initial authentication failures. By ignoring the unprotected Authentication Reject instead of resetting its security state (e.g., deleting keys or invalidating the USIM), the UE correctly enforced integrity protection rules, preventing a potential security compromise where an attacker could disrupt the session via forged reject messages. 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 with the AMF. The UE then sent an encrypted Uplink NAS Transport message containing a PDU session establishment request. Subsequently, the AMF responded with an unencrypted and unprotected Authentication Reject message, to which the UE provided no response. According to 3GPP standards (TS 24.501, 33.501), after 5G-AKA completion and security context activation, all NAS messages—except a few explicitly excluded (e.g., Authentication Request/Reject)—must be integrity-protected and encrypted to prevent tampering and eavesdropping. The Authentication Reject message, while permissible in plain form under specific pre-security-context conditions, becomes anomalous post-security-activation. Here, it was sent after security context establishment, violating the UE’s expectation of protected communication. A secure UE should discard such an unprotected message post-context-establishment, as processing it could lead to security risks like denial-of-service attacks or session termination. The UE’s lack of response aligns with discarding the message, demonstrating adherence to the standard by ignoring potentially malicious unprotected commands after security activation. Secure
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 successful completion of 5G-AKA authentication, establishing a security context between the UE and AMF. Following this, the UE sent a Registration Complete message. The AMF then responded with a Configuration Update Command, which was marked as "Protected" in the test summary, indicating intent for security protection. However, the security header was noted as "Unknown," and the UE provided no response to this message. According to 3GPP standards (TS 24.501 and TS 33.501), after 5G-AKA, all subsequent NAS messages must be integrity-protected and optionally encrypted to prevent tampering and ensure authenticity. The Configuration Update Command requires such protection, and the UE is mandated to verify the integrity and security of the message. If the security header was unrecognized or invalid—rendering the message unprotected—the UE should discard it and potentially initiate re-registration to re-establish security. The UE's lack of response suggests it either accepted an unprotected message without validation or failed to react to a security anomaly, both violating 3GPP requirements for mandatory security checks on protected downlink NAS commands. This behavior leaves the UE vulnerable to man-in-the-middle attacks, such as malicious reconfiguration via forged commands. Insecure

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 authentication, establishing a secure context, and sending a Registration Complete message to the AMF. Subsequently, the AMF responded with a Deregistration Accept message (indicating UE-terminated deregistration) sent in plaintext, lacking both encryption and integrity protection. The UE exhibited no response to this message. According to 3GPP standards (TS 33.501 and TS 24.501), after 5G-AKA completion, all NAS messages—especially critical commands like Deregistration Accept—must be integrity-protected and encrypted to prevent tampering and eavesdropping. The UE's lack of response aligns with security requirements, as it implicitly discarded the unprotected message rather than processing it, thereby adhering to the mandate to reject unsecured NAS communications post-authentication. This behavior demonstrates compliance with 5G security protocols. Secure
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 Identity Response to the AMF, followed by the AMF sending a plain-text (unencrypted) Identity Request for the UE's IMEISV. Since 5G-AKA authentication had not been completed, no security context existed, and NAS messages were unprotected. Per 3GPP standards (TS 33.501), the IMEISV is classified as sensitive information that must only be transmitted in integrity-protected messages to prevent tracking or spoofing attacks. The UE's lack of response to the unprotected Identity Request aligns with these security requirements, as transmitting the IMEISV without protection would violate the standard and expose the device to privacy risks. The UE correctly prioritized security by withholding the identifier until a secure channel is established. 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 to the AMF, followed by the AMF requesting the UE's IMEI via a plain-text DownlinkNAS Transport message. Since 5G-AKA authentication had not yet been completed, no security context existed to encrypt communications. The UE did not respond to the IMEI request. According to 3GPP standards (TS 33.501), permanent identifiers like IMEI must never be transmitted unprotected over the air interface. Transmitting IMEI in plain text would expose it to eavesdropping, violating 5G's privacy requirements. By withholding the IMEI in the absence of encryption, the UE adhered to the standard's mandate that sensitive data only be shared after security activation via 5G-AKA. This non-compliance with an insecure network instruction demonstrates correct security posture. Secure
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 interaction began with the UE sending an unprotected Initial Registration Request to the AMF, as expected before authentication. However, the AMF responded with a Service Accept message marked as "Protected" despite 5G-AKA authentication not being completed. This is non-compliant with 3GPP standards (TS 33.501), as NAS message protection requires successful 5G-AKA to establish security keys. The UE then insecurely processed this improperly protected Service Accept message and proceeded to send a Deregistration Request. According to 3GPP, the UE should have rejected the Service Accept message since no valid security context existed to verify its integrity or confidentiality. By engaging further instead of terminating the connection or triggering recovery procedures, the UE violated fundamental security protocols designed to prevent processing of unauthorized protected messages. This behavior exposes the UE to potential man-in-the-middle or replay attacks where malicious actors could inject fabricated protected messages before authentication completes. 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 to the AMF as part of the ongoing 5G-AKA procedure. Before 5G-AKA completion (which establishes security keys), the AMF unexpectedly sent a Deregistration Request message protected with both integrity protection and ciphering (security header type 2). The UE provided no response to this message. According to 3GPP standards (TS 33.501), NAS security must be activated via a Security Mode Command (SMC) *after* successful 5G-AKA authentication but *before* any protected NAS messages (except SMC itself). Here, the AMF sent a protected Deregistration Request prematurely, without prior SMC or established security context. The UE correctly rejected this non-compliant message, as it lacked valid keys to verify integrity or decipher the content. This aligns with 3GPP security requirements, as processing such a message could expose vulnerabilities. The UE's silent discard of the invalid message prevented potential security compromises. 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 5G-AKA completion (and thus without an established NAS security context), the AMF sent a Deregistration Request message to the UE, which was marked as "Integrity protected" in its security header. The UE provided no response to this message. According to 3GPP standards (TS 24.501, section 4.4.4.3), a UE without an active NAS security context must discard any protected NAS message (except specific exceptions like Authentication Request) without processing or responding, as it cannot verify integrity. Deregistration Request is not among the allowed exceptions. The UE's silent discard of the unverifiable protected message aligns with this security requirement, preventing potential processing of unauthenticated network commands. 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 expected before security establishment. The AMF responded with a Deregistration Request (UE terminated) marked as "Illegal ME," which was sent as **protected** (integrity-protected and ciphered, security header type 2) despite 5G-AKA not being completed. The UE provided no response to this message. According to 3GPP standards (TS 33.501), NAS protection (integrity/ciphering) requires a valid security context established via 5G-AKA. Since 5G-AKA had not been performed, the UE lacked the keys to verify or decrypt the protected message. The standard mandates that UEs discard such protected messages received before security context establishment to prevent processing potentially malicious or forged commands. The UE's non-response aligns with this requirement, as it ignored an unverifiable protected message, thereby avoiding forced deregistration or other unauthorized state changes. This behavior demonstrates adherence to security protocols by rejecting unprotected or improperly protected NAS messages during initial registration. 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 plaintext, followed by the AMF transmitting a Security Mode Command (SMC) also in plaintext. The SMC specified cryptographic algorithms (5G-EA6 for ciphering, 128-5G-IA1 for integrity) and included ABBA parameters but lacked any security header or protection. Crucially, 5G-AKA authentication had not been completed, meaning no shared keys were established to validate or secure the SMC. According to 3GPP standards (TS 33.501), the SMC must always be integrity-protected to prevent forgery, and it should only be sent after successful authentication when a security context exists. The UE’s lack of response to this unprotected SMC demonstrates compliance with the standard, as processing an unverified SMC could enable security downgrade attacks or malicious algorithm negotiation. By ignoring the command, the UE correctly prioritized security protocols over network directives. 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 to the AMF, as 5G-AKA authentication had not yet been completed. Subsequently, the AMF sent a Configuration Update Command, which was marked as "Integrity protected" (Security Header Type 1). According to 3GPP standards (TS 33.501), NAS messages requiring integrity protection must not be processed by the UE until after successful 5G-AKA authentication establishes a valid security context. Since 5G-AKA was incomplete, the UE lacked the keys to verify the message's integrity. The UE's lack of response indicates it correctly ignored the protected message, as acting on unverified commands could expose it to spoofed configuration attacks. This adherence to discarding unverifiable protected messages aligns with security protocols. 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 unprotected Identity Response to the AMF, as 5G-AKA authentication had not yet been completed. The AMF then sent a Configuration Update Command as a plain/unprotected NAS message (security header type 0). Instead of rejecting this unprotected sensitive command—which could modify critical network parameters like TAI lists or NITZ—the UE processed it and responded with an unprotected Deregistration Request. Per 3GPP TS 33.501, NAS messages carrying sensitive parameters or commands (like Configuration Update Command) **must be integrity-protected** after the initial registration procedure, even if 5G-AKA is ongoing. The UE violated this by accepting and acting upon an unprotected command that could compromise configuration integrity, exposing it to spoofing attacks (e.g., malicious network redirection or service disruption). Its subsequent Deregistration Request without protection further demonstrates non-compliance with 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 UE initiated the process by sending an unprotected Initial Registration Request to the AMF, which is standard behavior before security establishment. The AMF responded with a protected Deregistration Accept message without first completing the 5G-AKA authentication procedure. According to 3GPP standards (TS 33.501), NAS message protection (encryption/integrity) requires successful 5G-AKA to derive session keys. Since 5G-AKA had not been performed, the UE lacked the necessary security context to decrypt or validate the protected message. The UE's lack of response is appropriate, as processing an unverifiable protected message without established keys would violate security protocols. This inaction prevents potential exploitation from unauthenticated network commands. The AMF's premature protected message is non-compliant, but the UE correctly prioritized security by ignoring it. 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 required by 5G standards before security establishment. The AMF responded with a protected Deregistration Accept message (indicating UE-terminated deregistration) without first completing the 5G-AKA authentication procedure. Since 5G-AKA had not been performed, no security context (including encryption/integrity keys) existed between the UE and AMF. According to 3GPP TS 33.501, NAS security must be activated *after* successful 5G-AKA, and protected NAS messages (like Deregistration Accept) should only be sent/processed post-authentication. The UE correctly ignored the protected message, as it lacked the keys to validate its integrity or origin. This aligns with 5G security principles that prohibit processing protected NAS messages without an established security context, preventing potential exploitation by unauthorized network elements. The UE's non-response demonstrates adherence to the standard by rejecting unverifiable protected commands during initial registration. 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 is standard for the first step in NAS communication when no security context exists. Before 5G-AKA authentication could be completed to establish mutual authentication and derive security keys, the AMF sent a Configuration Update Command (CUC) protected with integrity and ciphering (security header type 4), claiming to use a "new security context." However, since 5G-AKA was not yet performed, no valid security context existed between the UE and AMF at this stage. The UE correctly provided no response to the CUC. According to 3GPP standards (TS 33.501), NAS security (integrity protection and ciphering) must only be applied *after* successful 5G-AKA authentication, which establishes a shared security context. Processing a protected NAS message without completed authentication would violate the security architecture, as the UE cannot verify the message's authenticity or origin. By ignoring the non-compliant protected message, the UE adhered to the standard and avoided potential security risks like processing forged network commands. Secure
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. However, the AMF responded with a Configuration Update Command (CUC) marked as "Integrity protected and ciphered" (security header type 2) despite 5G-AKA authentication not being completed. According to 3GPP TS 33.501, NAS security (integrity protection and ciphering) must be activated *only after* successful 5G-AKA, which establishes the necessary keys. Sending a protected CUC before authentication violates this requirement, as the UE lacks keys to verify or decipher the message. The UE correctly provided no response, as processing such a message without validated security context could expose it to malicious reconfigurations or downgrade attacks. By ignoring the invalid protected command, the UE adhered to security protocols, preventing potential exploitation of unauthenticated sessions. 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 at this stage since 5G-AKA authentication had not yet been completed. The AMF responded with a DownlinkNASTransport message containing a Service Accept, which was marked as "Protected" (indicating it was integrity-protected or encrypted). Critically, 5G-AKA had not been performed, meaning no security context (K~AMF~, derived keys) existed between the UE and AMF. According to 3GPP TS 33.501, NAS protection (integrity and confidentiality) must only be applied *after* successful 5G-AKA and NAS Security Mode Command (SMC) procedures. The UE exhibited no response to this protected Service Accept message. This lack of reaction is non-compliant with 3GPP standards: the UE should have rejected the message by initiating a recovery procedure (e.g., restarting registration or sending a failure indication), as accepting or ignoring an unsolicited protected message without an established security context could expose it to man-in-the-middle attacks or spoofed network commands. The UE's failure to challenge or respond to this anomalous condition indicates a security flaw in its implementation. Insecure
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 to the AMF, as expected without established security. The AMF then responded with a Service Accept message marked as "Protected," despite 5G-AKA not being completed and no security context existing. The UE, instead of rejecting this improperly protected message or initiating error handling, proceeded to send a Deregistration Request. According to 3GPP standards (TS 33.501), NAS messages requiring protection (like Service Accept) must only be sent after successful 5G-AKA establishes security keys. The UE's acceptance of a protected Service Accept without authentication violates this requirement, as it implies a failure to validate message security. Furthermore, the UE's subsequent Deregistration Request—sent without established security—demonstrates inconsistent behavior, though its protection status is unspecified. This sequence indicates the UE did not enforce downlink message security, creating a vulnerability where malicious protected messages could be accepted prematurely. 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 to the AMF, as part of the initial NAS procedures. Subsequently, the AMF sent a Deregistration Request (UE-terminated) marked as "Integrity protected and ciphered" (security header type 2) without completing the 5G-AKA authentication procedure. According to 3GPP standards (TS 33.501), NAS message protection (integrity and ciphering) requires a successfully established security context derived from 5G-AKA. Since 5G-AKA was not completed, the UE lacked the necessary keys to validate or decrypt the protected message. The UE correctly discarded the Deregistration Request, as it could not verify its authenticity or integrity, and provided no response. This aligns with 3GPP security protocols, which mandate that UEs must ignore protected NAS messages received before security context establishment to prevent processing potentially malicious commands. The UE's adherence to this requirement—despite the AMF's non-compliant protected message—demonstrates secure behavior. 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 UE initiated communication by 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 protected downlink NAS message (5GMM status with cause #98 – "message type not compatible with protocol state"), which was inappropriate since security keys were not established. The UE correctly refrained from responding to this protected message, as per 3GPP TS 24.501 and TS 33.501, which mandate that protected NAS messages must not be sent or processed before successful authentication and key agreement. By ignoring the improperly protected message instead of attempting decryption or responding, the UE avoided potential security risks such as processing malformed/unverified packets or exposing vulnerability to downlink injection attacks during the initial unprotected phase. This adherence to protocol state machines and rejection of out-of-context protected messaging aligns with 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 UE initiated the NAS communication by sending an unprotected Initial Registration Request, as expected prior to 5G-AKA completion. The AMF responded with a protected DownlinkNASTransport message containing a 5GMM Status (cause #3 – "Illegal UE"). Since 5G-AKA had not been performed, no security context existed for the UE to validate or decrypt protected NAS messages. Per 3GPP TS 24.501 and TS 33.501, the UE must discard protected NAS messages received without an established security context, as they cannot be authenticated. The UE correctly adhered to this requirement by providing no response, avoiding potential processing of unverified or malicious network commands. This behavior demonstrates strict compliance with 5G security protocols, which mandate that NAS protection (integrity/confidentiality) is only enforceable post-successful 5G-AKA. 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] 0.0008118152618408203 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 UE initiated communication by sending an unprotected Initial Registration Request. The AMF responded with a Security Mode Command (SMC) marked as "Integrity protected with new security context" using integrity algorithm 128-5G-IA2, while explicitly selecting null ciphering (5G-EA0). Crucially, this occurred before 5G-AKA authentication was completed, meaning no shared keys existed for security context validation. The UE rejected this SMC with a "5GMM status (Invalid mandatory information)" response, correctly identifying the AMF's premature activation of integrity protection without established keys as a protocol violation. This aligns with 3GPP TS 24.501 and TS 33.501, which mandate that security context activation via SMC must follow successful authentication and key agreement. By refusing to process an integrity-protected command without valid keys and signaling the error, the UE enforced fundamental security requirements, preventing potential exploitation of unauthenticated contexts. 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 sending an Identity Request for the GUTI in plain text, as 5G-AKA had not yet been completed to establish a security context. The UE failed to respond to this request. According to 3GPP standards (TS 33.501), before 5G-AKA completion, NAS messages like Identity Request are permitted to be sent unprotected, and UEs must respond to requests for non-sensitive identities such as GUTI even without security activation. The GUTI, being a temporary identifier, does not require the same protection level as permanent identities (e.g., SUPI). The UE's lack of response deviates from the protocol, which mandates compliance with such requests to maintain service continuity and network procedures. This non-response could disrupt authentication, indicating non-compliant behavior that undermines protocol reliability and interoperability. 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 (likely to an initial Identity Request from the AMF, possibly for a temporary or non-sensitive identifier like SUCI). Subsequently, the AMF sent a new Identity Request in plain text (unencrypted and without integrity protection), explicitly demanding the IMEISV—a permanent equipment identifier. The UE did not respond to this request. Since the 5G-AKA authentication had not yet been completed, no security context (including encryption or integrity protection) was established, as mandated by 3GPP standards (TS 33.501 and TS 24.501) for securing sensitive data. The IMEISV is considered sensitive personal data, and 3GPP requires it to be protected under a security context to prevent tracking or spoofing. By withholding the IMEISV in the absence of security, the UE adhered to the standard's privacy and security protocols, which prohibit transmitting such identifiers unprotected. This behavior mitigates risks like eavesdropping or identity capture by untrusted networks. 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 to the AMF, followed by the AMF requesting the UE's TMSI via a plain-text Identity Request—consistent with 5G standards, as NAS messages remain unencrypted prior to 5G-AKA completion. However, the UE failed to respond to the Identity Request. According to 3GPP TS 24.501, a UE must always reply to an Identity Request with either the requested identity (e.g., TMSI) or a valid cause code (e.g., if the identity is unavailable). This requirement applies even during pre-authentication communication, as the protocol relies on these exchanges to progress toward security establishment. The UE's lack of response violates the standard, disrupts the authentication workflow, and could indicate improper handling of unprotected NAS messages. Such behavior risks protocol stalling or exploitation, as unresponsive UEs might evade legitimate network queries or mask vulnerabilities to malicious actors. 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 unprotected Authentication Response to the AMF as part of the ongoing 5G-AKA procedure. Before 5G-AKA could complete (as explicitly noted in the test summary), the AMF sent a Deregistration Request message to the UE. This downlink message was marked as "Protected" with a security header indicating integrity protection (value 1). Crucially, the UE provided no response to this Deregistration Request. According to 3GPP standards (TS 33.501 and TS 24.501), NAS message protection (integrity/encryption) requires a fully established security context derived from a completed 5G-AKA. Since 5G-AKA was incomplete, the UE lacked the necessary keys to verify the integrity of the Deregistration Request. The UE's lack of response aligns with security requirements: processing or acting upon such a protected message without a valid security context would violate the standard, as it could expose the UE to spoofed commands. By discarding the unverifiable message and not engaging further, the UE avoided potential exploitation (e.g., forced deregistration by a malicious actor) and adhered to security protocols. 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, establishing a security context with the AMF. The UE then sent a Registration Complete message, indicating the conclusion of its registration procedure. Subsequently, the AMF transmitted a Configuration Update Command to the UE as a plain NAS message (security header type 0), meaning it was neither integrity-protected nor encrypted. 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 active, all NAS messages—including Configuration Update Command—must be integrity-protected and encrypted to prevent tampering and eavesdropping. The UE's failure to reject or respond to this unprotected message violates these requirements, as it implicitly accepts an insecure command without enforcing mandatory security mechanisms. This behavior leaves the UE vulnerable to man-in-the-middle attacks, such as malicious network configuration changes. Insecure
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 activation of NAS security (encryption and integrity protection) following a prior Security Mode Command from the AMF. Subsequently, the AMF sent an Authentication Request message in plaintext (unprotected), which included RAND and AUTN parameters for authentication. The UE did not respond to this message. According to 3GPP standards (TS 24.501 and TS 33.501), once NAS security is activated via the Security Mode Complete message, all subsequent NAS messages—except specific exceptions like identity requests or emergency-related messages—must be protected with encryption and integrity. The Authentication Request does not fall under these exceptions and should have been protected. The UE's lack of response indicates it discarded the unprotected message, adhering to the standard by refusing to process it. This behavior prevents potential security exploits, such as downgrade attacks or injection of malicious commands. Secure

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 successful completion of 5G-AKA, establishing mutual authentication and security keys between the UE and AMF. The UE then sent a Security Mode Complete message, confirming activation of NAS security (integrity protection and encryption) for subsequent communications. However, the AMF responded with a Service Reject message (5GMM Cause 111: "Protocol error, unspecified") sent in plaintext, violating 3GPP TS 24.501 mandates that all post-security-activation NAS messages must be integrity-protected and encrypted. The UE correctly ignored this unprotected message, providing no response, as processing it would risk accepting unverified or malicious network commands. 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 between the UE and AMF began with the UE sending a **Security Mode Complete** message (indicating successful activation of NAS security context) and a **Registration Request**. The AMF then responded with a **DownlinkNASTransport** containing an **Authentication Request** sent in **plain text** without encryption or integrity protection. This sequence is problematic because the Security Mode Complete message confirms that both parties have agreed to enable security protections (encryption/integrity) for subsequent NAS messages, as mandated by 3GPP standards (TS 33.501). After this point, all NAS messages must be protected. However, the AMF's Authentication Request violated this requirement by being sent unprotected. The UE correctly **did not respond** to this request, adhering to 5G security protocols which require UEs to discard or ignore any NAS messages received without security protection after security context activation. This non-response demonstrates the UE's compliance with 3GPP security enforcement mechanisms, as processing an unprotected post-security-activation message would have constituted a vulnerability. 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 NAS security), and the AMF responded with a **Deregistration Accept** message sent in plaintext without encryption or integrity protection. According to 3GPP TS 33.501, once 5G-AKA and the Security Mode Command procedure are completed, *all subsequent NAS messages* must be integrity-protected and encrypted (if confidentiality is enabled). The UE, upon receiving an unprotected NAS message after security activation, must discard it and should not process it, as it fails mandatory security checks. In this test, the UE correctly **discarded the unprotected Deregistration Accept** by providing no response, adhering to 3GPP security requirements and preventing potential exploitation of unverified network instructions. 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 UE sending a Security Mode Complete message, confirming successful activation of NAS security following the 5G-AKA procedure. Subsequently, the AMF sent an Authentication Reject message in plaintext (unencrypted and without integrity protection). According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA completes and the Security Mode Command procedure finalizes (acknowledged by Security Mode Complete), all subsequent NAS messages must be protected using the established security context—applying both encryption and integrity protection where required. The Authentication Reject, being a post-security-activation NAS message, violated this mandate by being transmitted unprotected. The UE's lack of response—failing to discard the message or trigger security error handling—indicates non-compliance with 3GPP security clauses (e.g., TS 24.501 §4.4.4.3 and §5.4.1.2), which demand rejection of unprotected messages after security setup. This omission exposes the UE to potential exploitation via spoofed or manipulated reject commands. 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 began with the UE completing 5G-AKA authentication and sending a Security Mode Complete message, confirming successful activation of NAS security (integrity protection and encryption) as per the AMF's earlier Security Mode Command. The AMF then responded with an Authentication Reject message sent in plaintext, without any security protections. The UE provided no response to this unsolicited reject message. According to 3GPP TS 33.501, once NAS security is established (after Security Mode Complete), all subsequent NAS messages **must** be integrity-protected to prevent forgery and replay attacks. The Authentication Reject—a security-critical command—was transmitted unprotected, violating 5G standards. The UE correctly ignored this message, as processing an unprotected post-security-establishment NAS message would expose it to spoofing or disruption attacks. By discarding the invalid reject instead of acting on it or resetting its state, the UE adhered to security protocols. 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. Subsequently, the AMF transmitted an Identity Request (for TMSI) in plain text, without encryption or integrity protection. Critically, the UE provided no response to this request. According to 3GPP standards (TS 33.501 and TS 24.501), once security is activated—confirmed by the UE's Security Mode Complete—all subsequent NAS messages must be integrity-protected and encrypted (where applicable) to prevent tampering and eavesdropping. The Identity Request is not among the limited exceptions allowing unprotected transmission. By discarding the unprotected Identity Request instead of processing it, the UE adhered to the standard's security requirements, which mandate rejection of unsecured messages post-security activation to mitigate potential attacks like forgery or replay. The lack of response demonstrates correct security enforcement by the UE. Secure