UE Response Evaluation Report: Test time: 2025-07-18 11:03:51

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.	In this test scenario, after the UE initiated a registration request to the AMF, the AMF responded with an identity request message, specifically requesting the IMEI, and sent this message in plain (unencrypted) form. The UE, in turn, did not respond to this identity request. According to the 3GPP 5G security standards, particularly TS 33.501, sensitive information such as the IMEI should not be transmitted in plain text before the completion of the 5G-AKA authentication and key agreement procedure, which establishes a secure, encrypted NAS signaling channel. By refusing to respond to the plain (unencrypted) identity request for the IMEI, the UE is adhering to the security guidelines that protect user privacy and device identity from potential interception or exposure before encryption is in place. This behavior demonstrates that the UE is following the 3GPP security requirements by not disclosing the IMEI in an unprotected manner. Therefore, the UE's action in this scenario is considered secure. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. In response, the AMF sent an identity request, specifically requesting the SUCI (Subscription Concealed Identifier), which is a privacy-preserving identifier designed to protect the subscriber's permanent identity (SUPI) during initial registration. The AMF's identity request was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that security context and encryption had not yet been established. The UE responded by providing an identity response, presumably containing the SUCI, also in plain text. According to the 3GPP 5G security standards, it is expected and secure for the UE to send the SUCI in response to an unprotected identity request prior to the completion of 5G-AKA, as the SUCI is specifically designed to be sent over an unprotected channel without revealing the permanent subscriber identity (SUPI). Therefore, the UE's actions in this scenario are compliant with the 5G security requirements and do not expose sensitive information. 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.	In this test scenario, the UE initiated NAS communication by sending an initial registration request to the AMF, which is expected behavior for a 5G standalone device beginning the attach procedure. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as encryption and integrity protection are not yet activated. The UE, upon receiving an Authentication Reject message in this state, is expected to silently discard the message and not respond, as per 3GPP TS 24.501, which states that the UE should not take further action or attempt to re-register immediately. In this test, the UE did not respond to the plain Authentication Reject, which aligns with the expected secure behavior defined by the standard, preventing potential downgrade or denial-of-service attacks that could be triggered by unauthenticated reject messages. Therefore, the UE's action was secure. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. In response, the AMF sent an identity request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE then responded with an identity response containing the requested SUCI. Importantly, this exchange occurred before the completion of the 5G-AKA (Authentication and Key Agreement) procedure, meaning that the NAS messages exchanged between the UE and AMF were sent in plain (unencrypted) form. According to the 3GPP 5G security standard, it is expected and acceptable for the initial registration and identity request/response messages to be transmitted in plain text prior to the establishment of a security context via 5G-AKA. The use of SUCI, which is a privacy-preserving, concealed version of the permanent subscriber identity (SUPI), is specifically designed to protect the user's identity even when sent without encryption at this early stage. Therefore, the UE's action in providing the SUCI in response to the AMF's plain identity request, before security activation, aligns with the 3GPP security requirements and does not expose sensitive information. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. Since the 5G-AKA authentication procedure had not yet been completed, the NAS messages exchanged between the UE and AMF were unencrypted (plain). The AMF, under test control, responded with a registration reject message using 5GMM Cause 111 (protocol error, unspecified), also sent in plain text as per the 3GPP standard before security activation. Upon receiving the registration reject, the UE responded by sending a deregistration request (UE originating), again in plain text. According to 3GPP specifications (TS 24.501), before the completion of 5G-AKA and the establishment of NAS security, all NAS messages are expected to be sent unprotected (plain). The UE's behavior—sending a deregistration request in response to a registration reject prior to security activation—aligns with the standard, as the UE cannot initiate NAS encryption until authentication and key agreement are completed. Therefore, the UE's actions were consistent with 3GPP security requirements for this stage of the registration process, and no security breach or deviation from the standard occurred. Secure
6	6	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 22 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0009021759033203125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Congestion) 0.20517516136169434 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under tester control, responded with a Registration Reject message (5GMM Cause 22: Congestion) before the 5G-AKA authentication procedure was completed. Notably, since 5G-AKA had not yet occurred, all NAS messages—including the Registration Reject—were sent in plain (unencrypted) form, as per 3GPP standards, which require security context establishment (via 5G-AKA) before NAS message encryption. Upon receiving the Registration Reject, the UE responded appropriately by sending a Deregistration Request (UE originating), also in plain text, since no security context existed. According to 3GPP TS 24.501, the UE is expected to accept and process Registration Reject messages sent in plain text prior to authentication, and it is correct behavior for the UE to deregister in response. Therefore, the UE's actions strictly adhered to the 3GPP security procedures for the pre-authentication phase, and no sensitive user data was exposed in this exchange. The UE did not accept any insecure procedures or behave in a way that would compromise its security posture. Secure

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.	In this test scenario, after the UE initiated a registration request to the AMF, the AMF responded with an authentication request message. Notably, this authentication request was sent in plain (unencrypted) form, and the authentication vectors provided (RAND and AUTN) were either all zeros or otherwise invalid. The UE, upon receiving this authentication request, responded with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, the UE should not proceed with authentication if the authentication request is invalid, malformed, or does not conform to expected 5G-AKA procedures. The UE is also expected to reject authentication attempts that do not use proper cryptographic protections or that attempt to downgrade security. By refusing to proceed and explicitly indicating that the authentication method was unacceptable, the UE correctly protected itself from a potentially insecure or malicious authentication attempt. This behavior aligns with the security requirements of the 5G standard, as the UE did not accept an authentication procedure that could compromise its security or privacy. Therefore, the UE's action in this scenario was secure. 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: 31303030000000078742b94d4550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005857944488525391 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20240378379821777 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an Initial Registration Request to the AMF. The AMF, under test control, responded with an Authentication Request message that was sent in plain (unencrypted) form and contained invalid or incomplete authentication parameters (e.g., AUTN was all zeros, ABBA was 0000, and the message was not integrity protected since 5G-AKA was not yet completed). Upon receiving this, the UE did not proceed with the authentication procedure but instead responded with a 5GMM Status message indicating "Invalid mandatory information." According to the 3GPP 5G security standards, the UE must not proceed with authentication or establish a security context if the authentication request is malformed, missing mandatory fields, or appears suspicious. Instead, it should report the error and halt further sensitive communication until a valid authentication request is received. By sending a status message and not proceeding with authentication, the UE adhered to the security guidelines, thereby protecting itself from potential downgrade or spoofing attacks that could arise from processing unauthenticated or tampered messages. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, the UE and AMF are engaged in NAS (Non-Access Stratum) communication, specifically during the identity management phase before the completion of 5G-AKA (Authentication and Key Agreement). The UE first sends an identity response to the AMF, after which the AMF issues another identity request for the SUCI (Subscription Concealed Identifier), sent in plain (unencrypted) form. The UE then responds again with an identity response. According to the 3GPP 5G standards, before 5G-AKA is completed, NAS messages—including identity requests and responses—are transmitted in plain text, as encryption and integrity protection are only activated after successful authentication and key establishment. The UE is expected to provide the SUCI (which is a privacy-preserving, concealed version of the SUPI) in response to identity requests prior to authentication, specifically to protect the subscriber's permanent identity even when messages are unprotected. Since the UE responded with a SUCI (not the SUPI) and followed the expected protocol behavior by responding to identity requests in plain text before security activation, the UE's actions align with 3GPP security requirements. Therefore, the UE's behavior in this test was secure according to the standard. 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: 31313131313131313131006f90d2550000 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 0.039749860763549805 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399777889251709 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2409358024597168 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE responded to an identity request from the AMF with an identity response. The AMF then sent an authentication request to the UE, but this message was sent in plain (unencrypted) text, as the 5G-AKA authentication procedure had not yet been completed and thus no NAS security context was established. The authentication request included parameters such as ABBA, RAND, AUTN, and indicated a native security context with ngKSI_KSI set to 2. Upon receiving this, the UE replied with an authentication failure message, specifically stating "ngKSI already in use." According to the 3GPP 5G standards, the UE is required to ensure that a new security context is not established with an already active ngKSI value, as this could indicate a replay or downgrade attack. By refusing to proceed with authentication under these circumstances and reporting the error, the UE is following the security guidelines set forth in the standard to prevent potential security breaches. This action demonstrates that the UE is correctly implementing the required security checks and is not vulnerable to this class of attack, as it does not proceed with authentication or establish a security context when there is a risk of key reuse or replay. Therefore, the UE's behavior in this scenario is secure. 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.	In this security test, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After completing the initial NAS procedures, the UE sent an Identity Response message to the AMF, which was transmitted in plain text since the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed. Subsequently, the AMF responded with a Service Reject message (cause: PLMN not allowed), also sent in plain text. The UE did not respond further after receiving the Service Reject. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA are permitted to be sent unencrypted, as security context and ciphering keys are not yet established. The UE's behavior—sending the Identity Response in plain text and ceasing communication after receiving the Service Reject—aligns with the expected protocol and does not expose the UE to additional risk, given that no sensitive user data or credentials are transmitted prior to authentication. Therefore, based on the 3GPP standard and the observed actions, the UE's behavior in this scenario is considered secure. 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.	In this test scenario, the UE participated in NAS communication with the AMF, where the 5G-AKA authentication procedure had not yet been completed. The UE first sent an identity response, after which the AMF issued another identity request, specifically requesting the SUCI (Subscription Concealed Identifier). The UE responded with another identity response. Importantly, the AMF sent its identity request message in plain (unencrypted) form, which is expected since encryption is only established after successful completion of the 5G-AKA procedure. According to the 3GPP 5G standard, prior to the completion of 5G-AKA, NAS messages, including identity requests and responses, are transmitted in plain text. However, the UE is required to never send its permanent identifier (SUPI) in plain text; instead, it must respond with the SUCI, which is a privacy-preserving, concealed version of the SUPI, even before security is activated. In this interaction, the UE complied by responding with the SUCI when requested, thus protecting the subscriber's permanent identity as per 3GPP requirements. Therefore, the UE's actions were secure and aligned with the 5G standard, as it did not expose sensitive information in the clear and followed the prescribed identity protection mechanisms. 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.	In this test scenario, the UE completed the initial NAS procedures and sent an Identity Response message to the AMF. The AMF, under test control, responded with an Authentication Reject message, which was sent in plain (unencrypted) form because the 5G-AKA authentication procedure had not yet been completed—meaning no NAS security context had been established. According to the 3GPP 5G standard, messages exchanged before the completion of 5G-AKA (such as identity requests and responses, and authentication requests and rejects) are permitted to be sent in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. The UE, upon receiving the Authentication Reject message, did not respond further, which is the expected and secure behavior as per the standard; the UE should terminate the procedure and not proceed with further communication when authentication is rejected. Therefore, the UE's actions were in line with 3GPP security requirements, as it did not expose any sensitive information or continue communication after authentication failure. 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.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After completing the initial NAS steps, the UE responded to an identity request by sending an Identity Response message to the AMF. Subsequently, the AMF, under tester control, sent a Registration Reject message with 5GMM Cause 22 (Congestion) to the UE. Importantly, this Registration Reject message was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning no NAS security context had been established. According to the 3GPP 5G standard (TS 24.501), before the completion of 5G-AKA, all NAS messages, including Registration Reject, are permitted to be sent in plain text, since encryption and integrity protection are only applied after a security context is established. The UE, upon receiving the Registration Reject, did not respond further, which is compliant with the standard, as the UE is expected to cease registration attempts upon receiving such a message. Therefore, the UE's actions—sending the Identity Response in plain text before security activation and not responding to a plain Registration Reject—are in line with 3GPP security requirements and do not introduce any security vulnerability in this context. 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.	In this test scenario, after the initial NAS procedures, the UE responded to an identity request from the AMF with an identity response. The AMF then sent an authentication request to the UE, but this request was sent in plain (unencrypted) form and included suspicious or invalid authentication parameters, such as an AUTN (Authentication Token) of all zeros and a RAND (random challenge) with a non-random value. The UE, upon receiving this authentication request, did not proceed with the 5G-AKA authentication procedure. Instead, it immediately responded with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, the UE is required to verify the validity of authentication challenges and reject any that are malformed, non-compliant, or potentially insecure, especially before a secure context is established. By refusing to proceed with authentication in the presence of an invalid or insecure authentication request, the UE is correctly implementing the security requirements of the standard and protecting itself from potential attacks or protocol downgrades. Therefore, the UE's action in this scenario was secure, as it did not accept or process a potentially insecure authentication procedure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF, which is the expected behavior. Subsequently, the AMF sent a Security Mode Command to the UE. However, the Security Mode Command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the "Security header: Plain NAS message (0)" and confirmed by the packet capture. According to the 3GPP 5G standard (TS 24.501), the Security Mode Command is always sent as a plain NAS message because, at this stage, NAS security (ciphering and integrity protection) has not yet been activated; the Security Mode Command is precisely the message that establishes which algorithms to use for subsequent protected communication. The UE, in this test, did not respond to the Security Mode Command. This lack of response is a secure behavior if the UE detected that the Security Mode Command was not valid, tampered with, or did not meet expected security parameters (for example, if the message was replayed, malformed, or the ABBA value was unexpected). However, if the message was valid and the UE simply failed to respond, that could be a problem. In this context, since the Security Mode Command is supposed to be sent in plain text and the test was to explore security, the UE's refusal to proceed (no response) could indicate a secure reaction to a potential anomaly or attack scenario. Therefore, based on the 3GPP standard and the information provided, the UE's action of not responding to the Security Mode Command—assuming it detected a security issue—aligns with secure behavior. Secure
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.	In this test scenario, the 5G standalone User Equipment (UE) initiated NAS communication and, after completing the initial steps, sent an Authentication Response to the Access and Mobility Management Function (AMF). However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is necessary for establishing NAS security and encryption—the AMF responded with a Service Reject message, specifically indicating a protocol error (5GMM Cause: 111), and sent this message in plain (unencrypted) text. The UE, upon receiving this unprotected Service Reject message prior to the establishment of NAS security, did not respond further. According to the 3GPP 5G standard, the UE should not accept or act on critical NAS messages (such as Service Reject) received in plain text before NAS security is activated, as this could expose the UE to security risks such as spoofing or denial-of-service attacks. By not responding to the unprotected Service Reject message, the UE correctly adhered to the security requirements outlined by the 3GPP standard, ensuring that it did not process potentially insecure or malicious messages. Therefore, the UE's behavior in this scenario was secure. Secure

18	18	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 4.243709087371826 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 4.243997097015381 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Identity request 4.445895195007324 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, which then replied with an identity request asking for the SUCI (Subscription Concealed Identifier). Importantly, this identity request was sent as a plain (unencrypted) message because the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet activated. The UE responded to this plain identity request with an identity response, also sent in plain text. According to the 3GPP 5G standard (TS 24.501), it is expected that before the completion of 5G-AKA, NAS messages, including identity requests and responses, are sent unencrypted because the security context has not yet been established. Furthermore, the SUCI is specifically designed to be a privacy-preserving identifier, protecting the subscriber's permanent identity (SUPI) even when sent in plain text. Therefore, the UE's action—responding to a plain identity request with a SUCI in plain text before security activation—aligns with the 3GPP security requirements and does not expose sensitive information. Based on this analysis, the UE's behavior in this scenario is compliant with the 5G standard and is considered secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was protected with integrity using the 128-5G-IA2 algorithm but specified the use of the null ciphering algorithm (5G-EA0), meaning that subsequent messages would not be encrypted. The UE responded with a Security Mode Reject message, indicating that it refused to accept the proposed security configuration, citing an unspecified reason. According to the 3GPP 5G security standards, after authentication, the UE and the network must negotiate both integrity and ciphering algorithms to protect NAS signaling. The use of the null ciphering algorithm (5G-EA0) is only allowed in very limited scenarios, typically for emergency services or when explicitly permitted by the UE's security policy. For normal operations, the UE is expected to reject a security mode command that proposes no encryption, as this would expose NAS signaling to eavesdropping and compromise confidentiality. The UE's action to reject the security mode command when only integrity protection was provided, and encryption was omitted, aligns with the security requirements of the 5G standard, as it prevents insecure communication. Therefore, the UE's behavior in this test was appropriate and secure according to 3GPP specifications. 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.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, and the AMF replied with another authentication request, which was sent in plain (unencrypted) form. The 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, which is a prerequisite for establishing a secure NAS security context and enabling encryption of subsequent NAS messages. According to the 3GPP 5G standard, until 5G-AKA is completed and security context is established, NAS messages—including authentication requests and responses—are permitted to be sent in plain text. The UE, upon receiving the plain authentication request, responded with another authentication response, also in plain text, as expected before security activation. This behavior aligns with the 3GPP specification, which allows unprotected NAS messages prior to the completion of authentication and key agreement. Therefore, the UE's actions were consistent with the standard and did not expose it to additional risk, given the state of the authentication process. 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.	In this test scenario, the UE and AMF were engaged in the NAS authentication procedure as part of the 5G-AKA process. After the UE sent an authentication response, the AMF, under test control, sent another authentication request to the UE, but this message was sent in plain (unencrypted) format and included specific authentication parameters (RAND, AUTN, ABBA, etc.). The UE, upon receiving this authentication request, responded with an "Authentication failure (MAC failure)" message. According to the 3GPP 5G standard, the UE is required to verify the integrity and authenticity of the authentication request, specifically checking the Message Authentication Code (MAC) in the AUTN parameter. If the MAC check fails, the UE must not proceed with authentication and should respond with an authentication failure indicating a MAC failure. This is a critical security measure to prevent replay or tampering attacks, especially before a secure context is established (i.e., before 5G-AKA is completed and NAS encryption is enabled). In this test, the UE correctly detected the MAC failure and refused to proceed, thus adhering to the 3GPP security requirements and protecting itself from a potentially malicious or malformed authentication request. Therefore, the UE's actions were secure and in line with the 5G standard. Secure

22	22	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3200 RAND: 303030303030300078b457a1d8550000 AUTN: 313131313131313310057a1d8550000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.11977601051330566 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999082565307617 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.3230268955230713 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, which then replied with another authentication request message. Notably, this subsequent authentication request from the AMF was sent in plain (unencrypted) form, and the 5G-AKA procedure had not yet been completed, meaning that a secure NAS security context had not been established. Upon receiving this plain authentication request, the UE responded with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it rejected the authentication attempt because it did not conform to 5G security requirements. According to the 3GPP 5G standard, after the initial authentication request/response exchange, further authentication requests should only be sent within a protected (encrypted and integrity-protected) NAS security context, unless the context has not yet been established. Since the AMF sent an additional authentication request in plain text after the UE had already responded, the UE correctly identified this as a security violation and refused to proceed. This behavior aligns with the 3GPP security specifications, as the UE did not accept potentially insecure or replayed authentication messages outside of a protected context. Therefore, the UE's action was secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command to the UE, specifying the use of the 5G-EA0 (null) ciphering algorithm (meaning no encryption) and the 128-5G-IA2 integrity algorithm, with the security header indicating that the message was integrity protected with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standards, after authentication, the UE and network must negotiate security algorithms for both integrity and ciphering. The use of 5G-EA0 (null ciphering) means that user data and signaling would not be encrypted, which is generally only allowed in exceptional cases (e.g., for emergency services or in specific regulatory environments). For normal operation, the UE is expected to reject the use of null ciphering to ensure confidentiality of communications. The UE's action to reject the Security Mode Command when only null ciphering was proposed aligns with the security requirements of the 5G standard, as it prevents the establishment of an insecure session. Therefore, the UE's behavior was secure and compliant with 3GPP security guidelines. Secure

24	24	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 5781adc4c6cd42baaf6e4fe6cef2e17f AUTN: 67373384aeb990006bc203d2c023b868 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication response The packet capture during the test using wireshark is: 0.11973094940185547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12026000022888184 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.32166409492492676 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication as part of the 5G-AKA authentication procedure. After the initial NAS steps, the UE sent an authentication response to the AMF. However, instead of proceeding to the next step in the authentication sequence, the AMF sent another authentication request to the UE, and this message was sent in plain (unencrypted) form. The UE, upon receiving this second authentication request, responded again with an authentication response. According to the 3GPP 5G standard, the authentication and key agreement (5G-AKA) procedure must be completed before any NAS messages containing sensitive information are exchanged in plain text; after authentication, NAS security (encryption and integrity protection) should be activated to protect further communication. In this test, since the 5G-AKA was not completed and the AMF sent a repeated authentication request in plain text, the UE responded to this unexpected and potentially insecure message by providing another authentication response, also in plain text. This behavior is problematic because the UE should not respond to repeated or unexpected authentication requests after already providing a valid authentication response, especially before NAS security is established. This could expose the UE to replay or downgrade attacks, as it is responding to potentially malicious or out-of-sequence requests without the protection of encryption or integrity. Therefore, based on the 3GPP standard, the UE's action in responding to a repeated plain-text authentication request after already responding once is considered insecure. **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.	In this test scenario, the UE initiated NAS communication with the AMF and, after completing the initial steps, sent an Authentication Response as part of the 5G-AKA procedure. However, before the 5G-AKA process could be completed (i.e., before security context establishment and NAS encryption), the AMF sent an Authentication Reject message to the UE in plain (unencrypted) form. Upon receiving this Authentication Reject, the UE did not attempt to continue with further NAS procedures but instead responded with a Deregistration Request, also sent in plain text, as the security context had not been established. According to the 3GPP 5G standard, if the authentication procedure fails or is rejected before security is activated, the UE is expected to abort further procedures and may deregister from the network. The UE must not attempt to establish a secure context or send sensitive information in plain text. In this case, the UE's action of sending a Deregistration Request after receiving an Authentication Reject, without attempting to proceed further or send protected messages, aligns with the expected secure behavior as per the standard. The UE did not expose itself to additional risk by continuing communication without security. Therefore, the UE's behavior in this scenario was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message, indicating that NAS security (integrity protection and ciphering) was established. The AMF then sent a Deregistration Request message, which was protected using the agreed security context (as indicated by the security header: integrity protected and ciphered). The UE responded with a Deregistration Accept message, also under NAS security protection. According to the 3GPP 5G standard, once the security context is established (after 5G-AKA and Security Mode Complete), all subsequent NAS messages between the UE and AMF must be integrity protected and ciphered. The packet capture confirms that both the downlink Deregistration Request and the uplink Deregistration Accept were transmitted with the appropriate security protections in place. The UE did not process or respond to any unprotected NAS messages after security was established, and it correctly followed the protocol by only accepting and responding to protected messages. Therefore, the UE's actions were in line with the 3GPP security requirements, and its communication can be considered secure. Secure
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.	In this test scenario, the 5G-AKA authentication procedure was successfully completed, establishing a secure context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent a "security mode complete" message, indicating that it had accepted the negotiated security algorithms and was ready to communicate securely. The AMF then sent a "deregistration request" to the UE, which was protected with both integrity and ciphering, as indicated by the security header (2). The UE responded with a "deregistration accept" message, completing the deregistration procedure. According to 3GPP 5G standards, after the successful completion of 5G-AKA and security mode procedures, all subsequent NAS messages must be integrity protected and, where required, ciphered. The packet capture confirms that the deregistration request from the AMF was indeed protected, and the UE responded appropriately. The UE's actions—accepting only protected messages and responding after security was established—are in line with 3GPP requirements, ensuring that sensitive signaling is not exposed to interception or tampering. Therefore, the UE's behavior in this interaction was secure and compliant with the 5G standard. Secure

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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the security parameters previously negotiated. However, the AMF then sent a second "security mode command" message, which was protected and specified the use of ciphering algorithm 128-5G-EA2 and integrity algorithm 5G-IA0 (null), with the security header indicating "integrity protected with new security context." Upon receiving this, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, after the security context is established and the security mode is completed, the AMF should not send another security mode command unless a new security context is required (e.g., due to a handover or re-authentication). Furthermore, the use of the null integrity algorithm (5G-IA0) is generally discouraged for normal operation, as it does not provide integrity protection for NAS messages, which is a potential security risk. The UE's decision to reject the security mode command—especially with the null integrity algorithm—demonstrates adherence to security best practices by refusing to operate under insecure conditions or unexpected protocol flows. Therefore, the UE's action was secure and in line with the 3GPP standard, as it protected itself from potentially insecure or non-standard operations initiated by the AMF. 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.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. However, the AMF then sent another "security mode command" message, which was protected, but specified the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, meaning that subsequent NAS messages would not be encrypted or integrity protected. Upon receiving this, the UE responded with a "security mode reject" message, refusing to proceed with the insecure security configuration. According to the 3GPP 5G standard (TS 24.501), the use of null algorithms (EA0/IA0) is only allowed in very specific scenarios, such as emergency services or when explicitly permitted by the UE. In normal operation, the UE is expected to reject a security mode command that attempts to downgrade security to null algorithms after authentication has been completed. The UE's action to reject the insecure security mode command aligns with 3GPP security requirements and demonstrates proper security behavior by not accepting a downgrade attack or insecure configuration. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity protection). However, the AMF then sent another "security mode command" to the UE, which is not the expected sequence according to the 3GPP 5G NAS protocol. Normally, after the UE sends "security mode complete," the security context is established, and further NAS messages should be protected using the agreed algorithms. The packet capture shows that after the initial "security mode complete," the UE again sent a "security mode complete" message in response to the subsequent "security mode command" from the AMF. This behavior is problematic because, per 3GPP TS 24.501, the UE should only respond to a "security mode command" once per security context establishment; receiving and responding to a second such command without resetting the context or re-authenticating may indicate that the UE is not properly tracking the NAS security state machine or is allowing unexpected state transitions. This could expose the UE to replay or downgrade attacks, as it may allow an attacker to trigger repeated security mode negotiations. Therefore, the UE's action of accepting and responding to a second "security mode command" after already completing the security mode procedure is not compliant with the 5G standard and is considered insecure. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the negotiated security algorithms (ciphering with 5G-EA4 and integrity protection with 5G-IA0, which is the null integrity algorithm). Subsequently, the AMF sent a "security mode command" message, which was protected (ciphered and/or integrity protected) as per the new security context. The UE then sent a "deregistration request (UE originating)" message. According to the 3GPP 5G standard, after 5G-AKA, all NAS messages should be protected using the agreed security algorithms. However, the use of 5G-IA0 (null integrity) means that while the messages are encrypted, they are not integrity protected, which exposes the communication to potential replay or modification attacks. The UE's acceptance of a null integrity algorithm (5G-IA0) is generally discouraged in 3GPP standards except for specific, limited scenarios, as it weakens the security guarantees. Since the UE proceeded to send sensitive signaling (deregistration request) without integrity protection, this behavior is considered insecure according to 3GPP security requirements, which expect both confidentiality and integrity protection for NAS signaling after security activation. 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.	In this 5G standalone security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to protect subsequent NAS messages. However, the AMF then sent another "security mode command" message, which was protected (integrity protected and ciphered) using the agreed-upon algorithms (5G-EA4 for ciphering and 128-5G-IA3 for integrity). According to the 3GPP 5G standard (TS 24.501), once the UE has sent "security mode complete," it expects all further NAS messages to be protected, and it should not receive another "security mode command" unless a new security context is being established (which would require a new authentication procedure). The UE, upon receiving this unexpected and redundant "security mode command," did not respond, which aligns with the 3GPP specification that the UE should ignore or silently discard such messages to prevent potential security vulnerabilities such as replay or downgrade attacks. By not responding, the UE demonstrated correct and secure behavior according to the standard, ensuring that its security context was not compromised by an out-of-sequence or potentially malicious message. 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.	In this test scenario, the UE and AMF completed the 5G-AKA authentication, establishing a secure context for subsequent NAS message protection. After this, the UE sent a "security mode complete" message, confirming that it had activated the negotiated security algorithms. The AMF then sent a protected 5GMM status message with cause 6 ("Illegal ME"), which the UE received. In response, the UE sent a deregistration request (UE originating) to the AMF. According to the 3GPP 5G standards, after security mode completion, all subsequent NAS messages must be integrity protected and, if possible, ciphered. The packet capture confirms that the AMF's status message was protected, and the UE's deregistration request was sent after receiving a status indicating an illegal ME (Mobile Equipment). The UE's action to deregister itself upon receiving an "Illegal ME" cause is compliant with 3GPP TS 24.501, which specifies that the UE should initiate deregistration when it is informed that it is not allowed to access the network. Since all messages after authentication were protected and the UE responded appropriately to the network's status message, the UE's actions were secure and in accordance with the 5G standard. Secure

34	34	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15963101387023926 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15987801551818848 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unprotected) 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (integrity protection and ciphering) was established. Subsequently, the AMF sent a "deregistration request" to the UE, which was protected with both integrity and ciphering as indicated by the security header. The UE responded with a "deregistration accept" message, also protected, thereby completing the deregistration process. According to the 3GPP 5G standard, once NAS security is activated (after 5G-AKA and security mode complete), all subsequent NAS messages—including deregistration—must be integrity protected and ciphered. The packet capture confirms that the UE only sent protected messages after security activation, and it properly responded to a legitimate, protected deregistration request from the AMF. There is no evidence of the UE accepting or responding to unprotected or suspicious messages after security was established. Therefore, based on the 3GPP standard and the observed behavior, the UE acted securely in this interaction. Secure
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.	In this test scenario, the 5G-AKA authentication procedure was successfully completed, establishing the necessary security context for subsequent NAS message protection. The UE then sent a "security mode complete" message, indicating that it had accepted the security algorithms and was ready to communicate securely. Following this, the AMF sent a "service accept" message, which was properly protected (i.e., integrity protected and ciphered) according to the packet capture. However, after receiving the protected "service accept" message, the UE did not respond further. According to the 3GPP 5G standard, once the security context is established and NAS security is activated, the UE is expected to process protected messages from the AMF and respond appropriately, unless there is a protocol reason not to. The lack of response from the UE after receiving a correctly protected message suggests that the UE either failed to process the message or did not behave as specified by the standard. This could indicate a failure in handling protected NAS messages, which is a security concern because it may expose the UE to denial of service or other vulnerabilities if it cannot properly process secure messages. Therefore, based on the observed behavior and 3GPP requirements, the UE's action in this scenario is considered insecure. Insecure

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.	In this test scenario, the 5G standalone User Equipment (UE) first completed the 5G-AKA authentication procedure, establishing a secure context for subsequent NAS communication. The UE then sent a "registration complete" message to the AMF, indicating successful registration. Immediately after, the AMF (under test control) sent a "deregistration request (UE terminated)" message to the UE, which was integrity protected and ciphered, as indicated by the security header value of 2. The UE responded with a "deregistration accept (UE terminated)" message, acknowledging the request. According to the 3GPP 5G standards, after the completion of 5G-AKA, all subsequent NAS messages must be integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions—accepting and responding to a properly protected deregistration request—align with the expected secure behavior defined by the standard. The UE did not process or respond to any unprotected or suspicious messages, and all its communications occurred within an established secure context. Therefore, based on the observed behavior and adherence to 3GPP security requirements, the UE's actions in this scenario were secure. Secure
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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "registration complete" message to the AMF, indicating that the initial NAS security procedures had been completed and that subsequent NAS messages should be protected (i.e., encrypted and integrity protected) as per 3GPP standards. The AMF then responded with a "service accept" message, which was correctly sent as a protected (encrypted) downlink NAS message. Following this, the UE sent a "deregistration request (UE originating)" to the AMF. According to 3GPP TS 24.501, once 5G-AKA is completed and NAS security is established, all subsequent NAS messages, including deregistration requests, must be sent as protected messages to ensure confidentiality and integrity. The packet capture shows that the UE followed the correct sequence: it waited for NAS security to be established before sending sensitive messages and responded to protected messages from the AMF appropriately. There is no indication from the provided capture that the UE sent any unprotected NAS messages after security was established. Therefore, the UE's actions were in line with 3GPP security requirements, maintaining the integrity and confidentiality of its communication throughout the interaction. Secure

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.	In this security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the initial registration process. Subsequently, the AMF sent a "Security Mode Command" message to the UE, which was integrity protected using a new security context, as indicated by the security header type (3). The message specified the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm. Importantly, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard, after receiving a Security Mode Command, the UE is required to verify the integrity of the message, check the proposed algorithms, and respond with a Security Mode Complete message if the command is valid and acceptable. If the AMF proposes the null ciphering algorithm (5G-EA0), the UE may accept it, but only if local policy allows; otherwise, it should reject the command or not respond. In this case, the UE's lack of response suggests that it either rejected the use of the null ciphering algorithm or detected an issue with the security context, which is a secure and standards-compliant behavior to prevent the establishment of an insecure connection. Therefore, the UE's action in this scenario aligns with the security expectations of the 5G standard. Secure
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.	In this test scenario, the 5G standalone User Equipment (UE) first completed the 5G-AKA authentication procedure, which is a prerequisite for establishing NAS security. Following this, the UE sent a "registration complete" message to the AMF, indicating successful registration. The AMF then sent a "configuration update command" to the UE, which, according to the packet capture, was transmitted with a security header indicating both integrity protection and ciphering (security header type 2). This means the message was both encrypted and protected against tampering, as required by 3GPP standards after successful authentication. The UE responded with a "configuration update complete" message, acknowledging receipt and processing of the command. According to 3GPP TS 24.501 and TS 33.501, after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF must be integrity protected and ciphered to ensure confidentiality and integrity. The UE's actions—accepting only protected messages after authentication and responding appropriately—align with these security requirements. Therefore, based on the message flow, the use of NAS security, and the adherence to 3GPP standards, the UE's actions in this test were secure. 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.	In this test scenario, after the completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "registration complete" message to the AMF, indicating that it had successfully registered and established a secure context. Following this, the AMF sent a "configuration update command" to the UE, which was observed in the packet capture as being integrity protected and ciphered, meaning it was both encrypted and authenticated according to the security header (value 2). The UE then responded with a "configuration update complete" message, confirming receipt and processing of the command. According to the 3GPP 5G security standards, after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF must be protected with both integrity and ciphering to ensure confidentiality and authenticity. The packet capture confirms that the downlink message from the AMF was protected, and the UE responded appropriately within the secure context. There is no indication that the UE sent or accepted any unprotected messages after security activation, nor did it behave in a way that would violate the 3GPP security requirements. Therefore, based on the observed actions and adherence to the 5G security procedures, the UE's actions were secure. Secure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior. The AMF then issued a "Security Mode Command" message, which was correctly protected (integrity protected with a new security context) and specified the use of 128-5G-EA2 for ciphering and 128-5G-IA2 for integrity. However, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after receiving a Security Mode Command that is properly protected and after 5G-AKA is completed, the UE is expected to process the command, derive the security keys, and respond with a Security Mode Complete message. The absence of a response from the UE indicates that it did not proceed with the security context activation as required. This is a deviation from the standard, as the UE should not ignore or fail to respond to a valid, protected Security Mode Command. The lack of response could potentially leave the communication insecure, as the security context is not established, and subsequent messages (such as the Service Request) may not be properly protected. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an UplinkNASTransport message to the AMF, which is expected behavior as NAS security should be active at this stage. The AMF then sent a protected Deregistration Accept message to the UE, indicating that the NAS security context was in use for this downlink message. According to 3GPP standards, upon receiving a protected Deregistration Accept message, the UE should process the message and respond appropriately, typically by ceasing NAS communication and releasing resources, or at least acknowledging the message if required by the procedure. However, in this test, the UE did not provide any response after receiving the protected Deregistration Accept. While the 3GPP TS 24.501 standard does not require an explicit response from the UE to a Deregistration Accept message (especially in the case of UE-initiated deregistration), it does require the UE to process the message and release the NAS security context. Since the UE did not send any further messages and there is no evidence of it continuing to use the NAS security context or sending unprotected messages, its behavior aligns with the expected secure handling of the deregistration procedure. Therefore, based on the information provided and the 3GPP standard, the UE's actions in this scenario were secure. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated uplink NAS communication by sending a UL NAS transport message to the AMF. Subsequently, the AMF responded with a configuration update command, which was sent as a protected message with both integrity protection and ciphering enabled, as indicated by the security header (2). Following this, the UE sent a deregistration request (UE originating) to the AMF. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected with integrity and ciphering to ensure confidentiality and authenticity. The packet capture confirms that the downlink message from the AMF was protected, and there is no indication that the UE sent any unprotected NAS messages after security activation. The UE's actions—responding only after the security context was established and using protected communication—align with the security requirements of the 5G standard. Therefore, based on the observed behavior and adherence to the 3GPP security procedures, the UE acted securely in this test scenario. Secure
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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a series of uplink NAS messages, including UplinkNASTransport and PDU session establishment requests, indicating that the security context was established and NAS messages should be protected. The AMF, under test control, responded with a deregistration request (UE terminated), which was sent with the security header indicating both integrity protection and ciphering, as required by 3GPP TS 33.501 for NAS signaling after authentication. The UE, upon receiving this protected deregistration request, responded with a Deregistration Accept message, also protected, thereby following the expected behavior outlined in the 3GPP standards. The UE did not accept or process any unprotected NAS messages after security activation, and all its responses were appropriately protected, ensuring confidentiality and integrity of the signaling. This demonstrates that the UE adhered to the 5G security requirements for NAS message protection post-authentication, and did not exhibit any insecure behavior in this interaction. Secure

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.	In this test scenario, the UE and AMF completed the 5G-AKA authentication procedure, which is a prerequisite for establishing NAS security (integrity protection and ciphering) as defined by the 3GPP 5G standard. After authentication, the UE sent an UplinkNASTransport message, and the AMF responded with a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent with a security header indicating that it was both integrity protected and ciphered, meaning it was encrypted and authenticated according to the NAS security context established during 5G-AKA. The UE then responded with a Configuration Update Complete message, which, by standard, should also be sent under NAS security protection. Since all sensitive NAS messages after 5G-AKA were exchanged with the appropriate security protections in place, and the UE responded as expected by the standard, the UE's actions adhered to the 3GPP security requirements for NAS message protection. Therefore, the UE's behavior in this interaction was secure. 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.	In this security test for a 5G standalone User Equipment (UE), the interaction began with the successful completion of the 5G-AKA authentication procedure, which is a prerequisite for establishing NAS security (encryption and integrity protection) between the UE and the Access and Mobility Management Function (AMF). Following this, the UE sent an Uplink NAS Transport message, after which the AMF responded with a Configuration Update Command. According to the packet capture, the Configuration Update Command from the AMF was sent as a protected message, specifically with the NAS security header indicating both integrity protection and ciphering (security header type 2). The UE then responded with a Configuration Update Complete message, also sent as an Uplink NAS Transport, indicating that it processed the command and maintained secure communication. Based on the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages carrying sensitive information must be both integrity protected and ciphered. The UE's actions—processing only protected messages and responding securely—align with these requirements. Therefore, the UE's behavior in this interaction was secure and compliant with the 3GPP 5G security standards. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, indicating that a secure NAS security context was established. Following this, the AMF sent a Configuration Update Command to the UE, which, according to the packet capture, was integrity protected and ciphered, as indicated by the security header (value 2). The UE then responded with a Configuration Update Complete message. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected by integrity and ciphering to ensure confidentiality and authenticity. The packet capture confirms that the downlink Configuration Update Command was sent as a protected message, and the UE responded appropriately, indicating that it accepted and processed the command within a secure context. Since the UE only responded to a protected, integrity-protected, and ciphered message after security activation, its actions align with the security requirements of the 5G standard, and no insecure behavior is observed in this interaction. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, indicating it was ready to proceed with further NAS signaling. The AMF then sent a Security Mode Command message, which was protected using the new security context established during 5G-AKA, specifying the use of 5G-EA4 for ciphering and 128-5G-IA2 for integrity protection, and included an ABBA value of 3200. The Security Mode Command was integrity protected, as indicated by the security header. Upon receiving this, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, the UE is expected to accept the Security Mode Command if the parameters and context are valid and consistent with the security context established during 5G-AKA. A Security Mode Reject is only expected if the UE detects an error, such as an invalid security context, unsupported algorithms, or inconsistencies in the message. Since the Security Mode Command was sent with a valid new security context and standard algorithms, and the rejection reason was unspecified, this behavior is not compliant with the 3GPP standard and could indicate either a misconfiguration or a security weakness in the UE's implementation. Therefore, the action taken by the UE in this scenario is considered insecure as it did not properly proceed with the expected secure communication flow after successful authentication and context establishment. Insecure

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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was integrity protected and used a new security context. The AMF specified the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm, with the ABBA parameter set to 0000. Upon receiving this Security Mode Command, the UE responded with a Security Mode Reject message, indicating "Security mode rejected, unspecified." According to the 3GPP 5G security standards, the use of the null ciphering algorithm (5G-EA0) means that user data would not be encrypted, which is generally only allowed in very specific, controlled scenarios (such as emergency services or when explicitly permitted by policy). In normal operation, the UE is expected to reject security configurations that do not provide adequate confidentiality protection, especially after successful authentication and establishment of a security context. The UE's decision to reject the Security Mode Command that proposed null encryption aligns with the 3GPP security requirements to prevent unencrypted user data transmission, thereby protecting user privacy and network integrity. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a protected service request message to the AMF, indicating that NAS security was established and the messages were encrypted and integrity-protected as required by the 3GPP 5G standard. In response, the AMF sent a protected DownlinkNASTransport message carrying a deregistration accept message, which was also properly secured. Upon receiving this protected deregistration accept, the UE did not respond further, which is consistent with expected behavior: according to the 3GPP TS 24.501 specification, after receiving a deregistration accept message (especially when the deregistration was initiated by the network or the UE), the UE should consider itself deregistered and is not required to send any further NAS messages unless it initiates a new registration procedure. The fact that the UE did not respond to the deregistration accept, and that all messages were protected after the completion of 5G-AKA, indicates that the UE followed the 3GPP security requirements and did not expose itself to any security risks in this interaction. Therefore, the UE's actions were secure and in compliance with the 5G standard. Secure

51	51	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 25.642455101013184 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 25.642899990081787 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Message type: deregistration request, after NAS security is established) 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step to request network services. In response, the AMF sent a deregistration request to the UE, with the message being integrity protected and ciphered, indicating that NAS security had been activated as required by the 3GPP 5G standard (TS 24.501). The UE then responded with a deregistration accept message, also sent over a protected NAS connection. The key point to consider is whether the UE accepted a deregistration request that was properly protected and whether it was in a valid protocol state to process such a request. According to 3GPP standards, after NAS security is established, all subsequent NAS messages, including deregistration requests, must be integrity protected and ciphered, which was the case here. Although the AMF sent a deregistration request immediately after a service request (which may be unusual in normal operation), the UE's action to process and respond to a protected deregistration request is compliant with the security requirements of the standard, as it did not accept or process any unprotected or unexpected messages. Therefore, the UE's actions in this scenario were secure and aligned with 3GPP 5G security procedures. Secure
52	52	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 11.176167011260986 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 11.17656421661377 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command 11.383517980575562 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, indicating that the security context was established and NAS messages should be protected. The AMF responded with a configuration update command, which was sent as a downlink NAS message with both integrity protection and ciphering enabled, as indicated by the security header (2). The UE then responded with a deregistration request (UE originating), which was sent as an uplink NAS message. According to the 3GPP 5G standard, once the security context is established via 5G-AKA, all subsequent NAS messages between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity. The packet capture confirms that the downlink message from the AMF was protected, and there is no indication that the UE sent any unprotected NAS messages after security activation. The UE's action of sending a deregistration request after receiving a protected configuration update command is consistent with secure behavior as per the 3GPP standard, assuming the deregistration request was also protected (which is typical after 5G-AKA). Therefore, based on the information provided and the sequence of events, the UE acted securely in its communication with the AMF. Secure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE initiated a Service Request, which was sent to the AMF. In response, the AMF sent a Deregistration Request (UE terminated) message, which was integrity protected and ciphered, indicating that NAS security had been activated and the message was both encrypted and authenticated as per 3GPP standards. Upon receiving this protected deregistration request, the UE responded with a Deregistration Accept message, also sent via a secured NAS message. According to 3GPP TS 24.501, once NAS security is established (after 5G-AKA), all subsequent NAS messages, especially those involving critical procedures such as deregistration, must be integrity protected and ciphered. The UE's behavior—accepting and responding to a properly protected deregistration request—aligns with the expected security requirements. There is no indication that the UE accepted an unprotected or improperly protected message, nor did it respond to a deregistration request that was not secured. Therefore, based on the observed actions, the UE adhered to the 5G security procedures as outlined by 3GPP, and its actions can be considered secure. Secure
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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step for requesting access to network services. The AMF then responded with a protected (encrypted and integrity-protected) GMM Status message, indicating a "Conditional IE error" with a 5GMM Cause value of 100. According to the 3GPP 5G specifications (TS 24.501), after security activation (i.e., after 5G-AKA), all NAS messages between the UE and AMF must be protected, and the UE should only process protected messages. The GMM Status message from the AMF was indeed protected, as required. However, the UE did not respond to the GMM Status message. Per 3GPP TS 24.501, section 8.2.21, upon receiving a protected GMM Status message, the UE is not required to send any response; the message is informational and is intended to notify the UE of an error in a previous message. The UE's lack of response is therefore compliant with the standard and does not indicate a security flaw. The UE did not process or respond to any unprotected messages after security activation, and all its actions adhered to the expected secure behavior as defined by 3GPP. Based on this analysis, the UE's actions were secure. 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.	In this test scenario, the UE initiated a 5G standalone registration procedure by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security architecture, NAS messages exchanged before the completion of 5G-AKA (i.e., before mutual authentication and key establishment) are not protected by NAS security (encryption and integrity protection). The Authentication Reject message is specifically allowed to be sent in plain text as per 3GPP TS 24.501, and the UE is expected to silently discard such a message if it is received before security activation, as a security measure to prevent downgrade or denial-of-service attacks. In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the 3GPP standard's security recommendations. By not reacting to an unauthenticated and unprotected Authentication Reject, the UE avoids being tricked by a potentially malicious AMF or attacker. Therefore, the UE's behavior in this scenario is considered secure according to the 5G standard. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, before the completion of 5G-AKA, NAS messages are allowed to be sent in plain text, as security context has not yet been established. The UE, upon receiving an Authentication Reject message prior to authentication, is expected to not respond further and should abort the registration procedure, as per the standard (see 3GPP TS 24.501, section 5.4.2.6 and 5.4.2.7). In this test, the UE did not respond to the plain Authentication Reject, which is the correct and secure behavior, since responding further could expose the UE to security risks such as downgrade or replay attacks. Therefore, the UE's action aligns with 3GPP security requirements for this scenario. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an Initial Registration Request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, before mutual authentication and key establishment (i.e., before 5G-AKA is completed), all NAS messages are sent in plain text, and the UE must be able to handle and respond to certain messages, including Authentication Reject, even if they are unprotected. The UE, upon receiving an Authentication Reject before authentication, is expected to silently discard the message and not respond, as per the standard, to prevent unnecessary signaling and potential security risks from unauthenticated sources. In this test, the UE did not respond to the plain Authentication Reject, which aligns with the secure behavior mandated by the 3GPP standard. Therefore, the UE's action was secure. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, prior to the completion of the 5G-AKA authentication procedure. According to the 3GPP 5G security standards, specifically TS 33.501, the UE is required to treat any plain (unencrypted and unauthenticated) NAS messages received before the completion of mutual authentication with suspicion, as these could be sent by a rogue or fake AMF. The standard mandates that the UE should not respond to such messages, particularly to plain Authentication Reject messages received before authentication is completed, to prevent downgrade or denial-of-service attacks. In this test, the UE did not respond to the plain Authentication Reject message, which is the correct and secure behavior as per the 3GPP specification. By refusing to process or acknowledge the unauthenticated message, the UE protected itself from potential security threats such as fake base station attacks. Therefore, the UE's action in this scenario was secure. Secure

59	59	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002620220184326172 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as encryption and integrity protection are only applied after successful authentication and key agreement. Upon receiving the Authentication Reject message, the UE did not respond further, which aligns with the expected behavior as per the standard; the UE should cease further NAS communication upon receiving an Authentication Reject prior to security context establishment. Therefore, the UE's behavior—sending its initial registration request in plain text, accepting a plain Authentication Reject, and not responding further—follows the 3GPP security guidelines and does not expose the UE to additional risk in this context. The UE did not proceed with any insecure actions or violate the expected security procedures. Secure
60	60	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003459453582763672 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an Initial Registration Request to the AMF, which is the expected first step in the NAS procedure. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, before the completion of 5G-AKA, all NAS messages are sent in plain text, and the UE is required to process only legitimate messages from the network. However, the 3GPP standard (TS 24.501) also specifies that upon receiving an Authentication Reject message before security context establishment, the UE should not take further action and should not respond, as this could be an indication of a security attack (such as a fake AMF or a replay attack). In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the security requirements of the 5G standard, as responding could expose the UE to security risks. Therefore, the UE's behavior was secure and compliant with 3GPP specifications. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. At this stage, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that NAS security context had not been established and messages were still being exchanged in plain (unencrypted) form, as per the 3GPP standard. The AMF, under tester control, responded with a Registration Reject message (5GMM Cause 111: Protocol error, unspecified), also sent in plain text. The UE, upon receiving this Registration Reject, did not respond further. According to 3GPP TS 24.501, before the completion of 5G-AKA and the establishment of NAS security, it is expected and compliant for the UE to send and receive initial registration messages in plain text. Furthermore, upon receiving a Registration Reject message before security activation, the UE is not required to respond, as the registration procedure is considered terminated. Therefore, the UE's actions—sending the initial registration request in plain, accepting a plain Registration Reject, and not responding further—are fully in line with the 5G security procedures and do not expose the UE to additional risk in this 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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a Service Request message to the AMF, indicating a desire to resume or establish a connection for mobile-originated data. In response, the AMF sent a Deregistration Accept message, which was protected (i.e., integrity protected and/or ciphered), as is required after security context establishment in 5G standalone networks. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be protected to prevent eavesdropping and tampering. The packet capture confirms that the downlink message from the AMF was indeed protected. The UE, upon receiving the protected Deregistration Accept message, did not respond further, which is consistent with expected behavior if the UE is being deregistered and has no further actions to take. There is no indication that the UE accepted or processed any unprotected NAS messages after security activation, nor did it respond inappropriately to the protected deregistration message. Therefore, based on the observed interaction and adherence to 3GPP security requirements, the UE's actions were secure. 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.	In this 5G standalone security test, the UE and AMF completed the 5G-AKA authentication procedure, after which the UE sent an Authentication Response to the AMF. The AMF then sent a Security Mode Command to the UE, which was integrity protected and indicated the use of new security context, as per the 3GPP standard. The ciphering and integrity algorithms (128-5G-EA1 and 128-5G-IA2) were negotiated, and the Security Mode Command was protected, indicating that the NAS security context was established before further sensitive communication. Following this, the UE sent a Deregistration Request (UE originating), which, according to the 3GPP standard, should only be sent after NAS security is activated to ensure confidentiality and integrity of the message. The packet capture confirms that the Security Mode Command was received and processed before the UE sent the Deregistration Request, meaning the UE waited for security activation before sending sensitive messages. This sequence aligns with 3GPP requirements for secure NAS communication, as the UE did not send any sensitive message before security was established. Therefore, the UE's actions were secure and compliant with the 5G standard. Secure
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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step for requesting access to network services. The AMF responded with a service accept message, which, according to the packet capture, was sent as a protected (i.e., integrity protected and/or ciphered) NAS message. However, the UE did not respond to this protected downlink message. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted to ensure confidentiality and authenticity. The UE is expected to process protected messages from the AMF and respond appropriately, such as by acknowledging or continuing the session. The lack of response from the UE to a properly protected service accept message indicates that the UE either failed to process the message or did not recognize it as valid, which is not compliant with 3GPP security requirements. This behavior could expose the UE to potential security risks, such as denial of service or session hijacking, if it fails to handle protected messages correctly. Therefore, based on the observed actions and the 3GPP standard, the UE's behavior in this scenario is considered insecure. Insecure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. Unexpectedly, the AMF then sent another "security mode command" message, this time protected with the new security context established during the previous exchange. Upon receiving this, the UE responded with a "security mode reject" message, citing an unspecified reason for the rejection. According to the 3GPP 5G standard, the "security mode command" is intended to be sent only once after authentication and before any protected NAS messages are exchanged; sending a second security mode command after security activation is not standard-compliant and could indicate a protocol anomaly or a potential attack (such as a replay or downgrade attempt). The UE's action to reject the second security mode command, especially after security context activation, demonstrates adherence to the standard's security principles by refusing to process unexpected or potentially malicious commands that could compromise the established security context. Therefore, the UE's behavior was secure, as it correctly identified and rejected an abnormal security procedure, thereby protecting itself from possible protocol exploitation or downgrade attacks. Secure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, indicating that it was ready for secure communication. The AMF, under test control, responded with a Security Mode Command message that was properly protected (integrity protected with a new security context) and specified the ciphering and integrity algorithms (128-5G-EA1 and 128-5G-IA2) as well as the ABBA parameter. However, instead of accepting the security mode, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to 3GPP standards, after successful 5G-AKA, the UE is expected to accept a valid and protected Security Mode Command from the AMF unless there is a legitimate reason to reject (such as an unsupported algorithm or a protocol error). Since the Security Mode Command was sent with appropriate protection and valid parameters, the UE's rejection without a specified cause is not compliant with 3GPP security procedures and could indicate a vulnerability or misconfiguration, as it prevents the establishment of a secure context for further communication. Therefore, the UE's action in this scenario is considered insecure, as it does not align with the expected secure behavior defined by the 5G standard. **Insecure**

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 0.8142230510711 67 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.	In this security test, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent a Service Request to the AMF, which is a standard procedure to resume or establish a session. The AMF, under test control, responded with a protected (encrypted and integrity-protected) 5GMM Status message carrying a 5GMM Cause value of 98. According to 3GPP TS 24.501, a 5GMM Status message is not expected in this protocol state, especially as a response to a Service Request. The UE, upon receiving this unexpected and protocol-incompatible message, replied with its own 5GMM Status message indicating "Message type not compatible with the protocol state." This behavior aligns with the 3GPP standard, which specifies that the UE should respond with a status message when it receives an unexpected or invalid message type, thereby maintaining protocol integrity and not processing potentially malicious or malformed messages. The UE's actions demonstrate correct protocol handling and secure behavior, as it did not proceed with any further actions that could compromise its state or security, and it provided appropriate feedback to the network. Therefore, the UE's response was secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a Service Request to the AMF, which is a standard procedure to resume or establish a session. The AMF responded with a Configuration Update Command, which was sent as a protected NAS message with integrity protection enabled, as indicated by the security header. The UE then replied with a Configuration Update Complete message, acknowledging receipt and processing of the configuration update. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected, and, where required, encrypted to ensure confidentiality and authenticity. The packet capture confirms that the Configuration Update Command was integrity protected, and the UE responded appropriately with a Configuration Update Complete message. There is no indication that the UE sent any unprotected or unencrypted NAS messages after the security context was established. Therefore, based on the observed behavior and adherence to 3GPP security procedures, the UE acted securely in this interaction. Secure

69	69	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3100 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11985111236572266 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12013506889343262 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3252840042114258 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was integrity protected and indicated the use of the 5G-EA0 (null) ciphering algorithm and 128-5G-IA2 for integrity protection. The Security Mode Command was sent with a security header indicating that a new security context was being established. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standards, after authentication, the UE and network must agree on security algorithms for both integrity and ciphering. The use of 5G-EA0 (null ciphering) means that user data would not be encrypted, which is generally discouraged except for specific scenarios (such as emergency services or regulatory requirements). A standards-compliant and security-conscious UE should reject a security mode command that attempts to establish a null ciphering algorithm for normal service, as this would expose user data to potential interception. Therefore, the UE's action to reject the Security Mode Command when only null ciphering was proposed aligns with best security practices and the intent of 3GPP standards to protect user confidentiality. The UE did not proceed with insecure parameters and thus acted securely in this context. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security procedures had been completed. Subsequently, the AMF sent a "Security Mode Command" message to the UE, which was integrity protected and ciphered using the new security context established during 5G-AKA. The ciphering algorithm selected was 5G-EA0 (null ciphering), and the integrity algorithm was 128-5G-IA2. According to the 3GPP 5G standard, after the security context is established, the UE is expected to respond to the Security Mode Command with a Security Mode Complete message, confirming that it has activated the indicated security algorithms. However, in this test, the UE did not respond to the Security Mode Command. This lack of response is a secure action, as the use of the null ciphering algorithm (5G-EA0) means that user data would not be encrypted, potentially exposing sensitive information. The 3GPP standard allows the UE to reject or not respond to security procedures if the proposed algorithms do not meet security requirements. Therefore, by not responding, the UE avoided establishing a session with insufficient security, which aligns with secure behavior as per the standard. Secure

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.	In this test scenario, after successfully completing the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, which is expected as part of normal NAS signaling. The AMF, under test control, responded with a Security Mode Command message that was both integrity protected and ciphered, using ciphering algorithm 128-5G-EA3 and integrity algorithm 5G-IA0 (null). According to the 3GPP 5G standard, after 5G-AKA is completed, the Security Mode Command is used to establish NAS security, and the UE is expected to respond with a Security Mode Complete message, confirming acceptance and activation of the negotiated security algorithms. In this test, the UE did not respond at all to the Security Mode Command. This lack of response is significant: the Security Mode Command was protected (ciphered and integrity protected, though with null integrity), and the UE should have been able to process and respond if it supported the selected algorithms and the procedure was correct. The absence of any response from the UE indicates a failure to comply with the 3GPP standard, as the UE is required to acknowledge and activate NAS security or at least reject if it cannot support the configuration. This behavior could expose the UE to potential security risks, such as denial of service or improper session establishment, and does not align with secure protocol operation as defined by 3GPP. Therefore, based on the UE's lack of response to a properly protected Security Mode Command after 5G-AKA, the UE's action in this scenario is considered insecure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, indicating that it was ready for further NAS-level communication. The AMF then sent a Security Mode Command, which was protected and specified the use of ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA2, along with a new security context and ABBA value 3300. The UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept the Security Mode Command if the parameters (algorithms, security context, etc.) are supported and valid. A Security Mode Reject is only expected if the UE detects an unsupported algorithm, an invalid security context, or any other security anomaly (such as a mismatch in negotiated parameters or an integrity failure). Since the Security Mode Command was protected and the UE still rejected it without specifying a concrete cause, this suggests the UE may have detected an inconsistency or potential security risk in the command, or it may not support the proposed algorithms. From a security standpoint, rejecting a Security Mode Command when something is amiss is the correct and secure behavior, as it prevents the establishment of a potentially insecure or unsupported security context. Therefore, based on the information provided and the 3GPP standard, the UE's action was secure. Secure

73	73	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1599750518798828 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602010726928711 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3605461120605469 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating its readiness to establish NAS security. Subsequently, the AMF sent a "security mode command" message back to the UE, which was integrity protected but specified the use of the 5G-EA0 (null) ciphering algorithm and 128-5G-IA2 for integrity protection. The security header indicated that a new security context was being used. Upon receiving this command, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. According to 3GPP standards (TS 33.501 and TS 24.501), after 5G-AKA, the UE is expected to only accept security mode commands that require both integrity and ciphering protection with non-null algorithms, unless local policy or emergency services dictate otherwise. The use of 5G-EA0 (null ciphering) means that the NAS messages would not be encrypted, exposing user data and signaling to potential interception. The UE's decision to reject the security mode command that specified null encryption aligns with 3GPP security requirements, as it prevents the establishment of an insecure NAS security context. Therefore, the UE's action was secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was protected using the newly established security context, specifying ciphering and integrity algorithms (128-5G-EA3 and 128-5G-IA2) and including the ABBA parameter. Upon receiving this command, the UE responded with a Security Mode Reject message, indicating "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard (TS 24.501), a UE is expected to accept the Security Mode Command if it can support the requested algorithms and the security context is valid. However, the standard also allows the UE to reject the command if it detects an issue, such as an unsupported algorithm, an invalid security context, or any integrity/ciphering mismatch. In this case, since the Security Mode Command was sent with the correct security header and algorithms, and the UE still rejected it with an unspecified cause, this behavior could be considered secure from a defensive perspective: the UE did not proceed with potentially insecure or mismatched security parameters, and it did not accept a security context it could not validate. This conservative approach is in line with the 3GPP principle of "fail safe"—if the UE cannot securely establish the context, it should reject rather than proceed insecurely. However, the use of "unspecified" as the rejection cause may limit diagnostic clarity, but it does not inherently indicate insecurity. Therefore, based on the information provided and the 3GPP standard, the UE's action was secure. 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.	In this test scenario, the 5G standalone User Equipment (UE) and the Access and Mobility Management Function (AMF) completed the 5G-AKA authentication procedure, which is a prerequisite for establishing a secure NAS (Non-Access Stratum) communication channel. After authentication, the UE sent an Uplink NAS Transport message to the AMF, and the AMF responded with a Security Mode Command, which was integrity protected and indicated the use of new security context, ciphering algorithm 5G-EA5, and integrity algorithm 128-5G-IA1, as per 3GPP standards. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G security specifications, upon receiving a Security Mode Command that is properly protected and after successful 5G-AKA, the UE is expected to process the command, activate the indicated security algorithms, and respond with a Security Mode Complete message. The absence of any response from the UE means it did not acknowledge or activate the negotiated security context, which is a deviation from the standard and could leave the communication channel unprotected or in an undefined state. This lack of response is considered insecure behavior, as the UE failed to complete the security procedure required to ensure confidentiality and integrity of subsequent NAS messages. 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.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, but the 5G-AKA authentication process was not yet completed. Subsequently, the AMF sent an identity request for the SUCI (Subscription Concealed Identifier) to the UE, and this request was sent in plain (unencrypted) form, as encryption cannot be established until 5G-AKA is complete. The UE did not respond to this identity request. According to the 3GPP 5G security standards, the SUCI is a privacy-protected identifier and is specifically designed to be sent even over unprotected NAS messages before authentication and key agreement are completed. However, the UE is expected to respond to a plain identity request for SUCI prior to the completion of 5G-AKA, as this is necessary for the network to proceed with authentication. By not responding to the identity request, the UE is being overly cautious, but this is not in line with the 3GPP standard, which allows and expects the SUCI to be sent in plain text at this stage. Therefore, while the UE's action does not expose sensitive information, it is not compliant with the standard procedure and could cause interoperability issues. Based on the 3GPP standard, the UE's behavior is secure from a privacy perspective but is not standard-compliant. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. In response, the AMF sent an Identity Request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE then replied with an Identity Response, providing the requested SUCI. Importantly, this exchange occurred before the completion of the 5G-AKA authentication procedure, meaning that NAS security (encryption and integrity protection) had not yet been established, and the messages were sent in plain (unencrypted) form. According to the 3GPP 5G standards, it is expected and required that the UE provides the SUCI (not the cleartext SUPI) in response to an identity request before security activation. The SUCI is a privacy-preserving, encrypted version of the SUPI, designed specifically to protect the subscriber's permanent identity even when sent over an unprotected channel. Therefore, the UE's action—responding with the SUCI in the clear prior to 5G-AKA completion—aligns with the 3GPP security requirements and does not expose sensitive information. The UE did not send the SUPI or any other sensitive identifier in the clear, and thus its behavior was secure according to the standard. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Security Mode Complete message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. However, the AMF then sent another Security Mode Command to the UE, this time with the ciphering algorithm set to 5G-EA0 (null ciphering, meaning no encryption) and integrity protection set to 128-5G-IA2, with the security header indicating "integrity protected with new security context." Upon receiving this, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to 3GPP 5G security standards (TS 33.501 and TS 24.501), after 5G-AKA, the UE is expected to accept only those security mode commands that provide both integrity and confidentiality protection, unless there are exceptional circumstances (such as emergency services). The use of 5G-EA0 (null ciphering) is generally not permitted for normal NAS signaling after authentication, as it would leave messages unencrypted and vulnerable to interception. By rejecting the security mode command that attempted to downgrade ciphering to null, the UE correctly enforced the 5G security policy and protected the confidentiality of its communication. Therefore, the UE's action was secure and in compliance with 3GPP standards. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was integrity protected using the 128-5G-IA2 algorithm but specified the use of the 5G-EA0 (null) ciphering algorithm, meaning that no encryption would be applied to subsequent NAS messages. The UE responded by rejecting the Security Mode Command with a "Security mode rejected, unspecified" message. According to the 3GPP 5G standards, after authentication, the UE and network must negotiate security algorithms for both integrity and ciphering to protect NAS signaling. The use of 5G-EA0 (null ciphering) is only permitted in specific, controlled scenarios (such as emergency calls or when ciphering is not possible), and it is generally considered insecure for normal operation because it leaves NAS messages unencrypted and vulnerable to interception. The UE's rejection of the Security Mode Command when only null ciphering was offered demonstrates correct and secure behavior, as it refused to operate without proper encryption, thereby upholding the security requirements of the 5G standard and protecting user data and signaling from potential eavesdropping or tampering. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF, which is a standard procedure for establishing or resuming a connection. The AMF, under test control, responded with a Configuration Update Command message that was integrity protected and used a new security context, as indicated by the security header. Upon receiving this message, the UE replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS protocol specifications, the UE is required to check the validity and compatibility of received messages with its current protocol state. If the UE receives a message that is not allowed in its current state, it should respond with a 5GMM Status message, as observed in this test. This behavior is a security feature designed to prevent the UE from processing unexpected or potentially malicious messages, thereby maintaining protocol integrity and preventing state confusion attacks. The UE's response demonstrates adherence to the 3GPP standard by not accepting or acting on an out-of-sequence or invalid message, and instead, it securely notifies the network of the protocol violation. Therefore, the UE's actions in this scenario were secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF, which then replied with a Security Mode Command. The Security Mode Command was sent with the security header set to "integrity protected," but both the ciphering and integrity algorithms were set to null (5G-EA0 and 5G-IA0), meaning that neither encryption nor integrity protection was actually applied to the NAS messages. The UE, upon receiving this Security Mode Command, did not respond. According to the 3GPP 5G standard, after authentication, the AMF must select appropriate ciphering and integrity algorithms to protect subsequent NAS messages. The use of null algorithms (EA0/IA0) is only permitted in very limited circumstances, such as for emergency services or when explicitly allowed by the UE's security capabilities. In normal operation, the UE is expected to reject a Security Mode Command that requests null algorithms for both ciphering and integrity, as this would leave the communication unprotected and vulnerable to interception or tampering. The UE's lack of response in this situation aligns with the security requirements of the 3GPP standard, as it avoids establishing an insecure connection. Therefore, the UE's action in this test was secure. Secure

82	82	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0363 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1200721263885498 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12030816078186035 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3220691680908203 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was protected and specified the use of ciphering algorithm 128-5G-EA3 and integrity algorithm 5G-IA0 (null). The security header indicated that the message was integrity protected with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard (TS 33.501), it is mandatory for the UE to support both ciphering and integrity protection; using a null integrity algorithm (5G-IA0) is generally not permitted for user plane or NAS signaling messages except in very limited and controlled scenarios (e.g., emergency services or specific test cases). The UE's refusal to accept a security context that does not provide integrity protection is a secure and standards-compliant behavior, as accepting such a context would expose the UE to potential security risks, such as message tampering or replay attacks. Therefore, the UE's action to reject the Security Mode Command when only a null integrity algorithm was proposed demonstrates adherence to security best practices and the 3GPP standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement, the UE initiated a service request to the AMF, which is the expected behavior for establishing a secure NAS session. The AMF then responded with a service accept message, which, according to the packet capture, was sent as a protected (i.e., integrity protected and/or ciphered) NAS message, as required by the 3GPP 5G security specifications after authentication. However, the UE did not provide any response to this protected downlink message from the AMF. According to 3GPP standards (TS 33.501 and TS 24.501), after the security context is established via 5G-AKA, the UE must only accept and process NAS messages that are integrity protected (and, where required, ciphered). If the UE receives a protected message and does not respond, it could indicate that the UE is either unable to process the protected message correctly or is failing to follow the protocol, which could be due to a security implementation issue or a protocol handling error. Since the UE did not respond to a properly protected message after authentication, this behavior is not compliant with the 3GPP security requirements, as the UE should have processed and acknowledged the protected service accept message. Therefore, the action taken by the UE in this scenario is considered insecure according to the 5G standard. Insecure

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.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then issued a Security Mode Command message. This command was integrity protected and indicated the use of the 128-5G-EA2 cipher and 128-5G-IA2 integrity algorithms, with a security header showing that a new security context was being established. Upon receiving this command, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to 3GPP standards, after successful authentication, the UE is expected to accept the Security Mode Command unless there is a valid reason (such as unsupported algorithms or mismatched parameters). The "unspecified" cause in the reject message suggests the UE did not provide a clear, standards-based reason for rejection, which is not typical behavior for a compliant and secure UE. This could indicate a potential issue in the UE's security handling, as it should only reject the command for specific, justified reasons and not with an unspecified cause, especially after a successful 5G-AKA. Therefore, based on the 3GPP standard, the action taken by the UE appears to be insecure, as it does not align with expected secure behavior following successful authentication and valid security mode command parameters. Insecure

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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security parameters. However, the AMF then sent a subsequent "security mode command" message, protected with integrity, specifying null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, which effectively means no encryption or integrity protection would be applied to subsequent NAS messages. Upon receiving this, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. According to the 3GPP 5G security standards (TS 33.501), the use of null algorithms is only permitted under specific, controlled circumstances (such as emergency services or when explicitly allowed by the UE's security policy). In normal operation, the UE is expected to reject any attempt to establish a security context with null algorithms, as this would leave NAS signaling unprotected and vulnerable to interception or tampering. The UE's action to reject the security mode command in this context demonstrates adherence to the 5G security requirements and protects the integrity and confidentiality of its communication. Therefore, the UE's behavior in this scenario is secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection) and was ready to secure subsequent NAS messages. However, the AMF, under tester control, responded with another "security mode command" message—this is an unexpected behavior, as per 3GPP standards, the "security mode command" should only be sent once after authentication, and the UE should not receive another such command after it has already completed the security mode procedure. Despite this, the UE responded again with a "security mode complete" message. According to 3GPP TS 24.501, Section 8.2.20, the UE should ignore any subsequent "security mode command" messages received after the security context is already established, to prevent replay or downgrade attacks. By responding to a second "security mode command," the UE potentially exposes itself to security vulnerabilities, such as replay or manipulation of security parameters, which could be exploited by an attacker with control of the AMF. Therefore, the UE's action of accepting and responding to a second "security mode command" after security context establishment is not compliant with the 3GPP standard and is considered insecure. 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) (UnitData) 0.9976592063903809 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information), InitialUEMessage, 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.	In this test scenario, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent a Service Request to the AMF, which is a normal procedure for initiating services. The AMF, under test control, responded with a Deregistration Request message that was integrity protected and ciphered, indicating that NAS security was active as per 3GPP requirements. Upon receiving this protected deregistration message, the UE replied with a 5GMM Status message indicating "Invalid mandatory information," suggesting that the UE detected an issue with the content or format of the deregistration request. This is a standard and secure behavior according to 3GPP TS 24.501, where the UE is expected to respond with a status message if it receives a NAS message with invalid or missing mandatory information. The Service request (RRCEstablishmentCause=mo-Data) protected. The subsequent messages show the UE attempting to re-initiate service, but the AMF rejects it due to an inability to derive the UE's identity, which is outside the UE's control. The UE's actions—responding to a protected but malformed message with a status indication and not accepting the deregistration blindly—demonstrate adherence to the security procedures defined by 3GPP, ensuring that it does not process potentially malicious or malformed messages even when they are integrity protected and ciphered. Therefore, the UE's behavior in this scenario is secure according to the 5G standard. 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.	In this test scenario, after the initial NAS steps, the UE sent an authentication response to the AMF. However, before the 5G-AKA authentication procedure was completed, the AMF sent an Identity Request message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE responded with an Identity Response containing the requested SUCI. According to the 3GPP 5G security standards, the SUCI is specifically designed to protect the subscriber's permanent identifier (SUPI) by encrypting it with the home network's public key, allowing it to be safely transmitted even before the establishment of a secure NAS signaling connection (i.e., before 5G-AKA is completed). Therefore, the UE's action of sending the SUCI in response to a plain Identity Request is compliant with the 5G security architecture, as the SUCI itself does not reveal the SUPI and is intended for exactly this use case. The UE did not expose any sensitive information in cleartext and followed the expected security procedures as outlined by 3GPP. Thus, the UE's behavior in this interaction was secure. 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.	In this test scenario, the 5G standalone User Equipment (UE) completed the initial NAS steps and sent an authentication response to the Access and Mobility Management Function (AMF). At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that NAS security (encryption and integrity protection of NAS messages) was not yet activated. The AMF then sent an identity request to the UE, specifically requesting the Subscription Concealed Identifier (SUCI), and this message was sent in plain (unencrypted) form. The UE responded with an identity response, also in plain text, as observed in the packet capture. According to the 3GPP 5G standard, before the completion of 5G-AKA, all NAS messages are exchanged in plain text because the security context has not yet been established. The SUCI is designed to protect the subscriber's permanent identifier (SUPI) by encrypting it with the home network's public key, so even when sent in plain text, it does not expose sensitive information. Therefore, the UE's action of responding with the SUCI in plain text before the completion of 5G-AKA is compliant with the 3GPP standard and does not compromise security, as the SUCI itself is a privacy-preserving identifier. Based on this analysis, the UE's behavior in this scenario is secure. 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.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, but before the 5G-AKA procedure was completed, the AMF sent an identity request for the SUCI (Subscription Concealed Identifier). The UE responded with an identity response containing the requested SUCI. According to the 3GPP 5G standard, NAS messages are only protected (i.e., encrypted and integrity protected) after the successful completion of the 5G-AKA authentication procedure. Prior to this, messages are sent in plain text. The SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) by encrypting it, allowing it to be safely transmitted even before NAS security is activated. Therefore, the UE's action of sending the SUCI in response to a plain identity request before completing 5G-AKA is compliant with the 3GPP standard and does not expose sensitive information. The UE did not send the SUPI or any unprotected permanent identifier, but rather the SUCI, which is meant for this exact use case. Thus, the UE's behavior in this scenario is secure according to the 5G standard. 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.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes security keys for integrity and ciphering), the UE initiated a Service Request to the AMF. In response, the AMF sent a Deregistration Request (UE terminated) message, which was integrity protected and ciphered, indicating that NAS security was active. Upon receiving this protected deregistration request, the UE responded with a 5GMM Status message indicating "Invalid mandatory information." According to the 3GPP 5G NAS protocol (TS 24.501), when the UE receives a NAS message with invalid or missing mandatory information, it is expected to respond with a 5GMM Status message, as the UE did here. The fact that the UE only responded with a status message and did not process or act upon the invalid deregistration request demonstrates that it correctly identified the protocol anomaly and did not proceed with potentially insecure or unintended actions. This behavior aligns with the 3GPP standard, which mandates that the UE should not process messages with invalid mandatory information and should instead report the error. Therefore, the UE's actions in this scenario were secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a Service Request to the AMF, indicating that NAS security had been established and further messages would be protected. In response, the AMF sent a Deregistration Request (UE terminated), which was integrity protected and ciphered, as indicated by the security header (2), confirming that the message was both encrypted and authenticated. Upon receiving this protected deregistration request, the UE responded appropriately with a Deregistration Accept message, also sent under NAS security. According to the 3GPP 5G standards, after 5G-AKA, all subsequent NAS messages must be integrity protected and, where required, ciphered. The UE's actions—sending a service request after authentication, accepting a protected deregistration request, and replying with a deregistration accept—are fully compliant with the expected secure behavior as outlined in the standard. The UE did not process or respond to any unprotected or unexpected messages, and all its communications were within the secure context established by 5G-AKA. Therefore, the UE's actions in this scenario were secure and in line with 3GPP requirements. Secure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters previously negotiated. However, the AMF then sent a new "security mode command" message, protected with the newly established security context, specifying the use of ciphering algorithm 5G-EA4 and integrity algorithm 5G-IA0 (null integrity). Upon receiving this, the UE responded with a "security mode reject" message, citing a "UE security capabilities mismatch." According to the 3GPP 5G standard, the UE is required to verify that the security algorithms proposed by the network are supported and acceptable. If the network requests a configuration that the UE does not support or that violates security requirements (such as using null integrity protection), the UE must reject the security mode command to prevent insecure operation. The UE's action to reject the security mode command due to a security capabilities mismatch aligns with the 3GPP standard and demonstrates proper security behavior, as it prevents the establishment of a potentially insecure connection. Therefore, the UE's response in this scenario was secure. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. In response, the AMF issued an identity request, specifically asking for the SUCI (Subscription Concealed Identifier), and this message was sent in plain (unencrypted) form. The UE then responded with an identity response, providing the requested SUCI. According to the 3GPP 5G security standards, before the 5G-AKA (Authentication and Key Agreement) procedure is completed, NAS messages between the UE and the AMF are not yet encrypted, and identity requests and responses—especially those involving the SUCI—are expected to be sent in plain text. The SUCI is specifically designed to protect the subscriber's permanent identifier (SUPI) by concealing it using public key cryptography, allowing it to be safely transmitted even before a secure channel is established. Therefore, the UE's action of sending the SUCI in response to a plain identity request before 5G-AKA completion is compliant with the 3GPP standard and does not expose sensitive information. Based on this analysis, the UE's behavior in this interaction is considered secure. 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 mismatch with NAS message protection) 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.	In this test scenario, after the successful completion of 5G-AKA authentication and security setup, the UE initiated a Service Request to the AMF, which was sent as an encrypted and integrity-protected NAS message, as expected. In response, the AMF sent a Deregistration Request (UE terminated), also protected with integrity and ciphering, even though this message type was not compatible with the current protocol state (since the UE had just requested service). Despite this protocol irregularity, the UE responded with a Deregistration Accept (UE terminated), also protected, thereby complying with the security requirements for NAS message protection post-authentication. From a security perspective, the UE's actions were in line with 3GPP 5G standards: it only accepted and responded to protected messages after security context establishment, and it did not process or respond to any unprotected or suspicious messages. The test did not reveal any security bypass or improper handling of NAS message protection by the UE, even when faced with an unexpected deregistration request. Therefore, the UE's behavior was secure according to the 5G standard. Secure
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.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the AMF, where the 5G-AKA authentication procedure had not yet been completed. The UE first sent an identity response, after which the AMF issued another identity request, specifically requesting the SUCI (Subscription Concealed Identifier). The UE responded with another identity response message. All of these messages, including the identity response containing the SUCI, were transmitted in plain (unencrypted) form, as indicated by the packet capture and the fact that 5G-AKA had not yet been completed. According to the 3GPP 5G standard, the initial identity exchange (including SUCI) is permitted to occur in plain text before security context establishment, as the SUCI is a privacy-preserving, concealed version of the subscriber's identity (SUPI). The SUCI is specifically designed to be sent over unprotected channels without exposing the subscriber's permanent identity. Therefore, the UE's action of sending the SUCI in response to the AMF's identity request, even in plain text prior to 5G-AKA completion, is compliant with the 3GPP standard and does not constitute a security vulnerability. The UE did not expose the SUPI or any sensitive information in cleartext, and its behavior aligns with the expected security procedures for initial NAS communication in 5G. 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.	In the described test scenario, the UE and AMF are engaged in NAS communication prior to the completion of the 5G-AKA authentication procedure. The UE first sends an identity response, after which the AMF issues another identity request for the SUCI (Subscription Concealed Identifier), and the UE responds accordingly. All these exchanges occur before the establishment of NAS security, meaning the messages are transmitted in plain (unencrypted) form. According to the 3GPP 5G standard, specifically TS 24.501, identity requests and responses prior to the completion of 5G-AKA are allowed to be sent in the clear, as security context and ciphering have not yet been established. The SUCI itself is designed to protect the subscriber's permanent identity (SUPI) by encrypting it, so even when sent in plain NAS, it does not expose sensitive information. Therefore, the UE's action of responding to the identity request with a SUCI in plain NAS before 5G-AKA completion is compliant with the 3GPP standard and does not constitute a security vulnerability. The UE did not send any sensitive information (such as the SUPI) unprotected, and the use of SUCI is specifically intended for this pre-authentication phase. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Service Request to the AMF, which is the expected behavior to initiate a session or resume communication. The AMF, under test control, then sent a Configuration Update Command to the UE, which was integrity protected and used a new security context, indicating that NAS security procedures were correctly established. Upon receiving this message, the UE responded with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS protocol (TS 24.501), the UE is required to check the validity and compatibility of received messages based on its current protocol state. If it receives a message that is not compatible with its state, the correct and secure behavior is to respond with a Status message indicating the incompatibility, rather than processing or accepting the message. This prevents the UE from acting on potentially malicious or out-of-sequence messages, thus maintaining protocol integrity and security. The UE's action demonstrates adherence to the 3GPP standard and proper handling of protocol errors, ensuring that it does not process unexpected or potentially harmful messages. Therefore, the UE's response in this scenario was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (PDU session establishment request) to the AMF. The AMF then responded with a Downlink NAS Transport message containing a Service Accept, which was marked as "Protected," indicating that it was integrity protected and/or encrypted as per 3GPP security requirements. However, the UE did not respond to this protected Service Accept message from the AMF. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted to ensure confidentiality and authenticity. The UE's action of not responding to a properly protected downlink message is not a violation of the security standard; rather, it may indicate that the UE either did not recognize the message, considered it invalid, or was unable to process it for some other reason. Importantly, the UE did not send any unprotected or insecure messages after the security context was established, nor did it accept or act on an unprotected message. Therefore, based on the information provided and the 3GPP standard, the UE's behavior in this interaction can be considered secure. Secure
100	100	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 92 UE provided: No response The packet capture during the test using wireshark is: 0.4685640335083008 UE to AMF UplinkNASTransport, Registration complete 0.4687800407409668 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Insufficient user-plane resources for the PDU session) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). The AMF then sent a downlink NAS message—a GMM Status message with 5GMM Cause 92 ("Insufficient user-plane resources for the PDU session")—which was correctly protected according to the packet capture. Upon receiving this protected status message, the UE did not respond. According to 3GPP standards (TS 24.501), the GMM Status message is used to inform the UE of error conditions, and the UE is not required to respond to a status message, especially if it does not have any corrective action to take or if the message is not relevant to its current state. Furthermore, since all NAS messages after 5G-AKA were protected, the UE's actions adhered to the security requirements of the 5G standard. The UE did not send any unprotected messages, nor did it respond inappropriately to the status message. Therefore, the UE's behavior in this scenario was secure and compliant with 3GPP specifications. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is a typical step in establishing a PDU session. The AMF then responded with a Security Mode Command message, which was sent as a protected (integrity-protected and ciphered) message using the negotiated security algorithms (128-5G-EA3 for ciphering and 128-5G-IA2 for integrity protection), and with the security header indicating a new security context. According to the 3GPP 5G standard, upon receiving a Security Mode Command, the UE is expected to process the message, apply the new security context, and respond with a Security Mode Complete message to confirm the activation of the negotiated security algorithms. However, in this test, the UE did not respond to the Security Mode Command. This lack of response is not compliant with the 3GPP standard, as it leaves the security procedure incomplete and could indicate that the UE failed to process or accept the new security context, potentially exposing the session to security risks or denial of service. Therefore, based on the standard, the UE's action in this scenario is considered insecure. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Service Request to the AMF, which then responded with a Security Mode Command. Notably, the Security Mode Command was sent with both ciphering and integrity protection algorithms set to null (5G-EA0 and 5G-IA0), meaning no encryption or integrity protection was applied, although the security header indicated "Integrity protected with new security context." Upon receiving this, the UE responded with a 5GMM Status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, after 5G-AKA, the UE and network must negotiate and use non-null security algorithms for both ciphering and integrity protection to ensure confidentiality and integrity of NAS messages. The use of null algorithms (EA0/IA0) after authentication is explicitly prohibited except in very limited cases (e.g., emergency services or specific fallback scenarios), and the UE is expected to reject or flag such insecure configurations. By sending a 5GMM Status message indicating "Invalid mandatory information" in response to a Security Mode Command with null algorithms, the UE correctly identified and rejected the insecure security configuration, as required by the standard. This action demonstrates that the UE adhered to 3GPP security requirements and did not proceed with insecure communication. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which was likely a PDU session establishment request. The AMF, under test control, responded with a Deregistration Request message that was integrity protected and ciphered, as indicated by the security header (2). According to the 3GPP 5G standard, after security context establishment (i.e., after 5G-AKA), the UE is required to process only those NAS messages that are both integrity protected and ciphered, discarding or ignoring any that are not properly protected. In this case, the UE did not respond to the protected Deregistration Request from the AMF. This behavior could be interpreted in two ways: either the UE failed to process a valid, protected message (which would be non-compliant and insecure), or the UE correctly ignored the deregistration request because it was unexpected or did not match its current state (which would be compliant and secure). However, since the deregistration request was properly protected and the UE simply did not respond, this suggests a potential issue in the UE's handling of valid, protected NAS messages. According to 3GPP standards, the UE should at least acknowledge or process valid, protected NAS messages unless there is a specific reason (such as an invalid context or unexpected message type) to discard them. Without further context on the UE's internal state, the lack of response to a valid, protected deregistration request points to a deviation from expected secure behavior as per 3GPP standards. Therefore, based on the observed behavior and the 3GPP requirements, the UE's action in this scenario appears to be insecure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as it initiates further NAS procedures (in this case, a PDU session establishment request). Subsequently, the AMF responded with a Deregistration Request message, which was integrity protected and ciphered, indicating that NAS security was active and the message was protected according to 3GPP standards. The UE, however, did not respond to this protected Deregistration Request. According to 3GPP TS 24.501, upon receiving a protected Deregistration Request from the AMF, the UE is required to process and respond appropriately (typically with a Deregistration Accept message). The lack of response from the UE to a properly protected and standard-compliant deregistration request indicates a deviation from expected secure behavior, as it could leave the UE in an undefined or insecure state regarding its registration status. This could potentially expose the UE to security risks or network inconsistencies. Therefore, based on the 3GPP standard and the observed behavior, the UE's action in this scenario was insecure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE initiated an Uplink NAS Transport message, which is a standard step in establishing a PDU session. The AMF then sent a Configuration Update Command to the UE. According to the packet capture, this downlink message was sent with a security header indicating that it was both integrity protected and ciphered, meaning it was encrypted and authenticated as per 3GPP security requirements. The UE responded with a Configuration Update Complete message, indicating it accepted and processed the command. Since the 5G-AKA procedure was completed before these NAS messages were exchanged, the security context was established, and all subsequent NAS messages (including the Configuration Update Command and the UE's response) were protected as required by the 3GPP 5G security standards (TS 33.501). The UE's actions—accepting and responding to a protected configuration update command only after a secure context was established—demonstrate adherence to the standard security procedures. Therefore, based on the sequence of events and the security protections in place, the UE's actions were secure and compliant with 3GPP requirements. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the negotiated cipher (5G-EA4) and integrity (128-5G-IA3) algorithms, and indicated a new security context in the security header. Upon receiving this command, the UE replied with a Security Mode Reject message, citing a mismatch in UE security capabilities. According to the 3GPP 5G standard (TS 24.501), the UE is required to verify that the security algorithms proposed by the network in the Security Mode Command are supported by its own capabilities, which were previously reported to the network. If there is a mismatch—meaning the network requests algorithms that the UE does not support—the UE must reject the command by sending a Security Mode Reject message with the appropriate cause value. This behavior prevents the UE from accepting unsupported or potentially insecure security configurations, thereby protecting the integrity and confidentiality of its communications. Based on this, the UE's action aligns with the 3GPP standard and demonstrates secure behavior by refusing to proceed with an unsupported security context. 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.	In this test scenario, after completing the 5G-AKA authentication and security procedures, the UE sent a "registration complete" message to the AMF, indicating the successful completion of the registration process. Subsequently, the AMF sent a "deregistration request" to the UE, which was integrity protected and ciphered, as indicated by the security header (2), ensuring confidentiality and integrity of the NAS message. The UE responded with a "deregistration accept" message, completing the deregistration process. According to the 3GPP 5G standards, after the establishment of NAS security (post-5G-AKA), all subsequent NAS messages, including deregistration procedures, must be protected by integrity and ciphering. The UE correctly accepted and responded to a protected deregistration request, as per the protocol, and did not process any unprotected or suspicious messages. This indicates that the UE adhered to the security requirements of the 5G standard, only responding to properly protected messages after security activation. Therefore, the UE's actions in this scenario were secure and compliant with the 3GPP specifications. 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.	In this test scenario, after successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message, which was followed by the AMF sending a Configuration Update Command. The AMF's downlink message was integrity protected and used a new security context, indicating that NAS security procedures were in place and the message was protected as per 3GPP standards. Upon receiving this message, the UE responded with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to 3GPP TS 24.501, the UE is required to check the validity of received NAS messages relative to its current protocol state and, if a message is not compatible, it should respond with a 5GMM Status message indicating the incompatibility. This behavior is a security feature designed to prevent the UE from acting on unexpected or potentially malicious messages, ensuring protocol robustness and preventing state confusion attacks. Therefore, the UE's action—rejecting the incompatible message and informing the AMF via a status message—demonstrates adherence to the 5G security standard and proper protocol handling. Secure
109	109	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5209951400756836 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215010643005371 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 0.7227599620819092 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (which establishes security context and enables NAS message protection), the UE sent an Uplink NAS Transport message to the AMF, which is a normal procedure. The AMF, under tester control, responded with a protected GMM Status message containing a 5GMM Cause value of 98. According to 3GPP TS 24.501, the GMM Status message is used to indicate protocol errors or abnormal conditions, and the cause value 98 corresponds to "Message type not compatible with the protocol state." Upon receiving this, the UE responded with a 5GMM Status message of its own, echoing the same cause value. This behavior aligns with the 3GPP standard, which specifies that the UE should respond with a GMM Status message if it receives a message type that is not compatible with its current protocol state, especially when the message is protected and the security context is active. The UE did not process the invalid message further and instead reported the protocol error as required, thereby maintaining protocol integrity and not exposing itself to potential attacks or state confusion. Therefore, the UE's action was in accordance with the 5G security requirements and protocol specifications, demonstrating secure behavior in this context. Secure

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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the NAS security context was established and subsequent NAS messages should be protected (i.e., integrity protected and ciphered). The AMF then sent a "5GMM Status" message with cause 101 ("Message not compatible with the protocol state") as a protected downlink NAS message. According to the 3GPP 5G standard (TS 24.501), when a UE receives a protected "5GMM Status" message with cause 101, it is not required to respond, especially if the message state is incompatible with its current protocol state. The UE's lack of response in this situation is compliant with the standard, as responding to an unexpected or invalid status message could potentially expose the UE to security risks, such as replay or reflection attacks. Therefore, the UE's action—choosing not to respond to this protected status message—demonstrates adherence to the 5G security requirements and proper protocol behavior. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was integrity protected and indicated the use of ciphering algorithm 5G-EA5 and a null integrity algorithm (5G-IA0). Upon receiving this, the UE rejected the security mode command, citing a "UE security capabilities mismatch." According to 3GPP standards, the UE is required to verify that the security algorithms proposed by the network are supported and acceptable. If there is a mismatch—such as the network proposing an integrity algorithm that the UE does not support or that does not meet security requirements—the UE must reject the security mode command to prevent insecure communication. In this case, the AMF proposed a null integrity algorithm (5G-IA0), which provides no integrity protection, while the ciphering algorithm was non-null. The UE correctly identified this as a security risk and responded by rejecting the command, thereby preventing the establishment of a potentially insecure security context. This action aligns with 3GPP security requirements and demonstrates that the UE is enforcing proper security checks to protect itself and the network. Therefore, the UE's action was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the negotiated cipher (5G-EA5) and integrity (128-5G-IA2) algorithms, and marked with a security header indicating the use of a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing a "UE security capabilities mismatch." According to the 3GPP 5G standards, if the UE detects that the security algorithms proposed by the network do not match its own capabilities (as indicated during earlier capability exchange), it is required to reject the security mode command to prevent the establishment of an insecure or unsupported security context. This behavior is a critical security measure to ensure that the UE does not accept security parameters it cannot support, which could otherwise expose it to potential vulnerabilities. Therefore, the UE's action to reject the security mode command upon detecting a mismatch is in strict compliance with the 3GPP standard and demonstrates secure behavior in the context of 5G security procedures. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the negotiated cipher (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and included a security header indicating integrity protection with a new security context. Upon receiving this protected Security Mode Command, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standards, after 5G-AKA, the Security Mode Command is used to activate NAS security, and the UE is expected to accept it unless there is a valid reason (such as an unsupported algorithm or an error in the security context). The unspecified rejection reason from the UE, especially after a correctly protected command, suggests either a malfunction or a deliberate refusal without a standards-based justification. This behavior is not aligned with 3GPP expectations, as it could disrupt secure communication establishment and may indicate a vulnerability or non-compliance in the UE's security handling. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. Insecure
114	114	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5208940505981445 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215411186218262 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7234148979187012 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated an Uplink NAS Transport message to the AMF, which is a standard step in establishing a secure NAS session. The AMF then sent a Configuration Update Command to the UE, and this message was protected with both integrity protection and ciphering, as indicated by the security header (2), meaning the message was both encrypted and authenticated. The UE responded with a Configuration Update Complete message, which is the expected behavior according to the 3GPP 5G NAS protocol. Since the 5G-AKA procedure was completed prior to these exchanges, the security context was established, ensuring that all subsequent NAS messages (including the Configuration Update Command and the UE's response) were protected as required by the standard. The packet capture also confirms that the messages were exchanged in the correct order and with the appropriate security protections in place. Based on this, the UE's actions were in full compliance with the 3GPP 5G security standards, as it only sent and accepted protected NAS messages after the security context was established, and responded appropriately to the AMF's commands. Secure

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.	In this test scenario, the 5G standalone User Equipment (UE) first completed the 5G-AKA authentication procedure, establishing the necessary security context for protected communication. The UE then sent a Service Request to the Access and Mobility Management Function (AMF), which responded with a Security Mode Command message. This Security Mode Command was sent as a protected message, using the agreed ciphering (5G-EA4) and integrity (128-5G-IA3) algorithms, and indicated a new security context with integrity protection. Upon receiving this, the UE responded with a 5GMM Status message indicating "Invalid mandatory information." According to the 3GPP 5G standards, after successful authentication and establishment of security context, all subsequent NAS messages must be integrity protected and, where required, ciphered. The Security Mode Command from the AMF was correctly protected, and the UE's response was a status message, which is permitted by the standard if the UE detects an error in the received message (such as missing or invalid mandatory information elements). The UE did not proceed with unprotected communication or accept an insecure context; instead, it reported the protocol error as specified by the standard. Therefore, the UE's action aligns with the expected secure behavior as outlined by 3GPP, as it maintained security and protocol integrity by not accepting or acting on a potentially malformed or non-compliant message. Secure

116	116	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00d2 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.480457067489624 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48129701614379883 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.6844742298126221 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, indicating that a secure context had been established and further NAS messages should be protected. The AMF then responded with a Security Mode Command, which was correctly sent as a protected message using the negotiated ciphering (128-5G-EA2) and integrity (128-5G-IA2) algorithms, and with the security header indicating "integrity protected with new security context." Upon receiving this, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to 3GPP standards, the UE is expected to accept the Security Mode Command if it is valid and properly protected, unless there is a specific reason (e.g., unsupported algorithms, invalid parameters, or internal errors) to reject it. Since the Security Mode Command was sent after 5G-AKA completion, was integrity protected, and used standard algorithms, the UE's rejection without specifying a concrete cause appears to be non-compliant with the standard. This behavior could expose the network to denial-of-service scenarios or indicate a failure in the UE's security handling. Therefore, the UE's action in this interaction is considered insecure according to the 3GPP 5G security standards. Insecure

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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent a Security Mode Command message, which was correctly protected using the negotiated ciphering (5G-EA5) and integrity (128-5G-IA1) algorithms, and marked as "Integrity protected and ciphered with new security context (4)," as per 3GPP standards. However, the UE did not respond to the Security Mode Command. According to 3GPP TS 24.501, after receiving a Security Mode Command that is properly protected and uses the correct security context, the UE is required to verify the integrity and decrypt the message, and then respond with a Security Mode Complete message if the command is valid. The absence of any response from the UE indicates that it did not follow the expected protocol behavior. This lack of response could be interpreted as a failure to establish a secure NAS security context, which is a critical step before any further NAS communication can securely proceed. Therefore, while the AMF behaved according to the standard, the UE's lack of response is not compliant with 3GPP security procedures and could be considered insecure, as it leaves the NAS security context incomplete and the session in an undefined or vulnerable state. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a NAS communication by sending an Uplink NAS Transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a Configuration Update Command to the UE. Importantly, this downlink message from the AMF was protected with both integrity protection and ciphering, as indicated by the security header (2), which is required by the 3GPP 5G standard for NAS messages after security context establishment. The UE then responded with a Configuration Update Complete message, indicating it properly processed and acknowledged the protected command. According to 3GPP TS 24.501, after 5G-AKA is completed and NAS security is activated, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, ciphered. The packet capture confirms that the UE only sent and responded to protected messages after security activation, and did not transmit any sensitive information in the clear. Therefore, the UE's actions adhered to the security requirements of the 5G standard, ensuring confidentiality and integrity of the NAS signaling. Secure

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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Security Mode Command. The Security Mode Command from the AMF specified the use of the null ciphering algorithm (5G-EA0) and an integrity protection algorithm (128-5G-IA1), and the message was sent as "protected" with a new security context. Upon receiving this, the UE responded with a Security Mode Reject message, indicating "Security mode rejected, unspecified." According to the 3GPP 5G standard, after authentication, the AMF should negotiate security algorithms with the UE, and the use of the null ciphering algorithm (5G-EA0) is only permitted under specific, limited circumstances (e.g., for emergency services or when explicitly allowed by policy). In normal operation, the UE is expected to reject the use of 5G-EA0 if it does not meet these criteria, as using no encryption would expose user data to potential interception. The UE's rejection of the Security Mode Command, which attempted to establish a security context with no encryption, aligns with the security principles of the 5G standard, as it prevents the establishment of an insecure communication channel. Therefore, the UE's action was secure and in compliance with 3GPP requirements. 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.	In this security test, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established and subsequent NAS messages should be protected (integrity protected and, if required, encrypted) as per 3GPP standards. The AMF then sent a "Deregistration Accept" message to the UE, which was marked as protected, meaning it was sent with the appropriate NAS security applied. Notably, after receiving this protected deregistration message, the UE did not respond further. According to the 3GPP 5G specifications (TS 24.501), after the UE receives a "Deregistration Accept" message, no further NAS response is required from the UE, and the UE should proceed to locally deactivate its 5G context and release resources. The fact that the UE did not respond to the protected deregistration message aligns with the expected behavior defined by the standard, and the use of NAS security after 5G-AKA ensures the confidentiality and integrity of the messages. Therefore, the actions taken by the UE in this scenario were secure and compliant with the 5G standard. 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.	In this test scenario, after the initial NAS procedures, the UE sent an Authentication Response message to the AMF before the 5G-AKA (Authentication and Key Agreement) procedure was completed. The AMF, under tester control, then sent a Service Reject message with 5GMM Cause 111 ("Protocol error, unspecified") in plain (unencrypted) form. According to the 3GPP 5G standards, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are transmitted in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. The UE, upon receiving the Service Reject message, did not respond further, which is compliant with expected behavior since a Service Reject is a terminal message and the UE should not proceed with further NAS signaling. The UE did not attempt to process or respond to a plain Service Reject message received before security activation, nor did it expose any sensitive information or continue communication in an insecure state. Therefore, based on the 3GPP standard and the described interaction, the UE's actions were secure and in line with expected protocol behavior. 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.	In this security test, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. The AMF, under test control, responded with a service reject message, specifically indicating "UE identity cannot be derived by the network" (5GMM Cause 9), and this message was sent in plain (unencrypted) form. The UE, upon receiving this service reject, did not respond further. According to 3GPP 5G standards, before 5G-AKA is completed, it is expected and required that NAS messages be sent in plain text, as security context has not yet been established. Furthermore, the UE is expected to accept and process plain service reject messages at this stage, and it is not required to respond to a service reject. Therefore, the UE's behavior—sending an initial registration request in plain, receiving a plain service reject, and not responding further—is fully compliant with the 5G standard and does not expose any security weakness in the UE's actions during this exchange. 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.	In this test scenario, after the UE sent an identity response to the AMF, the AMF responded with a Security Mode Command message that was "protected" (i.e., integrity protected with a new security context) and specified ciphering and integrity algorithms, but the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security architecture, the Security Mode Command should only be sent after successful completion of the 5G-AKA authentication and key agreement procedure, which establishes the necessary security context and keys for protecting NAS signaling. Since the 5G-AKA was not completed, the UE had not yet derived the required keys (KAMF, etc.) to securely process protected NAS messages. Upon receiving a protected Security Mode Command without an established security context, the UE correctly rejected the command with a Security Mode Reject message, as it could not verify the integrity or decrypt the message securely. This behavior aligns with 3GPP security requirements, which mandate that the UE must not accept security-protected NAS messages before the authentication and key agreement are completed. Therefore, the UE's action was secure and compliant with the 5G standard, as it prevented a potential security vulnerability where protected messages could be accepted without proper key 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.	In this test scenario, the UE and AMF were engaged in NAS communication prior to the completion of the 5G-AKA authentication procedure, which is necessary to establish security contexts for encryption and integrity protection of NAS messages. The UE first sent an identity response, after which the AMF issued another identity request for the SUCI (Subscription Concealed Identifier), and the UE responded accordingly. Notably, the AMF sent the identity request as a plain (unencrypted) message, and the UE responded in kind, also in plain text, since the 5G-AKA procedure had not yet been completed to enable secure message exchange. According to the 3GPP 5G standard, specifically TS 24.501, identity requests and responses that occur before the completion of authentication (i.e., before security contexts are established) are permitted to be sent in plain text, as there is not yet a shared key to enable encryption. The use of the SUCI, which is a privacy-preserving identifier, further protects the subscriber's permanent identity (SUPI) even when sent in the clear. Therefore, the actions taken by the UE—responding to identity requests with a SUCI in plain text before security activation—are compliant with the 3GPP standard and do not constitute a security breach. The UE's behavior is thus considered secure within the context of the standard and the test setup. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an Initial Registration Request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are allowed to be sent in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. The UE, upon receiving an Authentication Reject message in plain text prior to security context establishment, is expected to not respond further and to abort the registration procedure, as a security measure against potential attacks (such as false base stations or replay attacks). In this test, the UE did not respond to the plain-text Authentication Reject, which aligns with the expected secure behavior as per 3GPP standards. The UE's action prevents further exposure of information and mitigates the risk of unauthorized network access or information leakage. Therefore, the UE's behavior in this scenario was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating the end of the registration process. Following this, the AMF (under tester control) sent a "Deregistration Request (UE terminated)" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2), meaning that both confidentiality and integrity protection were applied according to 3GPP standards. The UE then responded with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to 3GPP TS 24.501 and TS 33.501, after 5G-AKA is completed, all subsequent NAS messages, including deregistration, must be integrity protected and ciphered to ensure secure communication. The UE correctly processed the protected deregistration request and responded appropriately, indicating compliance with the 5G security requirements. There is no evidence of the UE accepting unprotected messages or failing to apply security, and all actions taken by the UE align with the expected secure behavior as per 3GPP standards. Secure

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.	In this test scenario, the UE completed the initial NAS procedures and sent an Identity Response message to the AMF, which was still in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. The AMF, under test control, then sent a Deregistration Accept message (also in plain text) to the UE, after which the UE did not respond further. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as security protections (encryption and integrity) are only applied after successful authentication and key agreement. The UE's behavior—sending an unencrypted Identity Response prior to 5G-AKA and not responding to the plain Deregistration Accept—aligns with the standard's requirements, as it did not attempt to establish security before the necessary procedures were completed. Therefore, the UE's actions in this scenario were in accordance with the 3GPP 5G security specifications and did not introduce any security vulnerability in this context. Secure
128	128	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 00000000000000000000000000000000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Mapped security context ngKSI_KSI: 1 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.03987288475036621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04013490676879883 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24352788925170898 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response, the AMF replied with an authentication request message that was sent in plain (unencrypted) form, with both the RAND and AUTN fields set to all zeros—values that are not valid for a legitimate authentication challenge. The UE, upon receiving this malformed authentication request, did not proceed with the authentication procedure but instead responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G security standards, the authentication request message must contain valid, non-zero RAND and AUTN values, and the UE is expected to check the integrity and validity of these fields before proceeding. If the message is malformed or contains invalid mandatory information, the UE should reject it and not proceed with authentication or key establishment. By responding with a status message indicating the error, rather than attempting to process the invalid authentication request, the UE demonstrated correct and secure behavior as per 3GPP requirements, ensuring that it does not establish a security context based on invalid or potentially malicious input. Secure

129	129	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3100 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11980295181274414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12005805969238281 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.321152925491333 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then responded with a Security Mode Command. The Security Mode Command from the AMF specified the use of the 5G-EA0 (null) ciphering algorithm (meaning no encryption) and the 128-5G-IA2 integrity algorithm, and was sent with a security header indicating "integrity protected with new security context." Upon receiving this command, the UE rejected it, sending a Security Mode Reject message with the cause "Security mode rejected, unspecified." According to the 3GPP 5G security standards (TS 33.501), the use of the 5G-EA0 (null) ciphering algorithm is only permitted under specific, limited circumstances (such as emergency services or when ciphering is not required by the network policy). In normal operation, the UE is expected to reject a Security Mode Command that attempts to establish a security context with no encryption (i.e., 5G-EA0) unless those special conditions apply. The UE's rejection of the Security Mode Command in this case demonstrates that it is enforcing the security requirements outlined by the standard, refusing to operate without proper encryption after authentication. Therefore, the UE's actions were in line with the 3GPP security specifications and protected the confidentiality of its communications. 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.	In this test scenario, after the UE sent an identity response to the AMF, the AMF replied with an authentication request message that was sent in plain (unencrypted) form, as indicated by the packet capture and the test summary. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI, but crucially, the 5G-AKA authentication procedure had not yet been completed, meaning that a security context had not been established and messages were still unprotected. Upon receiving the plain (unencrypted) authentication request, the UE responded with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it rejected the authentication attempt because it did not conform to 5G security requirements. According to the 3GPP 5G standard, the UE should not accept authentication procedures that do not follow the expected 5G-AKA process or that are not properly protected, as this could expose the UE to security risks such as replay or man-in-the-middle attacks. By refusing to proceed with authentication in the absence of a secure context and when the authentication request was sent in plain text, the UE demonstrated compliance with 5G security requirements and protected itself from potential vulnerabilities. Therefore, the action taken by the UE was secure and in line with the 3GPP 5G standard. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a registration reject message using 5GMM cause 26 ("Non-5G authentication unacceptable") before the 5G-AKA authentication procedure was completed. The registration reject message was sent in plain (unencrypted) form, which is expected behavior according to the 3GPP 5G security architecture, as NAS message protection (encryption and integrity) is only activated after successful completion of the 5G-AKA authentication and key agreement. The UE, upon receiving the registration reject, did not respond further, which is also compliant with the standard, as the UE should not proceed with registration or attempt to establish a secure connection when authentication has not been completed and registration has been explicitly rejected. Therefore, the UE's actions—sending the initial request, receiving an unprotected reject message, and ceasing further communication—align with 3GPP security requirements and do not expose the UE to additional risk in this context. 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.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After completing the initial NAS steps, the UE sent an Identity Response message to the AMF, which was transmitted in plain (unencrypted) text because the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The AMF then responded with a Service Reject message, also sent in plain text, citing 5GMM Cause 99 ("Information element non-existent or not implemented"). Following this, the UE did not respond further. According to the 3GPP 5G standard, messages exchanged before the completion of 5G-AKA (such as identity requests and responses) are allowed to be sent in plain text, as encryption and integrity protection are only established after successful authentication and key agreement. The UE's behavior—sending the Identity Response in plain text before security activation and ceasing communication after receiving a Service Reject—aligns with the expected security procedures outlined by 3GPP. The UE did not proceed with any further actions that could compromise security, nor did it transmit sensitive information after the Service Reject. Therefore, based on the 3GPP standard and the observed behavior, the UE's actions in this scenario were secure. 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.	In this test scenario, after completing the initial NAS procedures, the UE responded to an identity request with an identity response, as expected. The AMF then sent an authentication request to the UE, but crucially, this message was sent in plain (unencrypted) text before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, sensitive messages such as authentication requests should only be accepted by the UE if they are protected by integrity and confidentiality, which is only possible after successful completion of the 5G-AKA procedure and establishment of a security context. The UE, upon receiving an unprotected authentication request, correctly identified this as a violation of the expected security procedures and responded with an "Authentication failure (Non-5G authentication unacceptable)" message. This behavior aligns with 3GPP security requirements, as it prevents potential security risks such as replay or man-in-the-middle attacks that could arise from processing authentication requests sent in plain text. Therefore, the UE's action demonstrates adherence to the 5G security standards and is considered secure. 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.	In this test scenario, the UE and AMF engaged in a NAS communication sequence where, after the initial NAS steps, the UE sent an Identity Response message to the AMF. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) had not been established, and messages were exchanged in plain (unencrypted) form as per 3GPP standards. Following the Identity Response, the AMF sent a Service Reject message with 5GMM Cause 3 ("Illegal UE") in plain text, which is also permitted by the standard prior to security activation. The UE, upon receiving this Service Reject message, did not respond further, which aligns with expected behavior since a Service Reject is a terminal message indicating that the UE is not allowed to proceed. According to 3GPP TS 24.501, it is acceptable for the UE to send and receive certain NAS messages in plain text before security is activated, and it is also correct for the UE to cease communication after a Service Reject. Therefore, the actions taken by the UE were in line with the 5G security requirements and did not expose the UE to additional risk in this context. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF responded with a Security Mode Command, which was sent as a protected message but specified the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, and indicated "integrity protected with new security context" in the security header. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that a valid security context was not yet established between the UE and the network. Upon receiving the Security Mode Command with null algorithms and an invalid security context, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G security standards, the UE must not accept a security mode command that attempts to establish a security context with null algorithms or before the completion of 5G-AKA, as this would leave the communication unprotected and vulnerable to attacks. The UE's action to reject the security mode command under these circumstances demonstrates adherence to the 5G security requirements and prevents the establishment of an insecure connection. Therefore, the UE's behavior in this scenario was secure. 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.	In this test scenario, after the UE sent an identity response to the AMF, the AMF responded with a Security Mode Command that was integrity protected with a new security context, specifying the use of the null cipher algorithm (5G-EA0) and the 128-5G-IA3 integrity algorithm. However, the 5G-AKA authentication procedure had not yet been completed, which means that the necessary security keys for establishing a secure NAS security context had not been derived. According to 3GPP standards (TS 33.501 and TS 24.501), the Security Mode Command should only be accepted by the UE after successful completion of authentication (5G-AKA), as only then are the required keys available for proper encryption and integrity protection. The use of the null cipher algorithm (EA0) is permitted, but only under specific conditions and with explicit agreement, and never before authentication is complete. The UE, upon receiving a Security Mode Command before authentication was finished, correctly rejected the command with an unspecified reason, as it could not securely establish a NAS security context without the necessary keys. This behavior aligns with the security requirements of the 5G standard, as accepting the command would have exposed the UE to potential security risks such as replay or man-in-the-middle attacks. Therefore, the UE's action to reject the Security Mode Command before authentication was completed was secure and compliant with 3GPP specifications. 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.	In this test scenario, the UE and AMF are engaged in the NAS authentication procedure as part of the 5G-AKA process. The UE initially sends an authentication response to the AMF, after which the AMF, under test control, sends another authentication request back to the UE. Notably, this subsequent authentication request from the AMF is sent in plain (unencrypted) form, and the 5G-AKA procedure has not yet been completed, meaning that a secure NAS security context has not been established. According to the 3GPP 5G standard, the UE should only respond to authentication requests in plain NAS messages prior to the completion of 5G-AKA, as encryption and integrity protection are only activated after successful authentication and key agreement. However, the unusual aspect in this scenario is that the AMF sends a second authentication request after already receiving an authentication response, which is not standard behavior and could indicate a replay or out-of-sequence attack. The UE, upon receiving this second authentication request, responds again with an authentication response, still in plain text, as the security context is not yet established. While the UE's actions are technically compliant with the 3GPP standard—since it is allowed to respond in plain text before 5G-AKA completion—the fact that it responds to a repeated or unexpected authentication request could be a security concern, as robust UEs are expected to detect and reject replayed or out-of-sequence authentication requests to prevent certain attacks. Therefore, while the UE's behavior is not strictly a protocol violation, it does not demonstrate strong security robustness against abnormal AMF behavior. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the registration process. Immediately following this, the AMF (under tester control) sent a "Deregistration Request (UE terminated)" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2). The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, also sent under the established security context. According to the 3GPP 5G standards, after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF must be integrity protected and, where required, ciphered to ensure confidentiality and authenticity. The UE's actions—accepting a properly protected deregistration request and responding with a deregistration accept—align with the expected behavior outlined in the standards. There is no indication that the UE accepted an unprotected or improperly protected message, nor did it respond inappropriately to the deregistration request. Therefore, based on the observed behavior and adherence to the security requirements post-authentication, the UE's actions were secure and compliant with 3GPP specifications. Secure

139	139	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 31303030000000007894d5bcdd550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00084686279296875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2040548324584961 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an authentication request message that was deliberately sent in plain (unencrypted) form, with suspicious or invalid authentication parameters (notably, AUTN was all zeros and RAND appeared non-random). According to the 3GPP 5G security standards, the UE must verify the integrity and validity of the authentication request before proceeding with the authentication and key agreement (5G-AKA) procedure. If the authentication request is malformed, invalid, or fails integrity checks, the UE is expected to reject it and notify the network of the failure, rather than proceeding with authentication or accepting the message. In this test, the UE responded with a 5GMM status message indicating "Invalid mandatory information," which means it detected the authentication request as invalid and did not proceed further with the authentication process. This behavior aligns with 3GPP security requirements, as it prevents the UE from accepting potentially malicious or tampered authentication requests and ensures that no sensitive information or cryptographic material is exposed before a secure context is established. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Request message that was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. Instead of responding to the authentication challenge, the UE immediately sent a Deregistration Request (UE originating) message back to the AMF. According to the 3GPP 5G security architecture, NAS messages exchanged before the successful completion of 5G-AKA (i.e., before mutual authentication and key establishment) are allowed to be sent in plain text, as security contexts are not yet established. However, the expected behavior for a compliant UE is to process the authentication request, attempt to authenticate, and only deregister if authentication fails or if the UE chooses to abort the procedure for a valid reason (such as detecting an invalid AUTN or other security anomaly). In this test, the UE did not attempt authentication but instead deregistered immediately after receiving the plain authentication request. This could be interpreted as a security-conscious action if the UE detected an anomaly (such as a suspicious or malformed authentication request, or a policy to avoid responding to unauthenticated plain messages), thereby preventing exposure of sensitive information. However, if the UE simply refused to proceed with authentication without valid cause, it may indicate non-compliance with the standard, as the 3GPP expects the UE to respond to authentication requests unless a security threat is detected. Since the test does not indicate any anomaly in the authentication request, the UE's immediate deregistration without attempting authentication suggests a deviation from the standard procedure, which could be considered insecure as it may prevent proper mutual authentication and secure context establishment. 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.	In this test scenario, the UE completed the initial NAS procedures and sent an Authentication Response to the AMF as part of the 5G-AKA authentication process. However, before the 5G-AKA procedure could be completed (and thus before NAS security could be activated), the AMF sent an Authentication Reject message to the UE in plain (unencrypted) form. According to the 3GPP 5G standard, Authentication Reject is one of the few NAS messages that can be sent in plain text prior to the establishment of NAS security, since the authentication process has not yet succeeded and security contexts are not yet available. The UE, upon receiving this plain Authentication Reject, did not respond further, which is the expected and secure behavior as per the standard; the UE should not proceed with further NAS signaling or attempt to establish a secure context after receiving an Authentication Reject. Therefore, the UE's action—sending the Authentication Response in plain text before security activation and then ceasing communication after receiving a plain Authentication Reject—aligns with 3GPP security requirements and does not expose the UE to additional risk in this context. 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.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF, under test control, sent another authentication request back to the UE. Notably, this subsequent authentication request was sent in plain (unencrypted) form, even though the 5G-AKA procedure had not yet been completed and a secure context had not been established. Upon receiving this plain authentication request, the UE responded with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it rejected the request because it did not conform to the expected 5G authentication procedures. According to the 3GPP 5G security standards, the UE must not accept authentication requests that do not follow the proper 5G-AKA sequence or are sent in an insecure manner, especially after an authentication response has already been provided. The UE's refusal to process a non-standard, plain authentication request demonstrates adherence to the 5G security requirements, as it prevents potential downgrade or replay attacks that could compromise the security context. Therefore, the UE's action was secure and aligned with 3GPP specifications. Secure
143	143	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5046439170837402 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 0.5048840045928955 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the registration process. Immediately following this, the AMF sent a "Deregistration Request" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2). According to the packet capture, the UE did not respond to this deregistration request. In the context of the 3GPP 5G standard, after the security context is established via 5G-AKA, all subsequent NAS messages, especially those related to mobility management such as deregistration, must be protected to ensure confidentiality and integrity. The AMF's deregistration request was indeed protected, fulfilling this requirement. However, the UE's lack of response to a valid, protected deregistration request is not compliant with the expected behavior outlined in the standard, which requires the UE to acknowledge or process such requests appropriately. The absence of a response could indicate a security flaw or a failure to handle the deregistration procedure as specified by 3GPP, potentially leaving the UE in an inconsistent state or vulnerable to certain attacks. Therefore, based on the observed behavior and the requirements of the 5G standard, the UE's action in this scenario is considered insecure. 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.	In this security test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the registration process. Following this, the AMF sent a "Configuration Update Command" to the UE, which was observed in the packet capture as being integrity protected and ciphered, as indicated by the security header (value 2). This means the message was both encrypted and protected for integrity, in line with 3GPP 5G security requirements, which mandate that sensitive NAS messages be sent only after security context establishment (i.e., after 5G-AKA). The UE then responded with a "Configuration Update Complete" message, also over the protected NAS signaling. The sequence of actions taken by the UE—waiting for 5G-AKA completion before exchanging protected NAS messages and responding appropriately to the AMF's command—demonstrates adherence to the 3GPP 5G security standards. The use of integrity protection and ciphering ensures confidentiality and authenticity of the communication, preventing eavesdropping or tampering. Therefore, the UE's actions in this interaction were secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms (ciphering: 5G-EA0, integrity: 128-5G-IA2) and the new security context. However, the AMF then sent another "security mode command" message, which is unusual since this command is typically sent only once after authentication, and the UE should not expect to receive it again after having already completed the security mode procedure. Despite this, the UE responded by sending another "security mode complete" message. According to 3GPP standards (TS 24.501), the UE should ignore any subsequent "security mode command" messages received after the security context has been established and should not respond to them, as this could indicate a replay or protocol anomaly. By responding to a second "security mode command" after already completing the security mode procedure, the UE deviated from the expected secure behavior, potentially exposing itself to replay or downgrade attacks. Therefore, the UE's action in this scenario was not secure according to the 3GPP 5G standard. 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.	In this test scenario, the 5G-AKA authentication procedure was completed, establishing the necessary security context for subsequent NAS message protection. The UE then sent a "security mode complete" message, indicating that it had accepted and activated the negotiated NAS security algorithms. After this, the AMF sent a "deregistration accept" message, which was protected (i.e., integrity protected and/or ciphered) as per the 3GPP 5G security requirements. The UE, upon receiving this protected deregistration accept message, did not respond further. According to the 3GPP 5G standard, after the security mode is completed, all subsequent NAS messages must be protected, and the UE should only accept protected messages from the AMF. The UE's lack of response to the protected deregistration accept message is compliant with the standard, as the deregistration accept is a terminal message that does not require an acknowledgment from the UE. The UE did not accept or process any unprotected messages after security was established, nor did it respond inappropriately to the protected message. Therefore, the UE's actions were secure and in line with the 3GPP 5G security requirements. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to communicate securely. The AMF then sent a "configuration update command" as a downlink NAS message, which was protected with integrity and ciphering using the new security context, as indicated by the security header. Upon receiving this message, the UE responded with a "5GMM status" message, specifically stating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS protocol (TS 24.501), after the security mode is complete and the security context is active, all subsequent NAS messages—including configuration update commands—must be integrity protected and, if required, ciphered. The UE is also expected to check the validity of received messages in its current protocol state and respond appropriately if an unexpected or invalid message is received. In this case, the UE correctly identified that the configuration update command was not compatible with its current protocol state and responded with a protected status message, as per the standard. This behavior demonstrates that the UE adhered to the security requirements and protocol state machine as defined by 3GPP, ensuring that no unprotected or out-of-sequence messages were accepted or processed insecurely. Therefore, the UE's actions were secure and compliant with the 5G standard. 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) (Consensus) 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had activated the negotiated NAS security context for integrity protection and ciphering. Subsequently, the AMF sent a "deregistration request" message to the UE, which was protected with both integrity and ciphering as indicated by the security header (type 2). The UE then responded with a "deregistration accept" message, completing the deregistration process. According to the 3GPP 5G standards, specifically TS 24.501, once the NAS security context is established (after 5G-AKA and Security Mode Command/Complete), all subsequent NAS messages, including deregistration procedures, must be integrity protected and ciphered. The packet capture confirms that the UE only sent its "deregistration accept" after receiving a properly protected "deregistration request," and there is no indication of the UE sending unprotected NAS messages after security activation. Therefore, the UE's actions were in line with the 5G security requirements, ensuring that sensitive signaling was always protected after security context establishment. Based on this analysis, the UE's behavior was secure according to the 3GPP 5G standard. Secure
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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the negotiated security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity protection) and was ready to operate in a secure mode. However, the AMF then sent another "security mode command" message, which is unusual because, according to the 3GPP 5G standard, the security mode command should only be sent once after authentication, and the UE should respond with a single "security mode complete." The packet capture shows that after the initial "security mode complete" from the UE, it again sent another "security mode complete" in response to the subsequent security mode command from the AMF. This behavior is not compliant with the standard, as the UE should not accept or process a second security mode command after security context has already been established and acknowledged. By responding to a repeated security mode command, the UE exposes itself to potential security downgrade or replay attacks, as a rogue AMF could exploit this behavior to renegotiate weaker security parameters or disrupt the established security context. Therefore, the UE's action of accepting and responding to a second security mode command after already completing the security procedure is not secure according to 3GPP specifications. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (integrity protection and ciphering) was established. Subsequently, the AMF sent a deregistration request to the UE, which was protected with both integrity and ciphering, as indicated by the security header (value 2). The UE then responded with a deregistration accept message, completing the deregistration process. According to the 3GPP 5G standard, after the 5G-AKA and security mode procedures are completed, all subsequent NAS messages must be protected using the agreed security context. The UE correctly followed this by sending and receiving protected messages only after security establishment. There is no indication that the UE accepted or processed any unprotected or suspicious messages, nor did it respond in an insecure manner. The UE's actions align with the expected secure behavior as per 3GPP specifications, ensuring that sensitive procedures like deregistration are only performed over protected channels. Therefore, the UE's communication in this scenario was secure. Secure
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.	In this test scenario, the UE initiated a 5G standalone registration by sending an Initial Registration Request to the AMF. In response, the AMF sent an Identity Request message, specifically requesting the UE's GUTI (Globally Unique Temporary Identifier), and this message was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. According to 3GPP 5G security standards (TS 33.501), before authentication and security context establishment, certain NAS messages, including identity requests, are allowed to be sent in plain text. However, the UE should only respond with its GUTI (or other permanent identifiers like SUPI) if the request is legitimate and not in a situation where it could be exposed to interception or replay attacks. In this case, the UE did not respond to the plain Identity Request for GUTI before security was established. This behavior aligns with best security practices, as it avoids exposing potentially sensitive identifiers over an unprotected channel, which could be exploited by an attacker (e.g., via an IMSI catcher or rogue AMF). Therefore, the UE's refusal to respond before 5G-AKA completion demonstrates a secure and standards-compliant approach to protecting its identity information in the absence of an established security context. 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.	In this test scenario, the UE initiated the registration process by sending an initial registration request to the AMF, which is a standard first step in establishing a 5G connection. The AMF, under test control, responded with a configuration update command sent as a protected downlink NAS message, even though the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed. According to the 3GPP 5G standard, the UE and the network must complete the 5G-AKA procedure before exchanging any NAS messages that require integrity protection or encryption, as this procedure establishes the necessary security context and keys. Since the 5G-AKA was not completed, the UE did not yet have the security context required to process protected NAS messages. The UE's action—providing no response to the protected configuration update command—demonstrates correct and secure behavior, as it did not attempt to process or respond to a message that should only be handled after security activation. This aligns with 3GPP security requirements, which state that the UE must ignore or reject protected NAS messages received before security is established. Therefore, the UE's actions in this scenario were secure. 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.	In this test scenario, the UE initiated a registration procedure by sending an Initial Registration Request to the AMF. The AMF responded with a Security Mode Command, which was sent as a protected message, specifying ciphering with 128-5G-EA3 and integrity protection with 5G-IA0 (null integrity). Notably, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary keys for secure NAS encryption and integrity protection were not yet established. According to 3GPP 5G security standards, the UE should not accept security mode commands that attempt to establish NAS security before successful completion of 5G-AKA, as this could expose the UE to security risks (e.g., replay or man-in-the-middle attacks). The UE responded with a 5GMM status message indicating "Invalid mandatory information," which is an appropriate response, as it refused to proceed with the security context establishment in the absence of a completed authentication procedure. This behavior aligns with the 3GPP standard, which requires the UE to reject or not process security mode commands that are not properly sequenced with authentication. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, before completing the 5G-AKA authentication and key agreement procedure, responded with a Configuration Update Command that was integrity protected and ciphered (security header type 2). According to the 3GPP 5G security architecture, NAS message protection (integrity and ciphering) should only be applied after successful completion of the 5G-AKA, when both the UE and the AMF have established shared security keys. Since the 5G-AKA was not completed yet, the UE did not have the necessary NAS security context to decrypt or verify the protected message. The UE, therefore, did not respond to the AMF's protected Configuration Update Command. This behavior aligns with the 3GPP standard, which specifies that the UE must ignore NAS messages that are protected before security context establishment, as processing such messages would be insecure and could expose the UE to security risks such as replay or spoofing attacks. Thus, the UE's action of not responding to a prematurely protected NAS message was correct and secure according to the standard. 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.	In this test scenario, the UE initiated NAS communication by sending an initial registration request to the AMF, which is the expected first step in establishing a 5G connection. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is necessary to establish mutual authentication and derive security keys for NAS message protection—the AMF responded with a deregistration accept message, marked as "protected." According to the 3GPP 5G standard, NAS message protection (integrity and encryption) should only be applied after successful completion of the 5G-AKA, as this is when the necessary security context is established. Since the UE had not yet completed 5G-AKA, it would not have the keys required to verify or decrypt protected NAS messages. The UE, in this case, did not respond to the protected deregistration accept message, which is the correct and secure behavior per the standard, as it should ignore protected messages until a security context is established. This prevents potential security vulnerabilities such as accepting spoofed or malformed protected messages before authentication. Therefore, the UE's action—providing no response—was secure and compliant 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.	In this test scenario, after the UE initiated the registration process with an InitialUEMessage, the AMF responded with a Security Mode Command message that was marked as "protected" but specified the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, and the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards, the Security Mode Command should only be accepted by the UE if it is received after successful completion of the authentication procedure (5G-AKA), and it should not accept null algorithms unless explicitly allowed by policy or for emergency services. The UE, upon receiving a Security Mode Command with null algorithms and without a completed authentication, responded with a Security Mode Reject, indicating it did not accept the proposed security context. This behavior aligns with 3GPP security requirements, as accepting a security context with no encryption or integrity protection before authentication would expose the UE to significant security risks, such as man-in-the-middle attacks. Therefore, the UE's action to reject the security mode command under these conditions demonstrates adherence to proper security protocols as outlined by the standard. 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) (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.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, instead of proceeding with the expected authentication and security procedures (notably, the 5G-AKA authentication and key agreement), responded with a Deregistration Request message that was integrity protected and ciphered, as indicated by the security header (2). However, since the 5G-AKA procedure had not yet been completed, no security context (keys for encryption and integrity protection) would have been established between the UE and the AMF. According to the 3GPP 5G standard, the UE should only accept and process NAS messages that are protected (integrity protected and/or ciphered) after a security context has been established through successful completion of the authentication procedure. Since the UE did not respond to the protected Deregistration Request sent before security context establishment, it correctly rejected the message as per the standard, thereby preventing potential security vulnerabilities such as replay or spoofing attacks. This behavior demonstrates that the UE adhered to the 3GPP security requirements by not accepting protected messages before authentication and key agreement. 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.	In this test scenario, the UE and AMF engaged in NAS communication prior to the completion of the 5G-AKA authentication procedure, which is necessary to establish a secure channel for message encryption. After the UE sent an identity response, the AMF issued another identity request, specifically asking for the IMEISV, and sent this request in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G security standards, sensitive information such as the IMEISV should not be transmitted over an unprotected NAS connection; instead, it should only be sent after security has been activated via 5G-AKA. The UE's refusal to respond to an unprotected IMEISV request aligns with these security requirements, as providing such information in plain text would expose the UE to privacy and security risks. Therefore, the UE's action demonstrates compliance with the 3GPP standard and shows that it is operating securely by withholding sensitive information until a secure channel is established. 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.	In this security test, after completing the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected to be in plain (unencrypted) form since the 5G-AKA authentication and key agreement procedure had not yet been completed. The AMF then responded with a GMM Status message, also in plain text, indicating a 5GMM cause of 13 ("Roaming not allowed in this tracking area"). The UE did not respond further to this message. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA are permitted to be sent in plain text, as encryption and integrity protection are only established after successful authentication and key agreement. The UE's behavior—sending the Identity Response in plain text and not responding to the GMM Status message—aligns with the standard, as it did not process or act upon a status message that could have been sent by an unauthenticated or malicious AMF. This cautious approach prevents the UE from taking potentially unsafe actions based on unauthenticated messages. Therefore, the UE's actions in this scenario were secure and compliant with the 3GPP 5G standard. Secure

160	160	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.038893938064575195 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039427995681762695 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF were engaged in NAS communication as part of the 5G registration procedure. After the UE sent an Identity Response message (which is expected to be sent in plain text before authentication), the AMF responded with a Configuration Update Command, also sent as a plain (unencrypted) NAS message. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that security context establishment (encryption and integrity protection of NAS messages) had not yet occurred. According to the 3GPP 5G standard, the UE should only accept certain types of plain NAS messages before security activation—specifically, messages related to authentication and security mode control. Configuration Update Command is not one of the permitted messages to be accepted in plain text before security is activated. The UE, in this case, did not respond to the plain Configuration Update Command, which aligns with the 3GPP security requirements and prevents potential security risks such as configuration manipulation before authentication. Therefore, the UE's action of not responding to the plain Configuration Update Command was secure and compliant with the 3GPP standard. Secure
161	161	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0400080680847168 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04023408889770508 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is a standard step in the authentication and security setup process. However, before the 5G-AKA authentication and key agreement procedure was completed—which is required to establish NAS security and encryption—the AMF sent a Deregistration Accept message to the UE. Notably, this downlink message from the AMF was sent as "Protected," implying it was integrity protected or encrypted, even though the security context (from 5G-AKA) had not yet been established. The UE, upon receiving this message, did not respond. According to the 3GPP 5G standard, the UE should not accept or process protected NAS messages before the security context is established via 5G-AKA, as it cannot verify their integrity or decrypt them. The UE's lack of response indicates that it correctly ignored the protected Deregistration Accept message, adhering to the standard and preventing potential security vulnerabilities, such as accepting spoofed or manipulated messages before security is in place. Therefore, the UE's behavior in this scenario was secure and compliant with 3GPP requirements. Secure

162	162	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.03969311714172363 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003500938415527 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the UE sent an Identity Response message to the AMF after completing the preceding NAS steps, but before the 5G-AKA authentication and key agreement procedure was completed. Subsequently, the AMF sent a Service Accept message to the UE, and this message was marked as "Protected" (i.e., encrypted or integrity protected). However, since the 5G-AKA procedure had not yet been completed, the necessary security context (NAS keys) for protecting NAS messages had not been established. According to the 3GPP 5G standard, NAS message protection (encryption and integrity) must only be applied after successful completion of 5G-AKA, which establishes the required security context. The UE, upon receiving a protected NAS message (Service Accept) before security activation, did not respond. This behavior aligns with the 3GPP standard, as the UE should ignore or reject protected NAS messages if security has not yet been activated. Therefore, the UE's action of not responding to the prematurely protected message was secure and compliant with the 5G standard. Secure
163	163	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039769887924194336 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399930477142334 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the AMF, where the UE sent an Identity Response message before the 5G-AKA authentication and key agreement procedure was completed. Immediately after receiving the Identity Response, the AMF sent a Deregistration Request to the UE, which was integrity protected and ciphered (security header type 2). According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) should only be applied after successful completion of the 5G-AKA procedure, as this process establishes the necessary security context and keys for encryption and integrity protection. Since the 5G-AKA was not completed, the UE had not yet derived the security keys required to process protected messages. The UE did not respond to the protected Deregistration Request, which is the expected and secure behavior according to the standard; it should ignore or discard any NAS messages that are protected before the security context is established. This prevents potential security vulnerabilities, such as accepting or acting on messages that it cannot verify or decrypt. Therefore, the UE's action of not responding to the protected Deregistration Request before 5G-AKA completion aligns with 3GPP security requirements and demonstrates secure behavior. 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.	In this test scenario, the 5G standalone User Equipment (UE) completed the initial NAS procedures and responded to an identity request with an identity response. Subsequently, the Access and Mobility Management Function (AMF) sent a Security Mode Command to the UE, which was marked as "protected" and indicated the use of ciphering and integrity algorithms (5G-EA4 and 128-5G-IA1) with a new security context. However, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is responsible for mutual authentication and the establishment of security keys, had not yet been completed at this point. According to 3GPP standards, encryption and integrity protection for NAS messages can only be securely applied after successful completion of 5G-AKA, as this process generates the necessary security keys. Since the AMF attempted to initiate NAS security procedures before 5G-AKA was completed, the UE appropriately rejected the Security Mode Command with an unspecified cause, as it did not yet have the required security context to safely engage in protected communication. This behavior aligns with 3GPP security requirements, as accepting protected messages or establishing a security context before authentication would expose the UE to potential security risks. Therefore, the UE's action in rejecting the Security Mode Command prior to 5G-AKA completion was secure and compliant with 3GPP standards. 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.	In this test scenario, the UE first sent an identity response to the AMF, after which the AMF issued a Security Mode Command in plain (unencrypted) NAS format, indicating that the 5G-AKA authentication and key agreement procedure had not yet been completed. The Security Mode Command specified the use of ciphering (128-5G-EA2) but null integrity protection (5G-IA0), and the security header was set to plain, meaning no encryption or integrity protection was applied to the NAS message. Upon receiving this, the UE responded with a Deregistration Request (UE originating), also sent in plain NAS format, before any security context was established. According to the 3GPP 5G standard, the UE should not accept security mode commands that do not provide integrity protection (i.e., use of 5G-IA0 is not allowed except for emergency services or specific cases), and should not send sensitive NAS messages (such as deregistration requests) in plain text before a security context is established via 5G-AKA. By sending a deregistration request in plain NAS before security activation, the UE exposed itself to potential security risks such as interception or manipulation of messages. Therefore, the UE's actions did not adhere to the 5G security requirements as outlined by 3GPP, making its behavior insecure in this context. 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.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, but the 5G-AKA (Authentication and Key Agreement) procedure was not yet completed. Immediately after, the AMF sent a Configuration Update Command to the UE, which was integrity protected (as indicated by the security header) but not encrypted, since encryption keys are only established after 5G-AKA completion. The UE did not respond to this protected message. According to the 3GPP 5G standard, the UE should only accept and process NAS messages that are integrity protected and, where required, encrypted, but only after the successful completion of the 5G-AKA procedure, which establishes the necessary security context. Since the 5G-AKA was not completed, the UE correctly did not respond to the Configuration Update Command, as accepting or processing such a message before security context establishment would be a security risk. Therefore, the UE's action of not responding aligns with the 3GPP security requirements and demonstrates secure behavior in this context. Secure

167	167	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.07818889617919922 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.07842707633972168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV, but this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA procedure had not yet been completed and security context was not established. According to the 3GPP 5G standard (TS 24.501), the UE must not send sensitive information such as the IMEI or IMEISV in response to a plain (unencrypted) identity request before NAS security is activated, as this would expose the UE's permanent identity to potential interception and compromise user privacy. In this test, the UE did not respond to the plain identity request for the IMEISV, which is the correct and secure behavior as per the standard. By refusing to send its IMEISV over an unprotected channel, the UE prevented possible leakage of sensitive information and adhered to the security requirements of the 5G system. 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.	In this test scenario, the UE completed the initial NAS steps and sent an authentication response to the AMF, indicating it was participating in the 5G-AKA authentication procedure. However, before the 5G-AKA process was completed (as indicated by "5G-AKA: Not completed yet"), the AMF sent a "service accept" message to the UE, which was marked as protected. Subsequently, the UE sent a deregistration request. According to the 3GPP 5G security standards, NAS message protection (encryption and integrity) should only be applied after successful completion of the 5G-AKA authentication and key agreement, which establishes the necessary security context. Since the 5G-AKA was not completed, the UE should not have accepted protected NAS messages or proceeded with further actions such as deregistration under the assumption of an established security context. By responding to a protected message and sending a deregistration request before the authentication process was finalized, the UE demonstrated insecure behavior, as it did not adhere to the required security procedures outlined by 3GPP for NAS message protection and state transitions. 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.	In this test scenario, the UE completed the initial NAS procedures and sent an Authentication Response to the AMF as part of the 5G-AKA authentication process. However, before the authentication procedure was completed, the AMF sent a GMM Status message with cause 26 ("Non-5G authentication unacceptable") in plain (unencrypted) form. According to 3GPP standards (TS 24.501), before the completion of 5G-AKA, NAS messages are exchanged in plain text since security context and ciphering keys have not yet been established. The UE, upon receiving the plain GMM Status message with cause 26, did not respond further. This behavior aligns with the 3GPP specification, which states that the UE should not proceed with further NAS procedures if authentication fails or is deemed unacceptable, and it is not required to respond to a GMM Status message indicating such a failure. The UE did not leak any sensitive information, nor did it continue communication in an insecure state after authentication was rejected. Therefore, based on the 3GPP standard, the UE's actions were appropriate and secure in this context. 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.	In the described test scenario, the UE and AMF engaged in NAS communication where the UE sent an authentication response to the AMF, but the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed. Immediately after receiving the authentication response, the AMF sent a deregistration request to the UE, which was integrity protected and ciphered (security header type 2). According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) should only be applied after successful completion of the 5G-AKA, when both the UE and the network have derived the necessary security keys. Since the 5G-AKA was not completed, the UE would not have the required keys to decrypt or verify the integrity of the protected deregistration request. The UE did not respond to this message, which is the correct and secure behavior as per the standard, because processing protected NAS messages without established security context could expose the UE to security risks such as replay or spoofing attacks. Therefore, the UE's action—refusing to process or respond to a protected message before security context establishment—demonstrates compliance with 3GPP security requirements. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should be active for subsequent messages. However, the AMF then sent an "identity request" message for the IMEISV in plain (unencrypted) NAS, rather than using a protected NAS message as required after security activation. The UE, upon receiving this unprotected identity request after security had been established, did not respond. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated, the UE must only accept and respond to NAS messages that are integrity protected and, where applicable, encrypted. Ignoring or rejecting plain NAS messages after security activation is the correct and secure behavior, as responding to such requests could expose sensitive information to interception or replay attacks. Therefore, the UE's refusal to respond to the unprotected identity request demonstrates adherence to the 5G security requirements and protects the user's privacy and device integrity. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE in plain (unencrypted) format, requesting the UE's GUTI. According to the 3GPP 5G standard (TS 24.501), once NAS security is established (i.e., after "security mode complete"), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore or discard any plain NAS messages received after security activation, as responding to such messages could expose sensitive information and compromise security. Therefore, the UE's action of not responding to the plain identity request was secure and compliant with the 5G security requirements. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Security Mode Complete message to the AMF, indicating that it was ready to establish NAS security (encryption and integrity protection). However, the AMF responded with a Service Reject message, which was sent in plain (unencrypted) form and included a 5GMM cause code 111 (protocol error, unspecified). Upon receiving this unprotected Service Reject, the UE proceeded to send a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G standard, after the Security Mode Complete message, all subsequent NAS messages between the UE and the AMF should be integrity protected and, if required, encrypted. The UE should only accept protected NAS messages after security activation; receiving and acting upon an unprotected (plain) Service Reject message after security mode completion is a violation of this requirement. By accepting a plain Service Reject and responding with a Deregistration Request, the UE demonstrated insecure behavior, as it failed to enforce the expected NAS security procedures and could be vulnerable to certain attacks (e.g., a plain message injection leading to denial of service). Therefore, the UE's action in this scenario was not compliant with the 5G security standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, which is the expected behavior as it indicates the UE has accepted the negotiated security algorithms and is ready to proceed with protected NAS communication. However, the AMF, under test control, subsequently sent an "authentication request" message to the UE in plain (unencrypted) form, despite the fact that the security context had already been established and NAS security should have been activated. According to 3GPP standards (TS 24.501), once the security mode is completed, all subsequent NAS messages must be integrity protected and, if required, ciphered. The UE, upon receiving a plain (unencrypted) authentication request after security activation, did not respond, which aligns with the 3GPP security requirements. This behavior is secure because the UE correctly rejected further plain NAS messages after security activation, thereby preventing potential security breaches such as replay or man-in-the-middle attacks. The UE's refusal to respond to an insecure message demonstrates compliance with the standard and proper security posture. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin protected NAS communication. However, the AMF then sent a "service accept" message to the UE in plain (unencrypted and unauthenticated) NAS, rather than using the agreed-upon security context. According to the 3GPP 5G standard (TS 24.501), once the security mode command is completed and acknowledged by the UE, all subsequent NAS messages between the UE and the AMF must be integrity protected and, if ciphering is enabled, also encrypted. The UE, upon receiving a plain (unprotected) NAS message after security activation, is required by the standard to discard the message and not respond, as accepting or acting on unprotected messages at this stage would expose the UE to security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected "service accept" message, which demonstrates correct and secure behavior as per the 3GPP specification. The UE's action of not responding to the plain message after security activation ensured that it did not compromise the integrity or confidentiality of its communication. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "registration complete" message to the AMF, indicating that the initial NAS security procedures had been finalized and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent an "identity request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted and unprotected) NAS format. According to the 3GPP 5G standards (TS 24.501), after the security context is established (i.e., after 5G-AKA and registration complete), the UE is required to reject or ignore any NAS messages that are not integrity protected and ciphered, as accepting plain messages at this stage would expose the UE to security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the plain identity request, which is the correct and secure behavior as per the standard, since responding to an unprotected identity request after security activation would compromise the UE's security. Therefore, the UE's action of not responding to the plain identity request was secure and compliant with 3GPP specifications. 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.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior. However, the AMF then sent an "Authentication Request" message to the UE in plain (unencrypted) form, even though the 5G-AKA procedure had already been completed and a native security context was established. According to the 3GPP 5G security standards (TS 33.501), after successful authentication and establishment of a security context, all subsequent NAS messages between the UE and AMF should be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) "Authentication Request" after security context establishment, did not respond. This behavior aligns with the 3GPP standards, as the UE is required to ignore or reject NAS messages that are not properly protected once a security context is in place, to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to the unprotected message demonstrates adherence to the security requirements of the 5G standard and protects against potential security vulnerabilities introduced by improperly protected signaling messages. 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.	In this security test, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "registration complete" message to the AMF, indicating that the initial NAS security context should have been established and all subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent an "identity request" message in plain (unencrypted) NAS, requesting the SUCI (Subscription Concealed Identifier) from the UE. Upon receiving this request, the UE responded not by providing the requested identity, but by immediately sending a "deregistration request (UE originating)" message. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), after 5G-AKA is completed and NAS security is activated, the UE must reject any further plain (unencrypted) NAS messages from the network, as accepting or responding to such messages could expose sensitive information or make the UE vulnerable to certain attacks (such as downgrade or replay attacks). By refusing to provide the SUCI in response to a plain identity request and instead deregistering, the UE correctly followed the security requirements and protected its identity and session. This behavior demonstrates that the UE is compliant with the 5G security standards and is not susceptible to this type of security downgrade or identity exposure attack. Secure

179	179	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.265115976333618 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2653589248657227 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.469132900238037 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security procedures should have been established and subsequent NAS messages should be protected (integrity protected and, if required, ciphered) as per 3GPP TS 24.501. However, the AMF then sent a "Configuration Update Command" as a plain (unencrypted and non-integrity protected) NAS message, which is not compliant with 3GPP security requirements post-authentication. Upon receiving this unprotected message, the UE responded by sending a "Deregistration Request (UE originating)" to the AMF, effectively terminating its registration. This action by the UE demonstrates that it detected the security violation (receipt of a plain NAS message after security context establishment) and responded as specified by the 3GPP standard, which mandates that the UE must reject or deregister upon receiving unprotected NAS messages when security should be active. Therefore, the UE's behavior was secure, as it correctly enforced the 5G security requirements by refusing to process insecure messages after authentication. Secure
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.	In this test scenario, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent an Uplink NAS Transport message to the AMF, which is expected to be protected by NAS security (integrity and ciphering) as per 3GPP standards. Subsequently, the AMF sent a Configuration Update Command to the UE, but this message was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to 3GPP TS 24.501, once NAS security has been activated (which should occur immediately after 5G-AKA), all subsequent NAS messages exchanged between the UE and the AMF must be protected using the established security context. The UE, upon receiving a plain Configuration Update Command after security activation, responded by sending a Deregistration Request (UE originating) to the AMF. This action aligns with the security requirements in the 3GPP standard, which states that the UE must treat any unprotected NAS message received after security activation as a potential security breach and should initiate deregistration or ignore the message to protect itself from possible attacks such as replay or man-in-the-middle. Therefore, the UE's behavior in this scenario—detecting the violation and deregistering—demonstrates adherence to the 5G security standard and is considered secure. Secure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Authentication Request message to the UE, but notably, this message was sent in plain (unencrypted) form, even though the 5G-AKA procedure had already been completed and a native security context was established. According to the 3GPP 5G security standards, once 5G-AKA is completed and a security context is in place, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where applicable, encrypted to prevent interception or tampering. In this test, the UE did not respond to the plain (unencrypted) Authentication Request from the AMF after security context establishment. This behavior aligns with the 3GPP standard, as the UE is expected to reject or ignore messages that are not properly protected after security activation. By refusing to respond to an unprotected message when it should have been protected, the UE demonstrated secure behavior in accordance with the standard. Secure

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, Registration 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.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes the security context for NAS message encryption and integrity protection), the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF responded with a Service Reject message, which was sent as a plain (unencrypted and unprotected) NAS message with 5GMM Cause 111 (Protocol error, unspecified). According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, ciphered. Therefore, the Service Reject message should have been sent in plain text, which is a violation of the standard, but since the AMF was under test control, the focus is on the UE's response. The UE, upon receiving a plain Service Reject after security context establishment, did not respond further. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore unprotected NAS messages after security activation, as processing such messages could expose the UE to security risks such as spoofing or downgrade attacks. Therefore, the UE's action—providing no response to the unprotected Service Reject—demonstrates adherence to the security requirements of the 5G standard. Secure

183	183	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000eeb598a00f560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5556139945983887 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.555833101272583 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5559549331665039 AMF to UE DownlinkNASTransport, Authentication request 0.7596380710601807 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, after which the AMF responded with an Authentication Request message that was sent in plain (unencrypted) form. Notably, the AMF included ABBA, RAND, AUTN, and ngKSI parameters, and the security context was indicated as native. Upon receiving this plain Authentication Request after 5G-AKA completion, the UE responded by sending a Deregistration Request (UE originating) to the AMF, effectively terminating its connection. According to the 3GPP 5G standard, after the 5G-AKA procedure is completed and a security context is established, all subsequent NAS messages between the UE and AMF must be integrity protected and, where required, encrypted. The fact that the AMF sent a critical message (Authentication Request) in plain text after security context establishment is a protocol violation and a potential security risk. The UE's action to deregister itself upon detecting this improper behavior aligns with the security requirements of the standard, as it prevents further communication over an insecure channel and protects the UE from possible replay or man-in-the-middle attacks. Therefore, the UE's response was secure and compliant with 3GPP specifications. Secure

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.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes security context for NAS message encryption and integrity protection), the UE sent an Uplink NAS Transport message to the AMF. The AMF then sent a Downlink NAS Transport message containing an Identity Request for the IMEI, notably transmitted as a plain (unencrypted) message. Instead of responding to the Identity Request with its IMEI, the UE immediately sent a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages—including identity requests and responses—must be integrity protected and, where possible, encrypted. Furthermore, the standard stipulates that the UE should not respond to identity requests for IMEI or IMEISV in plain NAS messages after security activation; instead, it should either ignore the request or deregister. By refusing to send its IMEI in response to an unprotected (plain) identity request and instead initiating deregistration, the UE demonstrated compliance with 3GPP security requirements, thereby protecting its sensitive identity information from potential interception or misuse. This behavior aligns with best security practices as defined by the standard. Secure
185	185	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 62 UE provided: No response The packet capture during the test using wireshark is: 2.4262688159942627 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4268429279327393 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.427194833755493 AMF to UE DownlinkNASTransport, Registration reject (No network slices available) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes security keys for NAS message encryption and integrity protection), the UE proceeded to send an Uplink NAS Transport message to the AMF. Subsequently, the AMF responded with a Registration Reject message, indicating "No network slices available" (5GMM Cause 62). Notably, this Registration Reject message was sent in plain (unencrypted and unprotected) form. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed and security context is established, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain Registration Reject message after security activation, should discard it and not act upon it, as accepting such a message could expose the UE to security vulnerabilities such as downgrade or denial-of-service attacks by malicious actors. In this test, the UE did not respond to the plain Registration Reject message, which aligns with the security requirements of the 5G standard, as it correctly ignored an unprotected message that should have been protected. Therefore, the UE's behavior was compliant with 3GPP security guidelines. Secure

186	186	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3200 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 5.633437156677246 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 5.634006023406982 AMF to UE SACK (Ack=11, Arwnd=106496) , DownlinkNASTransport, Security mode command 5.634031057357788 UE to AMF SACK (Ack=8, Arwnd=106454) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message (PDU session establishment request) to the AMF. The AMF then responded with a Security Mode Command message, which was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to 3GPP 5G security standards, the Security Mode Command is the mechanism by which the AMF instructs the UE to activate NAS security (ciphering and integrity protection) for subsequent messages. Upon receiving a plain Security Mode Command, the UE is expected to process it and respond with a Security Mode Complete message, which should be the first message protected with the negotiated security algorithms. However, in this test, the UE did not respond with a Security Mode Complete; instead, it immediately sent a Deregistration Request (UE originating) to the AMF, effectively aborting the session. This behavior suggests that the UE refused to proceed with the NAS security setup, possibly because it detected that the Security Mode Command was sent in plain text after authentication, which is permitted by the standard for this specific message but may be considered risky if the UE suspects any anomaly or misconfiguration. The UE's decision to deregister rather than proceed with potentially insecure communication demonstrates a cautious and security-conscious approach, aligning with the principle of failing safe in the presence of unexpected or potentially insecure conditions. Therefore, based on the 3GPP standard and the observed behavior, the UE's action can be considered secure. Secure
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.	In this security test, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message to the AMF. The AMF then responded with a Downlink NAS Transport message containing an Identity Request, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version) from the UE. Notably, this Identity Request was sent in plain (unencrypted) NAS, despite the fact that 5G-AKA had already been completed, which means that both the UE and the network had established security keys and were capable of encrypted NAS communication. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), after the completion of 5G-AKA, all subsequent NAS messages, especially those requesting sensitive information such as IMEISV, must be integrity protected and, where confidentiality is required, encrypted. The UE, upon receiving a plain (unencrypted) Identity Request after security activation, did not respond to the request. This behavior aligns with the 3GPP standard, which specifies that the UE must not disclose sensitive information like the IMEISV in response to unprotected requests once NAS security is active, as this would expose the UE to privacy and security risks (e.g., IMEI catching attacks). Therefore, the UE's refusal to respond to the unprotected Identity Request demonstrates correct and secure behavior according to the 5G standard. 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.	In this test scenario, the 5G-AKA authentication procedure was completed, establishing security context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Afterward, the UE sent a Service Request message to the AMF, which is expected behavior when the UE wants to resume or initiate a session. However, the AMF responded with a Deregistration Accept message sent in plain (unencrypted) form, even though the security context had already been established. According to the 3GPP 5G security standards (TS 33.501), after 5G-AKA completion, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. The UE, upon receiving a plain (unencrypted) Deregistration Accept message after security activation, did not respond. This behavior aligns with the 3GPP standard, which states that the UE should ignore any NAS messages that are not integrity protected or encrypted after security context is active, as accepting such messages could expose the UE to security risks like spoofing or session hijacking. Therefore, the UE's lack of response to the unprotected message demonstrates secure and standards-compliant behavior. Secure
189	189	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.602246046066284 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.602970123291016 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which then responded with a Security Mode Command message. Notably, this Security Mode Command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standards (TS 24.501), after 5G-AKA is completed, the Security Mode Command is the first message used to establish NAS security (ciphering and integrity protection) between the UE and the AMF. This message is allowed to be sent in plain text, as the security context has not yet been activated for NAS messages at this point. The UE, upon receiving this plain Security Mode Command, is expected to respond with a Security Mode Complete message, which would then be protected using the negotiated algorithms. However, in this test, the UE did not respond to the Security Mode Command at all. This lack of response means the UE did not proceed to establish NAS security, which is a deviation from the expected behavior as per the 3GPP standard. By failing to respond, the UE did not expose itself to immediate security risks (such as accepting an unprotected command or proceeding with unprotected communication), but it also did not fulfill the protocol requirements to establish secure communication. Therefore, while the UE did not act insecurely by accepting or processing an unprotected message beyond what is allowed, its lack of response is non-compliant and could be considered insecure from a protocol perspective, as it prevents the establishment of a secure channel for subsequent NAS messages. **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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF issued an authentication request message to the UE; notably, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, after 5G-AKA is completed and a security context is established (as indicated by ngKSI_TSC: Native security context), all subsequent NAS messages between the UE and AMF are required to be integrity protected and, where applicable, ciphered. The UE, upon receiving a plain (unencrypted) authentication request after security context establishment, did not respond. This behavior aligns with the 3GPP specification, which states that the UE must not accept or respond to plain NAS messages once a security context is in place, as this could expose the communication to security risks such as replay or man-in-the-middle attacks. Therefore, the UE's refusal to respond to the insecure message demonstrates correct and secure behavior according to the 5G standard. Secure

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.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. The AMF, instead of proceeding with a secured NAS communication (as would be expected after 5G-AKA completion), sent a new authentication request message in plain (unencrypted) form, using the same ngKSI (Key Set Identifier) as before. The UE responded with an "Authentication failure (ngKSI already in use)" message, indicating that it detected the reuse of an already established security context and refused to process the authentication request. According to the 3GPP 5G security standards, once a security context is established through 5G-AKA, all subsequent NAS messages between the UE and AMF must be integrity protected and, where required, encrypted. The UE is expected to reject or not process requests that attempt to reuse an active ngKSI or that are sent in plain text when a security context exists. By refusing to process the plain, repeated authentication request and signaling the error, the UE demonstrated correct and secure behavior as per the 3GPP specifications, protecting itself against potential replay or downgrade attacks. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Service Request to the AMF, which then responded with an Identity Request for the TMSI. Notably, the AMF sent this Identity Request as a plain (unencrypted) NAS message, even though the 5G-AKA procedure had already been completed, meaning that NAS security (encryption and integrity protection) should have been activated for subsequent messages. The UE, upon receiving this unprotected Identity Request, did not respond. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, the UE is required to only accept and respond to NAS messages that are integrity protected and, where applicable, encrypted. If the UE receives a plain (unprotected) NAS message after security activation, it should ignore or silently discard it to prevent potential security breaches such as identity theft or replay attacks. Therefore, the UE's action of not responding to the unprotected Identity Request aligns with the 5G security requirements and demonstrates secure behavior in this context. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step for requesting network services. The AMF then responded with a Configuration Update Command, sent as a protected downlink NAS message. However, the security header of the message was marked as "Unknown," and the UE did not provide any response to this message. According to the 3GPP 5G standards, after the 5G-AKA procedure, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. If the security header is not recognized or the message protection is not as expected, the UE is required to discard the message and not respond, to prevent potential security breaches or replay attacks. In this case, the UE's lack of response to a protected message with an unknown security header aligns with the 3GPP security requirements, as it avoids processing potentially malicious or malformed messages. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure
194	194	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 18.81248188018799 UE to AMF UplinkNASTransport, Service request 18.8126699924469 AMF to UE SACK (Ack=18, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a typical step to resume or establish a session. In response, the AMF sent an Authentication Reject message to the UE, and this message was transmitted in plain (unencrypted) form. According to the 3GPP 5G security standards, once 5G-AKA is completed, both integrity protection and ciphering (encryption) should be activated for all subsequent NAS messages, except for a few specific cases (such as initial registration or authentication messages before security context establishment). An Authentication Reject message sent after 5G-AKA completion should be protected, as the security context is already established. The UE, upon receiving an unprotected (plain) Authentication Reject after security activation, did not respond. This behavior aligns with 3GPP security requirements, which state that the UE must ignore or silently discard NAS messages that are not integrity protected when a security context is active, to prevent downgrade or replay attacks. Therefore, the UE's action—providing no response to an unprotected Authentication Reject after 5G-AKA—demonstrates correct and secure behavior as per the 3GPP standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF issued an identity request for the SUCI (Subscription Concealed Identifier) in plain (unencrypted) NAS, and the UE replied with an identity response. According to the 3GPP 5G security standard (TS 33.501), once 5G-AKA is completed, NAS security (encryption and integrity protection) should be activated for all subsequent NAS messages, except for a few specific cases (such as initial registration or when security context is unavailable). In this case, since 5G-AKA was already completed, the expectation is that the UE should only accept identity requests that are protected by NAS security. By responding to a plain (unencrypted) identity request after authentication, the UE exposes itself to potential security risks, such as identity disclosure or replay attacks, which the 5G standard is designed to prevent. Therefore, the UE's action of responding to an unprotected identity request after authentication is not compliant with 3GPP security requirements and is considered insecure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE initiated a Service Request to the AMF, which is a standard step to resume or establish a user session. The AMF then responded with a Configuration Update Command, which was sent as a protected (secured) downlink NAS message. However, the security header of the message was marked as "Unknown," and the UE did not provide any response to this message. According to the 3GPP 5G standards, after 5G-AKA, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, ciphered. If the UE receives a NAS message with an invalid or unknown security header, or if the message cannot be verified as protected, the UE is expected to discard the message and not respond, as a security measure to prevent potential attacks or protocol violations. In this test, the UE's lack of response to the configuration update command with an unknown security header indicates that it correctly identified a potential security issue and acted in accordance with the 3GPP security requirements by not processing or responding to the potentially insecure message. Therefore, the UE's action was secure. Secure

197	197	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005860328674316406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (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.	In this test scenario, the UE initiated the 5G registration process by sending an InitialUEMessage containing a Registration Request to the AMF. At this point, the 5G-AKA (Authentication and Key Agreement) procedure, which establishes security context for NAS message protection (integrity and ciphering), had not yet been completed. However, the AMF responded with a Deregistration Request message that was protected (integrity protected and ciphered), as indicated by the security header. According to the 3GPP 5G standard, the UE should only accept and process protected NAS messages after a successful authentication and security mode command exchange, which establishes the necessary keys for message protection. Since the 5G-AKA was not completed, the UE had not yet derived the security context required to decrypt or verify the integrity of protected messages. The UE, therefore, did not respond to the protected Deregistration Request from the AMF, which is the correct and secure behavior as per the standard. This prevents potential security vulnerabilities, such as accepting spoofed or malformed protected messages before security is established. In summary, the UE's action to ignore the protected message before completing 5G-AKA was secure and compliant with 3GPP specifications. 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.	In this test scenario, after completing the 5G-AKA authentication and security procedures, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message in plain (unencrypted) form, requesting the UE's GUTI. The UE did not respond to this request. According to the 3GPP 5G standards (TS 24.501), once NAS security is established (i.e., after the security mode complete message), the UE must only accept and respond to NAS messages that are integrity protected and, where required, encrypted. Any subsequent plain (unencrypted) NAS messages received after security activation should be ignored or rejected by the UE to prevent potential security breaches such as identity theft or man-in-the-middle attacks. The UE's lack of response to the plain identity request demonstrates correct and secure behavior, as it did not expose its identity information over an unprotected channel. Therefore, the UE's actions were in line with 3GPP security requirements and protected its sensitive information. Secure

199	199	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.1600339412689209 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602790355682373 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an Identity Request message to the UE, requesting the IMEISV, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), after NAS security is activated, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. The UE, upon receiving a plain (unencrypted) NAS message after security activation, is required by the standard to ignore the message and not respond, as responding to such a message could expose sensitive information to potential attackers. In this test, the UE did not respond to the plain Identity Request, which aligns with the security requirements of the 5G standard and demonstrates that the UE is correctly enforcing NAS security procedures to prevent information leakage. Therefore, the UE's action was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an Identity Request message to the UE in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier). According to 3GPP standards (TS 33.501), once NAS security is established, all subsequent NAS messages—especially those involving sensitive identifiers—must be protected (encrypted and integrity protected). The UE, upon receiving an unprotected (plain) Identity Request after security activation, did not respond. This behavior aligns with 3GPP security requirements, as responding to a plain request after security is established could expose sensitive information and make the UE vulnerable to certain attacks (such as replay or interception of identifiers). By refusing to respond to an unprotected request, the UE demonstrates compliance with the standard and maintains the confidentiality of its identity. Therefore, the UE's action in this scenario is secure. 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.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message in plain (unencrypted) form, requesting the UE's IMEI. According to 3GPP 5G standards (TS 24.501), once NAS security has been established (i.e., after the security mode complete), the UE must only respond to NAS messages that are integrity protected and, where applicable, ciphered. If the AMF sends a plain (unencrypted) identity request after security is established, the UE is expected to ignore it and not respond, in order to prevent potential security risks such as IMEI disclosure over an unprotected channel. In this test, the UE did not respond to the plain identity request, which aligns with the 3GPP security requirements and demonstrates secure behavior by not exposing sensitive information over an unprotected link. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security (integrity and encryption) should now be active for subsequent NAS messages. However, the AMF then sent an Identity Request message to the UE in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier). According to 3GPP 5G standards (TS 24.501), once NAS security has been established (i.e., after Security Mode Complete), all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) Identity Request after security activation, did not respond. This behavior aligns with the 3GPP security requirements, as the UE is expected to ignore or reject any unprotected NAS messages once security is active, to prevent potential security breaches or identity exposure. Therefore, the UE's action of not responding to the unprotected Identity Request was secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE requesting the GUTI, but this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), after NAS security is activated (i.e., after "security mode complete"), all subsequent NAS messages between the UE and the AMF must be protected by encryption and integrity. The UE, upon receiving an unprotected (plain) NAS message after security activation, is required by the standard to discard the message and not respond, as responding to such messages could expose sensitive information and create vulnerabilities. In this test, the UE did not respond to the plain identity request, which demonstrates correct and secure behavior as per the 3GPP specification. Therefore, the UE's action was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE, requesting the IMEISV, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standards (TS 24.501), once NAS security is established, the UE is required to only respond to NAS messages that are integrity protected and, where applicable, encrypted. If the UE receives a plain (unencrypted) NAS message after security activation, it should ignore it and not respond, as responding could expose sensitive information and undermine the security guarantees provided by the 5G-AKA procedure. In this test, the UE did not respond to the plain identity request, which is the correct and secure behavior as per the 3GPP specification. This ensures that sensitive information such as the IMEISV is not disclosed over an unprotected channel, maintaining the confidentiality and integrity of the UE's identity. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF. Subsequently, the AMF sent an "Identity Request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). Notably, this identity request was sent in plain (unencrypted) NAS signaling, despite the fact that 5G-AKA had already been completed, which should have established NAS security (encryption and integrity protection) for subsequent messages. The UE, upon receiving this plain identity request after security activation, did not respond. According to the 3GPP 5G standard (TS 24.501), once NAS security is established, the UE must only accept and respond to NAS messages that are integrity protected and, where required, encrypted. If the AMF sends a plain (unencrypted and unprotected) NAS message after security activation, the UE is expected to ignore it and not respond, as responding could expose sensitive information and violate security procedures. Therefore, the UE's action of not responding to the plain identity request after 5G-AKA completion aligns with the 3GPP security requirements and demonstrates secure behavior. 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.	In this test scenario, after the successful completion of 5G-AKA authentication and security setup, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security procedures were finished. Following this, the AMF sent an "Identity Request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). Notably, this identity request was sent in plain (unencrypted) NAS, even though the security context should have been established after 5G-AKA. According to the 3GPP 5G standards (TS 24.501), once NAS security has been activated, all subsequent NAS messages, including identity requests, must be protected (integrity protected and, if possible, encrypted). The UE, upon receiving an unprotected (plain) identity request after security activation, did not respond, which aligns with the 3GPP security requirements to prevent exposure of sensitive identifiers in the clear and to avoid responding to messages that violate the expected security context. This behavior demonstrates that the UE correctly enforced the security policy by refusing to process or respond to an insecure request, thereby protecting the subscriber's privacy and adhering to the standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that mutual authentication and key establishment had been achieved. Following this, the AMF sent an "Identity Request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). Notably, this identity request was sent in plain (unencrypted) NAS signaling, even though the security context should have been established after 5G-AKA. According to 3GPP standards (TS 33.501 and TS 24.501), after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered. The UE, upon receiving a plain (unencrypted) identity request after security activation, did not respond. This behavior aligns with 3GPP security requirements, as the UE must reject or ignore any NAS messages that are not integrity protected and ciphered after security mode is activated, to prevent potential security breaches such as replay or interception attacks. Therefore, the UE's refusal to respond to the unprotected identity request demonstrates correct and secure behavior according to the 5G standard. Secure
208	208	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4989509582519531 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.49918699264526367 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication and security procedures, the UE sent a "Registration Complete" message to the AMF, indicating that the NAS security context should now be active and all subsequent NAS messages must be protected (i.e., integrity protected and ciphered). However, the AMF, under test control, sent an "Identity Request" message in plain (unencrypted and non-integrity protected) NAS, requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE did not respond to this request. According to the 3GPP 5G security standard (TS 33.501), after the 5G-AKA and security mode command are completed, the UE must only accept NAS messages that are integrity protected and ciphered; any plain NAS messages received after this point should be ignored or rejected by the UE. By not responding to the plain "Identity Request" after security activation, the UE correctly followed the 3GPP security requirements, thereby protecting the subscriber's identity from potential exposure over an unprotected channel. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS security should be active. Subsequently, the AMF sent an "Identity Request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) NAS. According to the 3GPP 5G security standards, after the successful completion of 5G-AKA, all subsequent NAS messages, especially those that could reveal sensitive establishment request or request such information (like SUCI), must be protected using NAS security (i.e., encrypted and integrity protected). The UE, upon receiving a plain (unencrypted) identity request after security activation, correctly did not respond, as responding would risk exposing sensitive information in an insecure manner. This behavior is in line with 3GPP security requirements, which specify that the UE must not send identity responses containing sensitive information unless NAS security is active. Therefore, the UE's refusal to respond to an unprotected identity request after 5G-AKA demonstrates secure behavior as per the standard. 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.	In this test scenario, after the 5G-AKA authentication procedure was successfully completed, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS messages should now be protected (i.e., integrity protected and ciphered). However, the AMF subsequently sent an "Identity Request" message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and ciphered. If the UE receives a plain (unencrypted) NAS message after security activation, it is required by the standard to discard the message and not respond, as responding to a plain message could expose sensitive information and compromise security. Therefore, the UE's action of not responding to the plain "Identity Request" message after security was activated is compliant with the 3GPP 5G security requirements and demonstrates secure behavior. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that security context establishment and mutual authentication had been achieved. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the TMSI, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages between the UE and AMF must be integrity protected and, where required, encrypted. The UE, upon receiving an unprotected (plain) identity request after security activation, did not respond. This behavior aligns with the 3GPP specification, which states that the UE should ignore or discard any NAS messages that are not integrity protected after security is activated, to prevent downgrade or interception attacks. Therefore, the UE's refusal to respond to the plain identity request demonstrates compliance with 5G security requirements and protects against potential security threats. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with an Identity Request message asking for the IMEISV. Notably, the AMF sent this Identity Request as a plain (unencrypted) message, even though the security context had already been established through 5G-AKA. According to the 3GPP 5G standard (TS 24.501), once the security context is active, all subsequent NAS messages that could reveal sensitive information, such as identity requests for IMEISV, must be integrity protected and, where applicable, ciphered. The UE, upon receiving a plain (unencrypted) Identity Request after security activation, is expected to ignore the message and not respond, as responding would risk exposing sensitive information over an unprotected channel. In this test, the UE did not respond to the plain Identity Request, which aligns with the 3GPP security requirements and demonstrates that the UE correctly protected its identity information by refusing to send it in the clear. Therefore, the UE's behavior was secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending an Identity Request message to the UE. Notably, the Identity Request from the AMF was sent in plain (unencrypted) NAS, and it requested the SUCI (Subscription Concealed Identifier) from the UE. According to 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed, NAS security (i.e., encryption and integrity protection) must be activated for all subsequent NAS messages, especially those involving sensitive subscriber identities. The SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) and should only be transmitted over a secure, encrypted NAS connection after authentication and security mode command procedures are complete. In this test, the UE did not respond to the AMF's plain (unencrypted) Identity Request for the SUCI, which aligns with 3GPP security requirements to prevent exposure of subscriber information over an unprotected channel. Therefore, the UE's action in refusing to respond to an insecure identity request demonstrates adherence to the 5G security standards and proper protection of subscriber privacy. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, specifically a PDU session establishment request. In response, the AMF sent an Identity Request message to the UE, requesting the TMSI as the identity and notably sending this message in plain (unencrypted) form. The UE did not respond to this plain Identity Request. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted to prevent exposure of sensitive information. The TMSI, while a temporary identifier, is still considered sensitive and should not be transmitted in the clear after security activation. By refusing to respond to an unprotected (plain) Identity Request after security context establishment, the UE is adhering to the 3GPP security requirements and protecting its identity from potential interception or replay attacks. Therefore, the UE's action in this scenario is consistent with secure behavior as defined by the 5G standard. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message to the UE, specifically requesting the IMEISV, and this message was sent in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed, NAS signaling messages exchanged between the UE and the AMF must be integrity protected and, where confidentiality is required (such as for sensitive identifiers like IMEISV), encrypted. The IMEISV is considered sensitive information and should not be transmitted in plain text after security activation. By refusing to respond to a plain (unencrypted) Identity Request for the IMEISV after 5G-AKA completion, the UE is adhering to the 3GPP security guidelines and protecting the user's privacy and device identity from potential interception. Therefore, the UE's action in this scenario was secure and in compliance with the 5G standard. 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.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). Notably, this Identity Request message was sent in plain (unencrypted) form, even though the 5G-AKA authentication had already been completed, which should have established NAS security (encryption and integrity protection) for subsequent messages. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), after successful authentication and security mode command, all subsequent NAS messages—especially those involving sensitive identifiers like the SUCI—must be protected by NAS security. The UE, upon receiving an unprotected (plain) Identity Request after security was established, did not respond. This behavior aligns with the 3GPP security requirements, which state that the UE must ignore or reject requests for sensitive information if they are not properly protected after security activation. By refusing to respond to an insecure request for its SUCI, the UE prevented potential exposure of sensitive subscriber information. Therefore, the UE's action was consistent with the 5G security standards and demonstrated secure behavior in this context. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF issued an Identity Request message, specifically requesting the IMEISV, and sent this message in plain (unencrypted) NAS format. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted. Sensitive information such as the IMEISV should not be transmitted in plain text after security has been established, as this could expose the UE to privacy and security risks (e.g., IMEISV catching attacks). The UE's refusal to respond to a plain (unencrypted) identity request after 5G-AKA is completed aligns with the 3GPP security requirements, as the UE should only respond to such requests if they are integrity protected and encrypted. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Downlink NAS Transport message containing an Identity Request for the TMSI. Notably, this Identity Request was sent in plain (unencrypted) form, even though the 5G-AKA procedure—which establishes NAS security—had already been completed. According to 3GPP 5G security standards (TS 33.501), once NAS security is established after 5G-AKA, all subsequent NAS messages, including identity requests, must be integrity protected and, where applicable, encrypted. The UE, upon receiving an unprotected (plain) Identity Request after security activation, is expected to ignore or reject the request to prevent potential security breaches such as identity theft or interception by a rogue AMF. In this test, the UE did not respond to the unprotected Identity Request, which aligns with the 3GPP security requirements and demonstrates secure behavior by not exposing its identity information over an unprotected channel. Therefore, the UE's action was secure. 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.	In this test scenario, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent an Uplink NAS Transport message to the AMF, which is a standard procedure for initiating further NAS communication, such as a PDU session establishment request. The AMF then responded with an Identity Request message, specifically requesting the TMSI (Temporary Mobile Subscriber Identity), and this message was sent in plain (unencrypted) form. According to the 3GPP 5G security specifications, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where applicable, encrypted to prevent exposure of sensitive information and to protect against various attacks. The TMSI is a privacy-sensitive identifier, and the standard mandates that it should not be transmitted in the clear after security activation. In this test, the UE did not respond to the plain (unencrypted) Identity Request from the AMF, which is the correct and secure behavior as per 3GPP standards, since responding would have exposed the TMSI in an unprotected message. Therefore, the UE's refusal to respond to an unprotected identity request after security activation demonstrates adherence to the 5G security requirements and proper protection of subscriber privacy. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a plain (unencrypted) Identity Request asking for the UE's TMSI. The UE did not respond to this request. According to the 3GPP 5G standard, once 5G-AKA is completed, NAS messages carrying sensitive information—such as identity responses—must be integrity protected and, where applicable, encrypted. The AMF's plain (unencrypted) Identity Request after authentication is a deliberate test of the UE's security compliance. The UE's refusal to respond to an unprotected identity request after security activation is the correct and secure behavior, as it prevents potential exposure of sensitive identifiers over an unprotected channel. This demonstrates that the UE is adhering to the 3GPP security requirements by not disclosing its TMSI in response to an insecure request after the security context is established. Therefore, the UE's action in this scenario is secure. 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.	In this test scenario, the 5G-AKA authentication procedure was completed successfully, establishing a security context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent a Service Request to the AMF, which is a standard procedure to request access to network services. The AMF responded with a Service Accept message, but crucially, this message was sent in plain (unencrypted) text rather than being protected by NAS security, which should have been activated after the completion of 5G-AKA. According to the 3GPP 5G standard, once the security context is established via 5G-AKA, all subsequent NAS messages, including Service Accept, must be integrity protected and, where required, encrypted to prevent interception or tampering. The UE, upon receiving a plain (unencrypted) Service Accept message after security activation, did not respond further, effectively rejecting the insecure message. This behavior aligns with 3GPP security requirements, as the UE should not accept or process NAS messages that are not properly protected after security has been established. Therefore, the UE's action of not responding to the unprotected message demonstrates adherence to the 5G security standards and protects against potential security threats such as replay or man-in-the-middle attacks. Secure
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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a Service Request message to the AMF, which then responded with a Service Accept message. Notably, the Service Accept message from the AMF was sent in plain (unencrypted) text, and the UE did not provide any response to this message. According to the 3GPP 5G security standards, once 5G-AKA is completed, both NAS signaling integrity and ciphering should be activated before any further NAS messages are exchanged, except for a few specific exceptions (such as initial registration or authentication messages). The Service Accept message is not one of these exceptions and should be protected by NAS security. The fact that the UE did not respond to the unprotected (plain) Service Accept message indicates that it correctly detected the security anomaly and refused to process or acknowledge the insecure message. This behavior aligns with the 3GPP security requirements, which mandate that the UE must ignore or reject NAS messages that are not properly protected after security activation. Therefore, the UE's action in this scenario was secure. Secure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior for initiating a service. The AMF then responded with a Service Reject message, indicating a 5GMM Cause value of 9 ("UE identity cannot be derived by the network"), and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA, NAS messages exchanged between the UE and the AMF should be integrity protected and, where possible, encrypted to prevent eavesdropping or tampering. Upon receiving a plain Service Reject message after authentication, the UE did not respond further, which aligns with the security recommendations in the standard: the UE should ignore or drop unprotected NAS messages received after security has been activated, as these could be spoofed or malicious. Therefore, the UE's action of not responding to the unprotected Service Reject message demonstrates adherence to the 5G security requirements and protects against potential security threats such as downgrade or denial-of-service attacks. Secure
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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which then responded with a Service Reject message indicating "UE identity cannot be derived by the network" (5GMM Cause 9). Notably, the Service Reject message from the AMF was sent in plain (unencrypted) form, even though the security context should have been established after 5G-AKA. According to the 3GPP 5G standards, once the 5G-AKA procedure is completed, NAS messages exchanged between the UE and the AMF should be protected by integrity and, where applicable, encryption. The UE, upon receiving a plain (unencrypted) Service Reject message after security context establishment, did not respond further. This behavior is in line with 3GPP security recommendations, which state that the UE should ignore or silently discard any unprotected NAS messages that are received after security activation, as they could be the result of a security attack (e.g., replay or downgrade attacks). Therefore, the UE's action of not responding to the unprotected Service Reject message demonstrates adherence to the 5G security standard and proper handling of potentially insecure messages. 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.	In this test scenario, after successfully completing the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior for initiating a service in the 5G standalone architecture. The AMF, under test control, responded with a Service Reject message, indicating a protocol error (5GMM Cause 111), and crucially, this reject message was sent in plain (unencrypted) NAS format. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, ciphered. The UE, upon receiving a plain (unencrypted) Service Reject message after security context establishment, should not process or respond to this message, as accepting unauthenticated or unprotected messages could expose the UE to security risks such as spoofing or denial of service attacks. In this test, the UE did not respond to the unprotected Service Reject message, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by refusing to process a message that did not meet the expected security protections. Therefore, the UE's action was secure. Secure
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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior to initiate a service. The AMF, under test control, responded with a Service Reject message indicating a 5GMM Cause value of 21 (which corresponds to "synchronization failure"), and crucially, this reject message was sent in plain (unencrypted) form. According to the 3GPP 5G security specifications (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where possible, encrypted to ensure confidentiality and integrity of signaling. The UE, upon receiving a plain (unencrypted) Service Reject message after security context establishment, did not respond further. This behavior aligns with the 3GPP security requirements, as the UE is expected to ignore or silently discard any NAS messages that are not integrity protected or encrypted once a security context is active, to prevent potential security breaches such as replay or injection attacks. Therefore, the UE's action of not responding to the unprotected Service Reject message demonstrates compliance with the 5G security standard and is considered secure. Secure

227	227	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03d2 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.5453281402587891 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5457210540771484 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5461199283599854 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. The AMF then responded with a Security Mode Command, which was sent as a protected (i.e., ciphered and integrity-protected) message using the specified cipher (5G-EA6) and integrity (128-5G-IA2) algorithms. However, the UE did not respond to this Security Mode Command from the AMF. According to the 3GPP 5G standard, after 5G-AKA is completed, the AMF initiates the Security Mode Command to establish NAS security (encryption and integrity protection) for subsequent NAS messages. The UE is expected to process this command, validate the integrated security algorithms, and respond with a Security Mode Complete message. The fact that the UE did not respond to the Security Mode Command is a deviation from the standard, as it leaves the NAS security context unconfirmed and incomplete. This could expose the UE to potential security risks, such as replay or man-in-the-middle attacks, since the security context was not properly established and acknowledged. Therefore, the UE's lack of response to the Security Mode Command is considered insecure behavior according to the 3GPP 5G security procedures. Insecure

228	228	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00f2 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 2.722198963165283 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.7225029468536377 AMF to UE SACK (Ack=8, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.722743034362793 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) completed the 5G-AKA authentication procedure, after which it sent an Uplink NAS Transport message to the Access and Mobility Management Function (AMF). The AMF then responded with a Security Mode Command message, which was sent as a protected message, indicating that security procedures were being initiated. The Security Mode Command specified the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, meaning that no encryption or integrity protection would be applied to subsequent NAS messages. The security header in the message was marked as unknown, and notably, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standards, after successful authentication (5G-AKA), the UE and AMF must negotiate and activate security algorithms that provide at least integrity protection (and preferably encryption) for NAS messages. The use of null algorithms (EA0/IA0) is only permitted in exceptional cases (e.g., emergency services), and the UE is expected to reject or not respond to a Security Mode Command that requests null algorithms in normal operation, as this would leave the communication unprotected and vulnerable to attacks. In this test, the UE did not respond to the Security Mode Command requesting null algorithms, which aligns with the security expectations of the 3GPP standard by refusing to proceed with insecure parameters. Therefore, the UE's action was appropriate and secure in this context. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF, which is a standard step in establishing NAS communication. The AMF then responded with a Configuration Update Command, but crucially, this downlink NAS message was sent in plain (unencrypted) form, as indicated by the security header value of 0. According to the 3GPP 5G standards (TS 24.501), once NAS security has been activated following 5G-AKA, all subsequent NAS messages—except for a few explicitly allowed exceptions—must be integrity protected and, where applicable, encrypted. The Configuration Update Command is not one of the exceptions and should have been sent with security protection. The UE, upon receiving a plain (unprotected) NAS message after security activation, is required by the standard to discard the message and not respond, as a security measure to prevent downgrade or replay attacks. In this test, the UE did not respond to the unprotected Configuration Update Command, which aligns with the expected secure behavior defined by 3GPP. Therefore, the UE's action in this scenario was secure. Secure

230	230	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.6443009376525879 UE to AMF UplinkNASTransport, Registration complete 0.644589900970459 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command, Unknown code (0x31) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context establishment was finished. Subsequently, the AMF sent a "Security Mode Command" message to the UE, but crucially, this message was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), after the 5G-AKA procedure is completed and a NAS security context is established, all subsequent NAS messages, especially security-related ones like the Security Mode Command, must be integrity protected and, if possible, ciphered. The UE, upon receiving a Security Mode Command in plain text after security context establishment, is expected to treat this as a protocol error and should not respond to it, as responding could expose it to downgrade or replay attacks. In this test, the UE did not respond to the plain Security Mode Command, which aligns with the security requirements of the 5G standard and demonstrates that the UE correctly protected itself against a potential security vulnerability. Therefore, the UE's action was secure. Secure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE proceeds with NAS signaling. Subsequently, the AMF sent a Security Mode Command message to the UE, but crucially, this message was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, the Security Mode Command should be the first message to initiate NAS security (ciphering and integrity protection), and it is allowed to be sent in plain text. However, the UE is expected to respond to the Security Mode Command by activating the negotiated security algorithms and sending a Security Mode Complete message, which should be integrity protected (and possibly ciphered, depending on the configuration). In this test, the UE did not respond at all to the Security Mode Command. This lack of response is not compliant with the 3GPP standard, as the UE is required to process the Security Mode Command and reply accordingly. The absence of a response could indicate a security issue or a failure in the UE's NAS security handling, as it leaves the NAS signaling incomplete and potentially exposes the session to security risks. Therefore, based on the 3GPP standard and the expected behavior, the UE's action in this scenario is considered insecure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is the expected behavior to resume or establish a session. In response, the AMF sent an Authentication Reject message in plain (unencrypted) NAS, and the UE did not respond to this message. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF should be integrity protected and, where possible, encrypted. An Authentication Reject message sent in plain NAS after security context establishment is considered abnormal and potentially malicious. The standard specifies that the UE should ignore such messages if they are not integrity protected, as they could be an attempt to disrupt the session or downgrade security. The UE's lack of response to the plain Authentication Reject message indicates that it correctly recognized the message as non-compliant with security requirements and took no action, thus protecting itself from a possible attack or protocol downgrade. Therefore, the UE's behavior aligns with the 3GPP security standards and demonstrates secure handling of the situation. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF. In response, the AMF sent an Authentication Reject message back to the UE, and this message was sent in plain (unencrypted) form. The UE, upon receiving this plain Authentication Reject, did not respond further. According to the 3GPP 5G security standards, once 5G-AKA is completed, NAS signaling should be protected with integrity and ciphering, except for a few specific message types (such as initial registration and authentication messages before security is established). An Authentication Reject message sent after security context establishment (i.e., after 5G-AKA) should be integrity protected and ciphered. If the UE receives such a critical message in plain text after security has been established, it is expected to treat this as a potential security breach (e.g., a man-in-the-middle attack) and not process the message further. The UE's lack of response to the unprotected Authentication Reject message demonstrates that it correctly identified the message as insecure and refused to process it, as per 3GPP security requirements. Therefore, the UE's action in this scenario was secure. Secure
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.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the TMSI, but this request was sent as a plain (unencrypted) message because the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should not respond to identity requests that are sent in plain text after the authentication procedure has started but before security (ciphering and integrity protection) has been activated. This is to prevent potential interception or replay attacks by malicious actors, as sensitive information like the TMSI could be exposed if sent in the clear. In this test, the UE did not respond to the plain identity request, which aligns with the security requirements of the 5G standard and demonstrates that the UE is correctly protecting its identity information by refusing to transmit it before a secure channel is established. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF issued an identity request for the IMEISV, which was sent in plain (unencrypted) NAS message format because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should not be transmitted in plain text before the establishment of NAS security, which is only activated after successful completion of the 5G-AKA procedure. The UE, upon receiving an unprotected identity request for the IMEISV before NAS security was established, did not respond. This behavior aligns with the security requirements outlined in the standard, as the UE is expected to withhold sensitive information until a secure channel is established. By refusing to send the IMEISV in the clear, the UE protected its privacy and adhered to 3GPP security guidelines. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, after the 5G-AKA authentication procedure was completed, the UE sent an authentication response to the AMF. The AMF then sent a Security Mode Command to the UE, which, according to the packet capture and message details, was sent as a plain (unencrypted and unauthenticated) NAS message. The Security Mode Command is the critical step where the AMF instructs the UE which ciphering and integrity algorithms to use for subsequent NAS messages. According to the 3GPP 5G standard (TS 24.501), the Security Mode Command must be sent as a plain NAS message because NAS security context has not yet been established at this point. Only after the successful completion of the Security Mode Command procedure should the UE and AMF begin sending NAS messages with security protection (i.e., encrypted and integrity protected). However, in this test, the UE responded to the plain Security Mode Command by immediately sending a Deregistration Request (UE originating) as an uplink NAS message. If this Deregistration Request was sent as a plain NAS message (i.e., without NAS security protection), it would be considered insecure, as the UE should only send further NAS messages after security activation in a protected manner. The packet capture and test summary do not indicate that the Deregistration Request was integrity protected or ciphered, suggesting the UE sent it in the clear, which exposes the message to interception or tampering. This behavior does not comply with the 3GPP security requirements, as the UE should have waited for NAS security to be activated before sending further sensitive messages. Therefore, the action taken by the UE was insecure. 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.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which is the expected behavior. The AMF then sent a Security Mode Command to the UE, indicating the start of NAS security context setup. Notably, the Security Mode Command specified the use of ciphering algorithm 5G-EA5 and integrity algorithm 5G-IA0 (null), meaning that while the NAS messages would be encrypted, they would not be integrity protected. The security header was marked as "Unknown," and the ABBA parameter was set to 0000. Importantly, the UE did not respond to the Security Mode Command. According to 3GPP standards, the use of a null integrity algorithm (5G-IA0) is generally discouraged because it leaves NAS signaling vulnerable to modification attacks, even if encryption is applied. A compliant and security-conscious UE should reject or at least not proceed with a security context that does not provide integrity protection, as this would expose it to potential security risks. In this case, the UE's lack of response to the Security Mode Command can be interpreted as a refusal to accept insecure security parameters, which aligns with secure behavior as per 3GPP recommendations. Therefore, the UE's action in this scenario was secure. Secure
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.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF. The AMF, under test control, then sent another identity request to the UE, specifically requesting the TMSI, and this message was sent in plain (unencrypted) NAS signaling. At this stage, the 5G-AKA authentication had not yet been completed, meaning that NAS security context had not been established and all NAS messages were being exchanged in the clear. According to the 3GPP 5G standard (TS 24.501), before the completion of 5G-AKA and the establishment of NAS security, the UE is required to be cautious about what information it provides in response to plain (unencrypted) identity requests, especially sensitive identifiers such as the TMSI, SUPI, or IMSI. If the AMF requests an identity in plain NAS before security activation, the UE should only respond to certain types of requests (such as for SUCI or GUTI) and should not provide sensitive information like the TMSI or SUPI in the clear. In this test, the UE did not respond to the AMF's plain identity request for the TMSI, which aligns with the security requirements of the standard, as responding would have exposed sensitive information before a secure channel was established. Therefore, the UE's action was secure and compliant with 3GPP security guidelines. 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.	In this test scenario, the UE and AMF were engaged in NAS communication prior to the completion of the 5G-AKA authentication and key agreement procedure. The UE sent an identity response, after which the AMF issued another identity request, specifically requesting the IMEISV, and sent this request in plain (unencrypted) NAS signaling. According to the 3GPP 5G security standards, sensitive information such as the IMEISV should only be transmitted after the establishment of NAS security, which is achieved upon completion of the 5G-AKA procedure. Since the 5G-AKA was not yet completed, the NAS messages were unprotected, and the UE appropriately did not respond to the AMF's request for the IMEISV in plain text. This behavior aligns with 3GPP security recommendations, which state that the UE must not disclose sensitive identifiers over unprotected signaling channels. Therefore, the UE's refusal to respond with the IMEISV before NAS security was established demonstrates secure and standards-compliant behavior. 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.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then replied with a Security Mode Command. Notably, the Security Mode Command was sent as a plain (unencrypted and non-integrity protected) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), after successful authentication, the Security Mode Command is the first message that establishes NAS security (ciphering and integrity protection) between the UE and the AMF. The UE is expected to process this message only if it is received as a plain NAS message, as this is the standard behavior before security activation. However, after receiving the Security Mode Command, the UE did not respond. This lack of response could indicate that the UE either rejected the plain Security Mode Command or failed to process it, which is not compliant with the expected 3GPP behavior. The UE should accept a plain Security Mode Command immediately after authentication, as this is the only point in the NAS procedure where a plain message is allowed for security context setup. By not responding, the UE is not following the standard, but from a security perspective, this behavior is actually more restrictive and does not expose the UE to risk, as it does not process potentially insecure messages beyond the expected point. Therefore, while the UE's behavior is not fully compliant with 3GPP, it errs on the side of caution and does not create a security vulnerability. In summary, the UE's action was secure, as it did not process or respond to an unprotected message beyond the authentication phase, thus avoiding exposure to potential attacks. Secure

241	241	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.16009092330932617 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1604149341583252 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity protection). According to the 3GPP 5G standard, after the security mode complete message, both the UE and the AMF should have established and activated NAS security, meaning all subsequent NAS messages must be protected (i.e., integrity protected and, if applicable, ciphered). However, in this test, the AMF (under tester control) sent another "security mode command" message after the security mode complete, which is an unexpected and non-standard behavior, as the security mode command should not be sent again after security is activated. The UE did not respond to this message, which is the correct and secure behavior according to the 3GPP standard, as it should ignore or discard any unexpected or out-of-sequence security mode command messages received after security activation to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to the subsequent security mode command demonstrates adherence to the 5G security requirements and protects against potential security vulnerabilities introduced by protocol misuse. Secure

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.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF, which is the expected behavior. The AMF then sent a Security Mode Command to the UE, and this message was protected (i.e., encrypted and integrity protected) using the negotiated cipher (128-5G-EA1) and integrity (128-5G-IA2) algorithms, as indicated in the test summary. The ABBA parameter was also present, which is used for additional security binding. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard (TS 24.501), after successful authentication, the UE is expected to process the Security Mode Command, verify its protection, and respond appropriately (typically with a Security Mode Complete message). The fact that the UE provided no response is problematic: it means the UE did not acknowledge or process the protected Security Mode Command, which is a critical step for establishing secure NAS communication. This lack of response could indicate that the UE failed to recognize or accept the protected message, or that it did not support the required security algorithms or procedures. In either case, by not responding, the UE failed to complete the security setup as required by the standard, leaving the communication in an incomplete and potentially insecure state. Therefore, based on the 3GPP requirements for secure NAS communication, the UE's action in this scenario is considered insecure. Insecure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF, which is the expected behavior. The AMF then issued a Security Mode Command to the UE, but crucially, this command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standards (TS 24.501), after 5G-AKA is completed and before any security context is established, the Security Mode Command is the first message that should be protected by integrity (and optionally ciphering) using the negotiated algorithms. The UE is required by the standard to check the security header of received NAS messages after authentication, and if a Security Mode Command is received in plain text (i.e., without integrity protection), the UE must discard it and not respond, as this could be a security risk (e.g., a replay or man-in-the-middle attack). In this test, the UE did not respond to the plain Security Mode Command, which aligns with the 3GPP security requirements and demonstrates that the UE correctly enforced the standard's security policy by refusing to process or acknowledge an insecure message. Therefore, the UE's action was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms and the establishment of NAS security. However, following this, the AMF sent another "security mode command" message to the UE, but this message was sent in plain (unencrypted) form, even though security context had already been established. According to the 3GPP 5G standard (TS 24.501), once the security mode complete message is exchanged and security is activated, all subsequent NAS messages between the UE and the AMF must be integrity protected and, if a ciphering algorithm other than EA0 is selected, also encrypted. The UE, upon receiving a plain (unencrypted) security mode command after security activation, did not respond. This behavior aligns with the 3GPP standard, as the UE is expected to reject or ignore any NAS messages that are not properly protected after security activation, to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to an insecure, plain security mode command after security activation demonstrates secure and standards-compliant behavior. Secure
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 this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV, but crucially, this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), sensitive UE identities such as IMEISV should only be transmitted after NAS security (ciphering and integrity protection) is activated, which occurs only after successful completion of 5G-AKA. Since the AMF requested the IMEISV in plain text before security activation, the UE's refusal to respond is in strict adherence to the 3GPP security requirements, as responding would have exposed a sensitive identifier over an unprotected channel. Therefore, the UE's action of not responding to the unprotected identity request demonstrates correct and secure behavior as per the 5G standard. 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.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF responded with an identity request for the TMSI, which was sent as a plain (unencrypted) NAS message. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE should not respond to identity requests for sensitive identifiers (such as TMSI, IMSI, or SUCI) if the request is received in plain text after the authentication procedure has started but before security has been activated. This is to prevent exposure of subscriber identities over an unprotected channel, which could be exploited by attackers. In this test, the UE did not respond to the plain identity request from the AMF, which aligns with the security requirements of the 5G standard and demonstrates correct, secure behavior by the UE in protecting subscriber identity information. 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.	In this test scenario, after the UE completed the authentication response as part of the 5G-AKA procedure, the AMF sent an identity request for the IMEISV in plain (unencrypted) NAS, before the 5G-AKA procedure was completed and before NAS security was established. The UE did not respond to this identity request. According to the 3GPP 5G standard (TS 24.501), the UE should not send sensitive information such as the IMEI or IMEISV in plain NAS messages before NAS security (encryption and integrity protection) is activated, which only occurs after successful completion of 5G-AKA. By refusing to respond to the AMF's plain (unencrypted) identity request for the IMEISV prior to security activation, the UE correctly protected its sensitive information from potential interception or misuse. This behavior aligns with 3GPP security requirements and demonstrates that the UE is adhering to best security practices by not exposing its identity information over an unprotected channel. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, the 5G-AKA authentication procedure between the User Equipment (UE) and the Access and Mobility Management Function (AMF) was completed successfully, as indicated by the UE sending an authentication response. Following this, the AMF sent a Security Mode Command to the UE, which was protected (i.e., integrity protected and/or encrypted) and specified the use of ciphering algorithm 128-5G-EA2 and integrity algorithm 128-5G-IA3, with ABBA set to 1111. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard (TS 24.501), after successful authentication, the AMF initiates security mode control to establish NAS security; the UE is expected to respond with a Security Mode Complete message if it can process the command and agrees with the proposed algorithms. If the Security Mode Command is received with an unknown or unsupported security header, or if the message is not properly protected, the UE should discard the message and not respond, as a security measure to prevent downgrade or spoofing attacks. In this case, since the Security header was marked as "Unknown," the UE's lack of response aligns with the 3GPP standard's security requirements, as it prevents potential security vulnerabilities. Therefore, the UE's action in this scenario was secure. Secure
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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a normal step in resuming or establishing a user session. The AMF then responded with a Configuration Update Command, but crucially, this downlink NAS message was sent in plain (unencrypted and unauthenticated) form, as indicated by the security header value of 0 (Plain NAS message). According to the 3GPP 5G standard (TS 24.501), after the 5G-AKA procedure is completed and NAS security is established, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered. The UE, upon receiving a plain (unprotected) NAS message after security context establishment, is required by the standard to discard the message and not respond to it. In this test, the UE did not respond to the plain Configuration Update Command, which aligns with the security requirements of the 3GPP standard, as responding to such a message could expose the UE to security risks such as replay or man-in-the-middle attacks. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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.	In this test scenario, after completing the initial NAS steps, the UE sent an Identity Response to the AMF, and subsequently, the AMF sent another Identity Request, specifically requesting the IMEISV, in plain (unencrypted) NAS messaging. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to protect sensitive information such as the IMEI/IMEISV and should not send this information in plain text over the air interface if NAS security is not active. The UE, in this case, did not respond to the AMF's plain (unencrypted) request for the IMEISV, which aligns with the security requirements of the standard. This behavior prevents exposure of sensitive device identifiers before a secure channel is established. Therefore, the UE's action was secure, as it correctly withheld the IMEISV in the absence of NAS security, in compliance with 3GPP security guidelines. 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.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, following which the AMF sent another Identity Request for the TMSI in plain (unencrypted) NAS message format. At this point, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to respond to identity requests before security activation, but only for certain types of identities (such as SUCI or GUTI) and must not provide sensitive permanent identifiers (like IMSI) in plain NAS messages unless strictly necessary. In this case, the AMF requested the TMSI (a temporary identifier), and the UE chose not to respond. This behavior aligns with a conservative security posture, as responding to identity requests in plain NAS messages can expose the UE to privacy risks, such as identity interception or tracking. By withholding a response until NAS security is established, the UE avoids leaking even temporary identifiers over an unprotected channel. Therefore, the UE's action demonstrates a secure approach in line with the intent of 3GPP security guidelines, prioritizing the protection of its identity information in the absence of established NAS security. 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.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF. Subsequently, the AMF sent another identity request, specifically requesting the IMEISV, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should not be transmitted in the clear before security activation (i.e., before NAS security is established via 5G-AKA). The UE, upon receiving a plain identity request for the IMEISV before security activation, did not respond. This behavior aligns with the security recommendations in the 3GPP standard, which state that the UE should withhold sensitive identifiers until a secure NAS context is established. By refusing to send the IMEISV in the clear, the UE protected its privacy and adhered to the security requirements. Therefore, the UE's action was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a normal step to resume or establish a session. The AMF then responded with an Identity Request message, specifically requesting the GUTI (Globally Unique Temporary Identifier) from the UE. Notably, this Identity Request was sent in plain (unencrypted) NAS signaling, even though the 5G-AKA procedure had already been completed, meaning that both integrity and ciphering keys should have been established and NAS security should have been activated. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA and the activation of NAS security, all subsequent NAS messages, including Identity Requests, must be protected (i.e., integrity protected and, where applicable, ciphered). The UE, upon receiving an unprotected (plain) Identity Request after NAS security activation, is expected to ignore the message and not respond, as responding would expose sensitive information (such as the GUTI) over an unprotected channel, which could be exploited by an attacker. In this test, the UE did not respond to the plain Identity Request, which is the correct and secure behavior as per 3GPP standards. Therefore, the UE's action was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the security context should be established at this point. However, the AMF responded with a Service Accept message that was sent in plain (unencrypted) NAS, as indicated by the packet capture and test summary. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered (encrypted). The UE, upon receiving a downlink NAS message in plain text after security activation, is required by the standard to discard the message and not process it, as accepting plain NAS messages after security activation would expose the UE to security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the plain Service Accept message from the AMF, which indicates that it correctly identified the security violation and refused to process the insecure message. This behavior aligns with the security requirements of the 5G standard, demonstrating that the UE's actions were secure and compliant with 3GPP specifications. Secure
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.	In this security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which then responded with an Identity Request message asking for the IMEI. Notably, this Identity Request was sent in plain (unencrypted) NAS signaling, even though the security context should have been established after 5G-AKA. According to the 3GPP 5G standard (TS 24.501), once the security context is set up after authentication, all subsequent NAS messages—especially those requesting sensitive information such as the IMEI—must be integrity protected and, where possible, encrypted. The UE, recognizing that the AMF's Identity Request was sent in plain text after security activation, did not respond with its IMEI. This behavior aligns with 3GPP security requirements, which specify that the UE must not disclose sensitive identifiers like the IMEI over unprotected NAS signaling after security activation. Therefore, the UE's refusal to respond in this scenario demonstrates adherence to the 5G security standard and protects against potential privacy and security risks. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the registration process. Immediately after, the AMF sent a GMM Status message with cause value 97 ("Message type non-existent or not implemented") in plain (unencrypted) format. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed, NAS messages exchanged between the UE and AMF should be integrity protected and, where possible, encrypted. The GMM Status message was sent in plain text, which is not compliant with the security requirements post-authentication. The UE, however, did not respond to this unprotected message. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore any NAS messages received in plain text after security has been activated, unless explicitly allowed by the standard (which is not the case for GMM Status messages post-registration). By not responding to the unprotected message, the UE demonstrated correct and secure behavior as per 3GPP requirements, ensuring that it did not process or act upon potentially malicious or spoofed messages sent without proper security. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS security should be active. However, the AMF then sent an "Identity Request" message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE did not respond to this request. According to the 3GPP 5G standard, once 5G-AKA is completed and a security context is established, all subsequent NAS messages, including identity requests, must be protected with NAS security (i.e., encrypted and integrity protected). The UE is expected to ignore or reject any plain (unencrypted) NAS messages received after security activation, as responding to such messages could expose sensitive information and violate the security requirements of the standard. Therefore, the UE's action of not responding to the plain identity request after security was established aligns with the 3GPP security guidelines and demonstrates secure behavior in this context. Secure

258	258	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Plain Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.4842751026153564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4844861030578613 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport 2.688286066055298 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration and security setup were successfully finished. Subsequently, the AMF sent a "Deregistration Request" to the UE, which, according to the test summary, was sent as a plain (unencrypted) message but with the security header indicating "Integrity protected and ciphered (2)." The UE then responded with a "Deregistration Request (UE originating)" message. According to the 3GPP 5G standards, after the 5G-AKA procedure is completed, all subsequent NAS messages exchanged between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The UE's actions, as observed in the packet capture, show that it continued to respond to NAS messages and sent its own deregistration request after receiving a deregistration request from the AMF. However, the critical point is whether the UE accepted and processed a deregistration request from the AMF that was sent in plain (unencrypted) form after security activation. According to 3GPP TS 24.501, after security is activated, the UE must reject or ignore any NAS messages that are not integrity protected and ciphered. If the AMF sent a deregistration request in plain text and the UE accepted and acted upon it, this would be a violation of the 5G security requirements, as the UE should not process unprotected NAS messages post-security activation. Therefore, based on the information provided, the UE's action to process and respond to a plain (unencrypted) deregistration request after security activation is considered insecure according to the 3GPP 5G standard. Insecure
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.	In this security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected to be encrypted and integrity protected since 5G-AKA had already been completed. The AMF then responded with a GMM Status message, indicating a 5GMM cause of 99 ("Information element non-existent or not implemented"), and crucially, this message was sent in plain (unencrypted) text. According to the 3GPP 5G security standards (TS 24.501), after the security context is established (i.e., after 5G-AKA), all subsequent NAS messages, including GMM Status, must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) GMM Status message after security activation, is required by the standard to discard the message and not respond to it, as processing such a message could expose the UE to security risks such as replay or downgrade attacks. In this test, the UE did not respond to the unprotected GMM Status message, which is the correct and secure behavior as per the 3GPP specification. Therefore, the UE's actions were in full compliance with the 5G security requirements, ensuring the integrity and confidentiality of its communication. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration and security procedures had been finalized. Following this, the AMF sent a "5GMM Status" message with cause 101 ("Message not compatible with the protocol state") in plain (unencrypted) form, which is not standard behavior post-authentication, as all subsequent NAS messages should be integrity protected and, typically, encrypted according to 3GPP specifications. Upon receiving this unprotected status message, the UE responded by sending a "Deregistration Request (UE originating)" to the AMF. According to 3GPP TS 24.501, after 5G-AKA is completed, the UE is expected to reject or ignore any NAS messages that are not integrity protected, as accepting or acting on plain messages could expose the UE to security risks such as replay or man-in-the-middle attacks. By sending a deregistration request in response to an unprotected message, the UE did not adhere to the expected security behavior; instead, it should have ignored the message or reported a security error. This action could potentially allow an attacker to trigger deregistration by injecting plain status messages, which is a security vulnerability. Therefore, the UE's response in this scenario was not secure according to 3GPP standards. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request by sending an UplinkNASTransport message to the AMF. The AMF responded with a Security Mode Command, which was sent as a protected (encrypted and integrity-protected) message, specifying ciphering and integrity algorithms (128-5G-EA1 and 128-5G-IA2) and an ABBA value of 0101. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard, after 5G-AKA, the Security Mode Command is used to establish NAS security, and the UE is expected to respond with a Security Mode Complete message to confirm acceptance of the security context. The absence of any response from the UE is a deviation from the standard, as it neither accepts nor rejects the security context, potentially leaving the NAS signaling unprotected and failing to proceed with secure communication. This lack of response could indicate a security flaw or a non-compliant implementation, as the UE should either respond or explicitly reject the security mode if it cannot comply. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which then responded with a Security Mode Command message. Notably, the Security Mode Command was sent as a plain (unencrypted) NAS message, with the ciphering algorithm set to 5G-EA0 (null ciphering), and the integrity algorithm set to 128-5G-IA2. The UE did not respond to this Security Mode Command. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages should be integrity protected and, if possible, ciphered, except for specific cases such as the initial Security Mode Command, which is allowed to be sent in plain text to establish security algorithms. However, the use of the null ciphering algorithm (5G-EA0) is generally discouraged unless explicitly required, as it means no encryption will be applied to subsequent messages. The UE's refusal to respond to a Security Mode Command that proposes null ciphering (5G-EA0) aligns with best security practices, as responding would have resulted in unencrypted NAS communication, exposing sensitive information. Therefore, the UE's action to not respond to this insecure security configuration is compliant with 3GPP security recommendations and demonstrates secure behavior. Secure
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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which included a PDU session establishment request. In response, the AMF sent a Registration Reject message with 5GMM Cause 74 ("Temporarily not authorized for this SNPN"), and this message was sent in plain (unencrypted) NAS. The UE, upon receiving this plain Registration Reject, did not respond further. According to the 3GPP 5G security specifications (TS 33.501 and TS 24.501), after 5G-AKA is completed, NAS messages exchanged between the UE and AMF should be integrity protected and, where possible, encrypted. However, the 3GPP standard does allow certain critical messages, such as Registration Reject, to be sent in plain NAS under specific conditions, especially if security context establishment fails or if the network intentionally sends it in plain due to authorization issues. The UE's behavior—receiving a plain Registration Reject after 5G-AKA and not responding further—aligns with the standard, as the UE is expected to accept the rejection and cease further NAS communication. There is no indication that the UE accepted or acted upon any unauthorized or unprotected information, nor did it proceed with further communication that could compromise security. Therefore, based on the described interaction and adherence to 3GPP guidelines, the UE's actions were secure. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an UplinkNASTransport message to the AMF, which is expected behavior as the UE proceeds with NAS signaling under the assumption that security has been activated. However, the AMF responded with a Registration Reject message, specifically with 5GMM Cause 6 (Illegal ME), and crucially, this message was sent in plain (unencrypted) form. According to 3GPP 5G security standards (TS 24.501 and TS 33.501), once 5G-AKA is completed and NAS security is activated, all subsequent NAS messages, including Registration Reject, must be integrity protected and, if possible, encrypted. The UE, upon receiving a plain Registration Reject after security activation, is required by the standard to ignore such messages and not act upon them, as accepting unauthenticated or unprotected messages after security activation could expose the UE to security risks such as spoofing or denial of service. In this test, the UE did not respond to the unprotected Registration Reject, which aligns with the 3GPP security requirements and demonstrates that the UE correctly enforced NAS security procedures by refusing to process a plain message after security activation. Therefore, the UE's behavior in this scenario was secure. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF sent an authentication request message to the UE in plain (unencrypted) form, using the same ngKSI (Key Set Identifier) as previously established, indicating that the AMF was attempting to initiate a new authentication procedure with an already active security context. The UE responded with an "Authentication failure (ngKSI already in use)" message, indicating that it recognized the reuse of an existing ngKSI and refused to proceed with the authentication. According to the 3GPP 5G security standard (TS 33.501), once a security context is established via 5G-AKA, the ngKSI should not be reused for a new authentication procedure unless the previous context is invalidated or expired, and all subsequent NAS messages should be protected (integrity protected and, if possible, ciphered). The UE's refusal to accept a new authentication request with an already-in-use ngKSI and its detection of an unprotected (plain) downlink NAS message demonstrates adherence to the 5G security requirements, as it prevents potential replay or downgrade attacks and ensures that the security context is not compromised. Therefore, the UE's action in this scenario was secure and compliant with the 3GPP standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically a PDU session establishment request) to the AMF. In response, the AMF sent an Authentication Reject message in plain (unencrypted) NAS format. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed, both the UE and the AMF are expected to establish NAS security, which means subsequent NAS messages should be integrity protected and, where applicable, encrypted. The Authentication Reject message is an exception in some cases as it may be sent in plain NAS if NAS security context is not established or has been deleted, but in this scenario, since 5G-AKA was completed, the expectation is that the UE would have a valid NAS security context and would only accept Authentication Reject if it is integrity protected. The UE, in this test, did not respond to the plain (unencrypted and unprotected) Authentication Reject message from the AMF, which aligns with the 3GPP security requirements: the UE should ignore unauthenticated or unprotected messages after security context establishment to prevent security attacks such as downgrades or spoofing. Therefore, the UE's action of not responding to the plain Authentication Reject message after 5G-AKA completion is secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, specifically a PDU session establishment request. In response, the AMF sent an Authentication Reject message back to the UE, and this message was transmitted in plain (unencrypted) form. According to the 3GPP 5G standards, once 5G-AKA is completed, both the UE and the AMF are expected to derive NAS security keys and switch to protected (integrity protected and, if required, ciphered) NAS communication for all subsequent messages, except for a very limited set of messages (such as Service Reject or Deregistration Accept) that are explicitly allowed to be sent in plain text. The Authentication Reject message is not among those exceptions and, after authentication, should be protected. The UE, upon receiving an unprotected (plain) Authentication Reject message after 5G-AKA completion, correctly did not respond, as processing such a message could expose it to security risks such as downgrade or replay attacks. By refusing to process or respond to an unprotected message that should have been protected, the UE adhered to the security requirements of the 5G standard and demonstrated secure behavior in this context. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context had been established. Subsequently, the AMF sent a "Configuration Update Command" message to the UE, which, according to the test summary, was sent as a protected (secured) message. However, the security header of the downlink message was marked as "Unknown," and the UE provided no response to this message. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, ciphered. If the UE receives a NAS message with an unknown or invalid security header, or if the message cannot be verified as protected, the UE is required by the standard to discard the message and not process it further to prevent potential security breaches. In this test, the UE did not respond to the configuration update command with an unknown security header, which suggests that it correctly identified the message as potentially insecure or malformed and refused to process it. This behavior aligns with the security requirements of the 5G standard, as it prevents the UE from acting on potentially malicious or tampered messages. Therefore, the UE's action in this scenario was secure. Secure

269	269	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.46799302101135254 UE to AMF UplinkNASTransport, Registration complete 0.4681861400604248 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, which is expected behavior as part of the NAS registration procedure. Subsequently, the AMF sent a "Deregistration Accept" message to the UE; however, this message was sent in plain (unencrypted) form, despite the fact that 5G-AKA had already been completed and NAS security should have been activated. According to the 3GPP 5G security standards (TS 24.501), once NAS security is established following 5G-AKA, all subsequent NAS messages—except for a few specific exceptions (such as initial registration requests and certain emergency procedures)—must be integrity protected and, where applicable, ciphered. The "Deregistration Accept" message does not fall under these exceptions and should have been sent as a protected message. The UE, upon receiving this unprotected message, did not respond, which indicates that it correctly rejected or ignored the message due to its lack of security protection. This behavior aligns with the 3GPP security requirements, as the UE must not process or respond to NAS messages that are not properly protected after security activation. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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.	In this test scenario, the 5G standalone User Equipment (UE) completed several NAS procedures and sent an identity response to the Access and Mobility Management Function (AMF). Subsequently, the AMF, still before the completion of the 5G-AKA authentication procedure, sent another identity request to the UE, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version). Importantly, this identity request was sent in plain (unencrypted) NAS signaling, as the 5G-AKA procedure—which establishes the NAS security context—had not yet been completed. The UE did not respond to this identity request. According to the 3GPP 5G standards (TS 24.501), the IMEISV is considered a sensitive identifier, and the standard mandates that the IMEISV should only be requested and transmitted after NAS security has been activated (i.e., after 5G-AKA is completed and NAS messages are encrypted). By refusing to send the IMEISV in response to a plain (unencrypted) identity request, the UE is adhering to the security requirements of the 5G standard and protecting its sensitive information from potential interception. Therefore, the UE's action in this scenario is considered secure and compliant with 3GPP specifications. 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.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, and the AMF subsequently issued another Identity Request, specifically requesting the IMEI, in a plain (unencrypted) NAS message. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to protect sensitive information such as the IMEI and should not respond to identity requests for the IMEI or IMEISV in plain NAS messages before security activation. The UE's lack of response to the AMF's plain (unencrypted) Identity Request for the IMEI demonstrates adherence to this security requirement, as responding would have exposed the IMEI over an unprotected channel. Therefore, the UE's action was secure and compliant with the 3GPP standard, as it refused to send sensitive identity information before NAS security was established. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a Service Accept message that was marked as "Protected," even though the 5G-AKA authentication and key agreement procedure had not yet been completed. Following this, the UE sent a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G security standard, NAS messages between the UE and AMF should only be integrity protected and encrypted after successful completion of the 5G-AKA procedure, which establishes the necessary security context and keys. Since the 5G-AKA was not completed, the UE should not expect to receive or process protected (encrypted or integrity-protected) NAS messages from the AMF. The UE's action to deregister upon receiving a protected message before security context establishment is correct and aligns with 3GPP security requirements, as it prevents the processing of potentially spoofed or malformed messages and avoids premature trust establishment. Therefore, the UE's behavior in this scenario was secure and compliant with the 5G standard. Secure

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.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF immediately sent a deregistration request that was integrity protected and ciphered, as indicated by the security header (2). However, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that the necessary security context for encryption and integrity protection was not yet established between the UE and the network. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must only be applied after successful completion of 5G-AKA, when both parties have derived the required keys. Since the AMF sent a protected message before this process was complete, the UE, following the standard, did not respond to the deregistration request because it could not verify or decrypt the message without the security context. This behavior demonstrates that the UE correctly adhered to the 3GPP security requirements by refusing to process protected messages before authentication and key agreement were finalized, thus preventing potential security vulnerabilities. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, the UE completed the initial NAS steps and sent an Authentication Response to the AMF, but the 5G-AKA authentication procedure was not yet completed. Immediately after receiving the Authentication Response, the AMF sent a Deregistration Request to the UE, which was integrity protected but not encrypted, as 5G-AKA had not finished and security context was not established. The UE did not respond to this Deregistration Request. According to the 3GPP 5G standard, NAS messages that require confidentiality and integrity protection should only be accepted by the UE after the security context is established, which occurs after successful completion of 5G-AKA. Since the Deregistration Request was sent before 5G-AKA completion, the UE correctly did not respond to a message that was only integrity protected and not encrypted, as it could not verify the authenticity or confidentiality of the message. This behavior aligns with 3GPP security requirements, as the UE should not process or respond to protected messages before security activation. Therefore, the UE's action was secure and compliant with the standard. 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.	In this test scenario, the UE initiated a 5G registration procedure by sending an initial registration request to the AMF. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that security contexts for integrity protection and ciphering had not been established. Despite this, the AMF responded with a deregistration request message that was integrity protected and ciphered, as indicated by the security header (2). According to the 3GPP 5G standard, the UE should only process protected NAS messages after the 5G-AKA procedure has been successfully completed and the security context is in place. Since the UE had not yet established a security context, it correctly did not respond to the protected deregistration request from the AMF. This behavior aligns with the 3GPP security requirements, as processing protected messages without a valid security context could expose the UE to security vulnerabilities such as replay or spoofing attacks. Therefore, the UE's lack of response to the protected message prior to security context establishment demonstrates secure behavior in accordance with the 5G standard. 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.	In this test scenario, the UE completed the initial NAS steps and responded to an identity request from the AMF with an identity response. Subsequently, the AMF sent a Security Mode Command message to the UE as a plain (unencrypted and unauthenticated) NAS message, indicating that the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards, specifically TS 33.501, the Security Mode Command is the message that initiates the activation of NAS security (ciphering and integrity protection) and must be sent as a plain NAS message because security context is not established until after successful authentication (5G-AKA). However, the UE did not respond to the Security Mode Command. This behavior aligns with the 3GPP standard, which states that the UE should not proceed with security mode procedures if the authentication process (5G-AKA) has not been completed, as this would expose the UE to potential security risks such as replay or man-in-the-middle attacks. By not responding, the UE avoided establishing security based on an unauthenticated context, thereby protecting itself from possible attacks. Therefore, the UE's action in this scenario was secure and in compliance with the 5G security standards. 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.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF. Immediately after, the AMF sent a Configuration Update Command to the UE, which was integrity protected (as indicated by the security header) but not encrypted, since the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G standard, NAS message protection—specifically integrity protection and encryption—should only be applied after successful completion of the 5G-AKA procedure, which establishes the necessary security context. Since the 5G-AKA was not completed, the UE had not yet established the security keys required for protected communication. When the AMF sent a protected (integrity protected) message before the security context was established, the UE did not respond, which aligns with the 3GPP standard: the UE should ignore or discard NAS messages that are protected before security activation. This behavior prevents potential security vulnerabilities, such as replay or downgrade attacks, that could arise from processing protected messages without an established security context. Therefore, the UE's action of not responding to the prematurely protected message was secure and compliant with the 5G standard. Secure
278	278	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.3110721111297607 UE to AMF UplinkNASTransport, Identity response 2.311551094055176 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Configuration update command 2.3115811347961426 UE to AMF SACK (Ack=3, Arwnd=106437) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, which is expected to be in plain NAS since 5G-AKA authentication and security context establishment had not yet occurred. The AMF then sent a Configuration Update Command to the UE, also as a plain NAS message, which is permitted prior to the completion of 5G-AKA. However, the UE did not process the Configuration Update Command and instead immediately sent a Deregistration Request to the AMF. According to the 3GPP 5G standard (TS 24.501), certain NAS messages, such as Configuration Update Command, should only be accepted as plain messages before security is activated if they do not alter security-sensitive parameters. However, it is generally considered best practice for a UE to be cautious and, if it receives unexpected or potentially security-impacting plain NAS messages before security activation, to reject them or deregister, as a defense against possible attacks (such as configuration tampering or downgrade attacks). In this case, the UE's action to deregister rather than process the plain Configuration Update Command before 5G-AKA completion demonstrates a secure and standards-compliant behavior, as it avoids accepting potentially insecure configuration changes before a secure context is established. Secure

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.	In this test scenario, the UE initiated a 5G registration by sending an initial registration request to the AMF, which is the expected first step in establishing a secure connection. However, before the 5G-AKA (Authentication and Key Agreement) procedure could be completed—which is necessary to establish mutual authentication and derive encryption keys for NAS message protection—the AMF responded with a deregistration accept message that was marked as "protected." According to the 3GPP 5G standard, NAS message protection (integrity and encryption) must not be applied before the successful completion of the 5G-AKA procedure, as the required security context and keys are not yet established. The UE, upon receiving a protected message before security activation, correctly did not respond, as it cannot verify or decrypt the message without the necessary keys. This behavior aligns with the 3GPP security requirements, as the UE must ignore or discard any protected NAS messages received prior to the completion of authentication and security context setup. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is required to establish mutual authentication and derive keys for NAS message protection—the AMF responded with a deregistration accept message. Notably, this deregistration accept message was sent as a protected (integrity-protected and/or ciphered) NAS message, even though the security context had not yet been established. The UE, upon receiving this protected message before the completion of 5G-AKA, did not respond further. According to the 3GPP 5G security standards, the UE should only accept protected NAS messages after a security context has been established via 5G-AKA. Any protected message received before this point should be ignored or rejected, as the UE cannot verify its integrity or decrypt it without the necessary keys. The UE's lack of response indicates that it correctly ignored the prematurely protected message, thereby preventing potential security vulnerabilities such as replay or spoofing attacks. This behavior aligns with the 3GPP security requirements, demonstrating that the UE acted securely in this scenario. 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.	In this test scenario, the UE initiated the NAS communication by sending an initial registration request to the AMF. The AMF, under test control, responded with a Configuration Update Command that was integrity protected and ciphered using a new security context, as indicated by the security header type (4). However, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed at this stage, meaning that the necessary security context for encryption and integrity protection had not been properly established between the UE and the AMF. According to the 3GPP 5G standard, the UE should only accept and process NAS messages that are protected with a valid security context after successful completion of the 5G-AKA procedure. Since the UE did not respond to the protected Configuration Update Command sent before 5G-AKA was completed, it correctly rejected or ignored the message, thereby adhering to the security requirements of the standard. This behavior prevents potential security vulnerabilities, such as accepting messages with an invalid or unestablished security context. Therefore, the UE's action in this scenario was secure. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an Initial Registration Request to the AMF. The AMF, without completing the 5G-AKA authentication and key agreement procedure, responded with a Configuration Update Command that was integrity protected and ciphered (i.e., sent with a security header indicating protection). According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must only be applied after successful completion of the 5G-AKA procedure, which establishes the necessary security context and keys between the UE and the network. Since the 5G-AKA was not yet completed, the UE had not derived the required keys to decrypt or verify the protected message. The UE, therefore, did not respond to the AMF's protected Configuration Update Command. This behavior aligns with 3GPP security requirements, as the UE should not process or respond to protected NAS messages before security context establishment. By refusing to respond to a prematurely protected message, the UE avoided a potential security vulnerability. Thus, the UE's action in this scenario was secure. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an unprotected InitialUEMessage containing a Registration Request to the AMF, which is expected and compliant with the 3GPP standard, as initial NAS messages are sent unprotected before security context is established. However, the AMF responded with a Service Accept message that was protected (i.e., encrypted and/or integrity protected), even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security architecture, NAS message protection (encryption and integrity protection) can only be applied after successful completion of 5G-AKA, which establishes the necessary security context and keys. Since the UE had not yet completed 5G-AKA, it did not have the keys required to decrypt or verify the protected Service Accept message, and therefore, it did not respond to the AMF. This behavior is correct and secure according to the 3GPP standard, as the UE must ignore or discard any protected NAS messages received before security context is established. By not responding to the prematurely protected message, the UE prevented a potential security vulnerability or protocol confusion. Therefore, the UE's action in this scenario was secure. Secure
284	284	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006928443908691406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2013227939605713 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a Service Accept message that was marked as "Protected," even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G standard, NAS message protection (integrity and confidentiality) can only be properly established after successful completion of 5G-AKA, as this procedure provides the necessary security context and keys for message encryption and integrity protection. Since the UE had not yet completed 5G-AKA, it should not have accepted or processed any protected NAS messages from the AMF, as it would not have the cryptographic keys required to verify or decrypt them. Instead, the UE responded with a Deregistration Request, indicating it did not proceed with the registration under these insecure conditions. This behavior aligns with the 3GPP security requirements, as the UE did not accept protected messages without a valid security context and took steps to terminate the registration process. Therefore, the UE's actions were secure and compliant with the 5G standard. Secure

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) (Re-Protected Deregistration 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 this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected behavior during NAS registration. However, before the 5G-AKA authentication procedure was completed, the AMF sent a Deregistration Request message to the UE. Notably, this Deregistration Request was sent with a security header indicating that it was both integrity protected and ciphered, which should only be possible after the 5G-AKA procedure has been successfully completed and security contexts have been established. Since 5G-AKA had not yet been completed, the UE would not have the necessary keys to decrypt or verify the integrity of this message. The UE did not respond to the Deregistration Request, which aligns with the 3GPP 5G standard: the UE should ignore NAS messages that are protected with security algorithms if the security context has not yet been established (i.e., before completion of 5G-AKA). This prevents potential security vulnerabilities where an attacker could send protected messages before authentication is complete. Therefore, the UE's action—providing no response to the protected Deregistration Request—was secure and compliant with the 3GPP standard. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security context (encryption and integrity protection) was not yet established between the UE and the AMF. Following the registration request, the AMF responded with a GMM status message (5GMM Cause: 98, "Message type not compatible with the protocol state") as a protected (i.e., integrity protected and/or encrypted) downlink NAS message. According to the 3GPP 5G standard (TS 24.501), the UE is required to ignore any NAS messages that are protected (i.e., encrypted or integrity protected) before the NAS security context is established, as the UE cannot verify or decrypt such messages prior to successful 5G-AKA completion. In this test, the UE did not respond to the protected GMM status message, which aligns with the expected secure behavior defined by the standard. This prevents potential security vulnerabilities, such as replay or spoofing attacks, that could arise if the UE processed protected messages without an established security context. Therefore, the UE's action of not responding to the protected message before 5G-AKA completion was secure and compliant with 3GPP specifications. 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.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a GMM Status message indicating a 5GMM cause of 3 ("Illegal UE"), and this message was sent as "protected" (i.e., integrity protected and/or encrypted). However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for NAS message protection (encryption and integrity protection) was not yet established between the UE and the network. According to the 3GPP 5G standard (TS 24.501), the UE should only process protected NAS messages after security has been activated through the completion of 5G-AKA. If a protected NAS message is received before security activation, the UE is expected to discard the message and not respond, as it cannot verify its authenticity or integrity. In this test, the UE did not respond to the protected GMM Status message sent before security activation, which is the correct and secure behavior as per the 3GPP standard. By refusing to process or respond to a prematurely protected message, the UE avoids potential security risks such as replay or spoofing attacks. Secure
288	288	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00081181526184082 03 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.20334196090698242 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an initial registration request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using integrity protection (128-5G-IA2) but with no ciphering (5G-EA0, or null cipher), and indicated the use of a new security context. At this stage, the 5G-AKA authentication procedure had not yet been completed, meaning that the keys required for full encryption and integrity protection had not been established. Upon receiving the Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G security standards, the Security Mode Command should only be integrity protected (not encrypted) until the authentication procedure is complete, as encryption keys are not yet available. The UE correctly detected an issue with the received Security Mode Command (possibly due to the use of an invalid or incomplete security context or improper message formatting) and responded with an appropriate status message, rather than proceeding insecurely or accepting the command blindly. This behavior aligns with the 3GPP security requirements, as the UE did not accept potentially insecure parameters and did not proceed with further NAS procedures without proper authentication and key agreement. Therefore, the UE's actions were secure and compliant with the standard. 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.	In this test scenario, the UE and AMF engaged in NAS communication, where the UE first sent an Identity Response message to the AMF. Subsequently, the AMF sent another Identity Request message to the UE, specifically requesting the GUTI (Globally Unique Temporary Identifier), and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards, sensitive information such as permanent or temporary identifiers (like GUTI) should not be transmitted in plain text after the security context is established; however, before 5G-AKA is completed, messages are necessarily sent unprotected. Importantly, the UE did not respond to the AMF's subsequent plain Identity Request for the GUTI. This behavior aligns with security best practices, as the UE avoided exposing its identity information in an unprotected message, which could otherwise be susceptible to interception or replay attacks. By withholding its response until a secure context is established, the UE demonstrated adherence to the 3GPP security guidelines and protected its sensitive information. Secure
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.	In this test scenario, the UE and AMF were engaged in NAS communication prior to the completion of the 5G-AKA authentication procedure, which is necessary to establish a secure, encrypted channel for subsequent messages. After the UE sent an identity response, the AMF issued another identity request, specifically requesting the IMEISV, and sent this message in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G security standards, sensitive information such as the IMEISV should not be transmitted in plain text before the completion of 5G-AKA, as this would expose the UE to potential privacy and security risks, including device tracking and identity theft. By refusing to respond to the plain (unencrypted) identity request for the IMEISV before the security context was established, the UE adhered to the security requirements outlined by 3GPP, thereby protecting its sensitive information from potential interception. This behavior demonstrates that the UE acted securely and in compliance with the 5G standard. 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.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF, and subsequently, the AMF sent another Identity Request message to the UE, specifically requesting the TMSI. Importantly, this Identity Request was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard, the UE must be cautious about responding to identity requests that are not protected by NAS security, especially after it has already provided its identity. The standard (TS 24.501, section 5.4.4.4) specifies that the UE should not respond to further identity requests sent in plain NAS after it has already responded, to prevent exposure of sensitive information to potential attackers who might inject such requests before security is activated. In this test, the UE did not respond to the second, unprotected Identity Request, which aligns with the security recommendations of the 3GPP standard and demonstrates good security practice by not exposing its identity information in the clear. Therefore, the UE's action was secure. Secure
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.	In this test scenario, after the initial NAS procedures, the UE sent an Authentication Response to the AMF, indicating that the 5G-AKA authentication procedure was still ongoing and not yet completed. Immediately following this, the AMF sent a Deregistration Request to the UE, which was integrity protected (as indicated by the security header), but not encrypted, since the 5G-AKA had not been completed and thus no NAS security context (keys) had been established. The UE, upon receiving this protected Deregistration Request, did not respond. According to the 3GPP 5G standard, NAS message protection (integrity and encryption) can only be applied after successful completion of the 5G-AKA and the establishment of a security context. If the UE receives a NAS message with a security header indicating protection before the security context is established, the standard mandates that the UE must discard the message and not respond, as it cannot verify the integrity or decrypt the message. Therefore, the UE's lack of response to the integrity-protected Deregistration Request before 5G-AKA completion is compliant with the 3GPP security requirements and demonstrates secure behavior. 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.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the security context should have been established and that subsequent NAS messages should be integrity protected and, where required, encrypted according to 3GPP TS 24.501. However, the AMF then sent a "Configuration Update Command" to the UE as a plain (unencrypted and non-integrity protected) NAS message, which is not compliant with the 3GPP standard, as such messages must be protected after security activation. The UE, upon receiving this plain NAS message after security context establishment, did not respond. According to 3GPP specifications, the correct behavior for the UE in this situation is to discard any unprotected NAS messages received after security activation and not to process or respond to them, as accepting such messages could expose the UE to security risks such as replay or tampering attacks. Therefore, the UE's action of not responding to the unprotected "Configuration Update Command" was in line with the 3GPP security requirements and demonstrates secure behavior in this context. Secure
294	294	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 31313131313131313131005fb686550000 AUTN: 3030303030303000ee555fb686550000 ngKSI_TSC: Mapped security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 0.11998605728149414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.12024092674255371 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin secure NAS communication. However, the AMF then sent an "authentication request" message to the UE in plain (unencrypted) form, even though the security context should have already been established. According to the 3GPP 5G standard (TS 24.501), after the security mode command is successfully completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, if required, ciphered. The UE, upon receiving a plain (unencrypted and unprotected) authentication request after security mode completion, did not respond to this message. This behavior aligns with the 3GPP security requirements, as the UE must reject or ignore any NAS messages that are not properly protected after the security context is established, to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to the unprotected message was secure and compliant with the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to begin secure NAS communication. However, the AMF then sent a "service reject" message with 5GMM Cause 111 (protocol error, unspecified), and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standards (TS 24.501), after the security context is established and NAS security mode is complete, all subsequent NAS messages between the UE and AMF must be integrity protected and, if required, encrypted. The UE, upon receiving a plain (unencrypted) NAS message after security activation, is required by the standard to discard the message and not process it further, as accepting such messages could expose the UE to security risks such as replay or downgrade attacks. In this test, the UE did not respond to the plain "service reject" message, which is the correct and secure behavior as per the 3GPP specifications. By refusing to process or acknowledge the unprotected message, the UE maintained the integrity and confidentiality of the NAS signaling. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin secure NAS communication. However, the AMF subsequently sent an "authentication request" message to the UE in plain (unencrypted) form, despite the fact that, according to the 3GPP 5G standards, all subsequent NAS messages after the security mode complete should be integrity protected and, if possible, encrypted. The UE, upon receiving this plain authentication request after security context establishment, did not respond. This behavior aligns with the 3GPP security specifications, which state that the UE must reject or ignore any NAS messages that are not properly protected once a security context is active, as accepting such messages could expose the UE to security risks such as replay or downgrade attacks. Therefore, the UE's action of not responding to the unprotected message demonstrates adherence to the 5G security standard and reflects secure behavior. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to begin secure NAS communication with encryption and integrity protection enabled. Immediately after, the AMF sent a "deregistration accept" message to the UE, but this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once NAS security has been activated (i.e., after the security mode complete message), all subsequent NAS messages exchanged between the UE and the AMF must be protected with the agreed-upon security algorithms. The UE, upon receiving an unprotected (plain) NAS message after security activation, is expected to discard the message and not respond, as processing such a message could expose the UE to security risks such as replay or downgrade attacks. In this test, the UE did not respond to the unprotected deregistration accept message, which is the correct and secure behavior as per the 3GPP standard. By refusing to process or acknowledge the plain message after security activation, the UE demonstrated compliance with the security requirements of the 5G standard. 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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to establish NAS security (encryption and integrity protection). However, the AMF subsequently sent an "authentication reject" message to the UE, and this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once the security context is established (i.e., after the security mode complete message), all subsequent NAS messages between the UE and the AMF must be protected by encryption and integrity algorithms. If the UE receives a plain (unencrypted) NAS message after security activation, it should treat this as a potential security breach (such as a downgrade or replay attack) and must not process the message or respond to it. In this test, the UE did not respond to the plain "authentication reject" message sent by the AMF after security was established, which is the correct and secure behavior as per the 3GPP standard. This ensures that the UE is not vulnerable to attacks that attempt to bypass or downgrade security after authentication and key agreement have been completed. Secure

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.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with NAS security-protected communication. However, the AMF then sent an "authentication reject" message to the UE, and notably, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), after the security mode procedure is completed, all subsequent NAS messages—including any reject messages—must be integrity protected and, if possible, ciphered. The UE, upon receiving a plain "authentication reject" message after security activation, did not respond. This behavior aligns with the 3GPP specification, which states that the UE should ignore any unauthenticated or unprotected NAS messages once security is activated, as accepting such messages could expose the UE to security risks such as spoofing or downgrade attacks. Therefore, the UE's lack of response demonstrates secure behavior, as it correctly rejected an insecure message that did not meet the required security protections after the security context was established. 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.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. Following this, the AMF sent an "identity request" message to the UE, requesting the TMSI, but crucially, this message was sent in plain (unencrypted) form. According to 3GPP standards (TS 33.501 and TS 24.501), once NAS security is established (i.e., after the security mode complete), all further NAS messages must be protected (encrypted and integrity protected) to prevent interception or manipulation by unauthorized parties. The UE, upon receiving an unprotected identity request after security activation, did not respond. This behavior aligns with the 3GPP security requirements, which specify that the UE should ignore or discard any unprotected NAS messages received after NAS security is established, as responding to such messages could expose sensitive information or open the UE to security risks. Therefore, the UE's action—refusing to respond to an unprotected identity request after security activation—demonstrates compliance with the 5G security standard and is considered secure. Secure