UE Response Evaluation Report: Test time: 2025-07-17 10:57:23

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, 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 IMEI, 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, particularly TS 33.501, the IMEI is considered a permanent equipment identifier and is classified as sensitive information. The standard mandates that the IMEI should not be transmitted over the air in plain text unless it is strictly necessary and, ideally, only after a secure NAS connection has been established (i.e., after 5G-AKA is complete and NAS security is activated). In this test, the UE did not respond to the plain-text Identity Request for the IMEI, thereby refusing to expose its permanent identifier before a secure channel was established. This behavior aligns with the security recommendations of the 3GPP standard, as it prevents potential exposure of sensitive information to eavesdroppers. Therefore, the UE's action in this scenario was secure and in compliance with 5G security best practices. 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 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 containing 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 standard, it is expected and required that the UE provides the SUCI (which is a privacy-preserving, encrypted form of the permanent identifier SUPI) in response to such requests before NAS security is activated. The SUCI is specifically designed to protect the subscriber's identity even when sent over an unprotected channel. Therefore, the UE's action of sending the SUCI in plain text prior to 5G-AKA completion is compliant with the 3GPP standard and does not expose the permanent identifier (SUPI) or other sensitive information. Based on this, the UE's behavior in this scenario is considered secure. 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 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 activated after successful authentication and key agreement. The UE, upon receiving the plain Authentication Reject message, did not respond further, which aligns with the expected behavior: the UE should cease further NAS communication upon receiving an Authentication Reject, as it indicates that authentication has failed or is not permitted. This prevents the UE from proceeding with any potentially insecure or unauthorized communication. Therefore, the UE's action—sending the initial registration request, receiving 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. 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 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 containing 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 standard, it is expected and secure for the UE to provide the SUCI in plain text prior to the establishment of NAS security, as the SUCI is a privacy-preserving, encrypted version of the permanent subscriber identity (SUPI). The use of SUCI ensures that the actual SUPI is not exposed over the air, even when messages are unprotected. Therefore, the UE's action of responding with the SUCI in plain text before NAS security activation is compliant with 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 security context was not established, and all subsequent NAS messages, including the registration request and the AMF's registration reject, were exchanged in plain (unencrypted) form. Upon receiving a registration reject message from the AMF with 5GMM cause 111 (protocol error, unspecified), the UE responded by sending a deregistration request (UE originating) to the AMF, also in plain text. According to the 3GPP 5G standard, it is expected and acceptable for the UE to send and receive NAS messages in plain text prior to the completion of 5G-AKA, as security context and encryption are only established after successful authentication. The UE's behavior—sending a deregistration request in response to a registration reject before security activation—aligns with the standard and does not expose additional security risks, since no sensitive user data is transmitted before authentication. Therefore, the UE's actions in this scenario are consistent with 3GPP security requirements and do not constitute a security vulnerability. 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 initial registration request to the AMF. The AMF, under test control, responded with a registration reject message (5GMM Cause 22: Congestion) before the 5G-AKA authentication and key agreement procedure was completed. As a result, the registration reject message was sent in plain (unencrypted) form, which is expected since security context establishment (via 5G-AKA) had not yet occurred. Upon receiving the registration reject, the UE responded with a deregistration request (UE originating), also sent in plain text, as no security context was available. According to 3GPP standards (TS 24.501), the UE is required to accept and process registration reject messages sent in plain text prior to security activation, and it is also permitted to send subsequent NAS messages (such as deregistration request) in plain text under these circumstances. The UE's actions—accepting the plain registration reject and responding appropriately—are in line with the 5G security procedures, as encryption and integrity protection are only mandated after successful authentication and key agreement. Therefore, the UE's behavior in this scenario is compliant with the 3GPP standard and does not introduce any security vulnerability within the defined protocol flow. 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, the UE initiated a registration procedure 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, with the ABBA field set to 0000, a RAND value of all zeros, and an AUTN value that does not appear to be valid. The ngKSI indicated a native security context, but the 5G-AKA authentication procedure had not yet been completed, which is a prerequisite for establishing a secure NAS communication channel. Upon receiving the authentication request, the UE responded with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it rejected the authentication attempt because the request did not conform to 5G security requirements (e.g., the use of a non-random RAND, invalid AUTN, or the message being sent in plain text). According to the 3GPP 5G standard, the UE must not accept authentication requests that do not meet the security requirements, such as those with invalid parameters or those sent in plain text before the security context is established. By refusing to proceed with the authentication and signaling the failure, the UE demonstrated correct and secure behavior as per the 5G standard, protecting itself from potential security threats such as replay or downgrade attacks. 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, with the 5G-AKA authentication procedure not yet completed. The authentication request included a RAND and an AUTN value of all zeros, which is not a valid AUTN per 3GPP standards. Upon receiving this, the UE did not proceed with authentication but instead responded with a 5GMM status message indicating "Invalid mandatory information." According to 3GPP 5G security standards, the UE should not process or respond to authentication requests that are malformed or contain invalid mandatory fields, especially before a security context is established. By refusing to process the invalid authentication request and instead reporting an error, the UE demonstrated correct and secure behavior, as it did not expose itself to potential security risks such as replay or downgrade attacks that could arise from processing unauthenticated or malformed messages. This response aligns with the 3GPP security requirements, which mandate that the UE must validate the integrity and correctness of NAS messages before proceeding with sensitive operations. 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 communication prior to the completion of the 5G-AKA authentication procedure. The UE first sends an identity response to the AMF, after which the AMF issues another identity request, specifically requesting the SUCI (Subscription Concealed Identifier), and the UE responds accordingly. Importantly, these messages are exchanged in plain (unencrypted) form, as the 5G-AKA procedure—which establishes NAS security and enables encryption—has not yet been completed. According to the 3GPP 5G standard, it is expected that initial identity requests and responses (such as SUCI) may be sent in plain text before authentication and key agreement are established, since the UE and network have not yet derived the necessary security context. However, the UE must ensure that it never sends the cleartext SUPI (Subscription Permanent Identifier) before security is activated; only the SUCI, which is a privacy-preserving, encrypted form of the SUPI, is allowed in this phase. In this test, the UE responded with the SUCI as requested, and did not send the SUPI in cleartext. Therefore, the UE's actions are in line with the 3GPP security requirements for pre-authentication identity exchange, and there is no evidence of insecure behavior in this context. 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 message to the UE in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. Upon receiving this authentication request, the UE replied with an authentication failure message, specifically indicating "ngKSI already in use." According to the 3GPP 5G security standards, the UE should not accept authentication requests that reuse an ngKSI (NAS key set identifier) that is already in use, as this could indicate a replay attack or an attempt to compromise the security context. The UE's action to reject the authentication request and respond with an authentication failure is in line with the 3GPP security requirements, as it prevents the establishment of a potentially insecure or compromised security context. This behavior demonstrates that the UE is correctly enforcing the security procedures required before establishing a secure NAS communication channel. Therefore, the UE's action in this scenario was 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 test scenario, the UE and AMF engaged in NAS communication where, after the initial steps, the UE sent an Identity Response message to the AMF. The AMF, under test control, replied with a Service Reject message indicating "PLMN not allowed" (5GMM Cause 11), and this message was sent in plain (unencrypted) form. The 5G-AKA authentication procedure had not yet been completed, which is a prerequisite for establishing NAS security (encryption and integrity protection of messages). According to the 3GPP 5G standard, before 5G-AKA is completed, NAS messages are permitted to be sent in plain text, as security contexts have not yet been established. The UE, upon receiving the Service Reject message, did not respond further, which is consistent with expected behavior since the network has denied service. Therefore, the UE's actions—sending the required Identity Response in plain text before security activation and not responding to a valid Service Reject—are in line with 3GPP security procedures. There is no indication that the UE exposed itself to unnecessary risk or deviated from the standard. 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 and AMF engaged in NAS communication before the completion of the 5G-AKA authentication procedure, which is required to establish NAS security (encryption and integrity protection). 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. All these messages, including the identity response containing the SUCI, were exchanged in plain (unencrypted) NAS messages, as indicated by the packet capture and the fact that 5G-AKA was not yet completed. According to the 3GPP 5G standard, the initial identity exchange (including SUCI) is permitted to occur before NAS security is established, and the SUCI itself is a privacy-preserving identifier designed to be sent in the clear without exposing the subscriber's permanent identity (SUPI). Therefore, the UE's action of sending the SUCI in response to an identity request, even in plain NAS, is compliant with the standard and does not expose sensitive information. The UE did not send the SUPI or any other sensitive identifier in the clear. Based on this, the UE's actions were secure and in line with 3GPP requirements for this stage of the procedure. 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 5G standalone User Equipment (UE) completed the initial NAS procedures and sent an Identity Response message to the Access and Mobility Management Function (AMF). The AMF, under test control, responded with an Authentication Reject message, which was sent in plain (unencrypted) form. The UE, upon receiving this Authentication Reject, did not respond further. According to the 3GPP 5G standard, NAS messages are only protected (encrypted and integrity protected) after the successful completion of the 5G-AKA authentication procedure. Since the 5G-AKA was not completed in this test, it is expected and compliant for the UE to accept and process plain NAS messages, including the Authentication Reject. Furthermore, the UE's lack of response to the Authentication Reject is also in line with the standard, as the UE is expected to abort the registration procedure and not take further action upon receiving such a message. Therefore, the UE's behavior in this scenario is secure and conforms to the 3GPP specifications for handling NAS messages prior to the establishment of security context. 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. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the security context for NAS message encryption and integrity protection was not yet established. The AMF then sent a registration reject message with 5GMM Cause 22 (Congestion) to the UE, and this message was sent in plain (unencrypted) form. The UE did not respond further after receiving the registration reject. 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 encryption and integrity protection are only mandated after successful authentication and key agreement. The UE's behavior—sending an identity response in plain text before 5G-AKA and ceasing communication after receiving a registration reject—aligns with the expected and secure operation as defined by the standard. Therefore, the UE's actions in this scenario were secure and compliant with 3GPP requirements. 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 UE sent an identity response to the AMF, the AMF replied with an authentication request message that was sent in plain (unencrypted) form, with the 5G-AKA procedure not yet completed. The authentication request included suspicious or invalid parameters, such as an AUTN value of all zeros and a RAND value that does not appear to be random. Upon receiving this, 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 authentication requirements. According to the 3GPP 5G standard, the UE must verify the validity of authentication requests and should not proceed with authentication if the request is malformed, uses invalid parameters, or is not protected as required. The UE's refusal to accept a non-5G-compliant authentication request, especially one sent in plain text before the establishment of a security context, demonstrates adherence to the security requirements of the standard. This behavior prevents potential security breaches, such as replay or downgrade attacks, and ensures that sensitive authentication steps are not performed unless the proper security procedures are followed. Therefore, the UE's action in this scenario was secure. 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, 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 standard (TS 24.501), after the completion of 5G-AKA, the Security Mode Command is the first message that establishes NAS security (ciphering and integrity protection) between the UE and the AMF. However, the Security Mode Command itself is always sent as a plain NAS message, since security context is not yet established at this point. The UE is expected to process this message, derive the security keys, and respond with a Security Mode Complete message, which should be the first NAS message protected with the negotiated security algorithms. In this test, the UE did not respond to the plain Security Mode Command. This behavior is not compliant with the 3GPP standard, as the UE is expected to accept and process a plain Security Mode Command after 5G-AKA, and only reject it if there is a mismatch or error in the parameters. By not responding, the UE is not following the standard procedure, but from a security perspective, it is not exposing itself to risk by refusing to process a plain message at this stage. However, this also means the UE cannot establish secure NAS communication, which is required for normal operation. Therefore, while the UE's action is not compliant with the standard, it is not insecure in the sense of exposing sensitive information or accepting insecure commands. It is, however, overly strict or non-functional. **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 AMF. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is required to establish security context and enable encryption—the AMF responded with a Service Reject message, specifically with 5GMM Cause 111 (Protocol error, unspecified). Notably, this Service Reject message was sent in plain (unencrypted) form, as expected since security context had not yet been established. The UE, upon receiving this plain Service Reject, did not respond further. According to the 3GPP 5G standards, the UE should not expect encrypted messages before the completion of 5G-AKA, and it is correct behavior for the UE to accept and process certain critical NAS messages, such as Service Reject, in plain form prior to security activation. Furthermore, the UE's lack of response after receiving the Service Reject is appropriate, as the session is considered terminated. Therefore, the UE's actions in this scenario align with the security requirements and expected behavior as outlined by 3GPP. 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, but the 5G-AKA authentication procedure was not yet completed. Subsequently, the AMF sent an identity request for the SUCI (Subscription Concealed Identifier) in plain (unencrypted) NAS, and the UE responded with an identity response. According to the 3GPP 5G security standard, NAS messages are only protected (encrypted and integrity protected) after the successful completion of the 5G-AKA procedure, which establishes the necessary security context. Before this, messages—including identity requests and responses—are sent in plain text. The use of SUCI, which is a privacy-preserving, encrypted form of the subscriber identity (SUPI), is specifically designed to protect the subscriber's identity even when sent over an unprotected channel. 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. The UE did not send the SUPI or any unprotected permanent identifier, which would have been a security risk. Thus, the UE's behavior in this scenario is considered secure according to the 5G standard. 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, 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 would be applied to subsequent NAS messages, while integrity protection was set to 128-5G-IA2. 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 security standards, after authentication, the UE and network must negotiate security algorithms for both integrity and ciphering. The use of 5G-EA0 (null ciphering) is only permitted under specific, controlled circumstances (such as emergency services or regulatory requirements), and generally, the UE is expected to reject security mode commands that attempt to establish a null ciphering algorithm in normal operation, as this would leave user data unprotected. The UE's action to reject the Security Mode Command when only null encryption was proposed aligns with the security requirements of the 5G standard, as it prevents the establishment of an insecure communication channel. Therefore, the UE's behavior in this scenario was secure and compliant with 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, the UE and AMF are engaged in the NAS authentication procedure as part of the 5G-AKA process. The UE first sends an Authentication Response to the AMF, which is expected behavior after receiving a valid Authentication Request. However, the AMF, under test control, then sends another Authentication Request to the UE, and the UE responds again with an Authentication Response. Notably, the 5G-AKA procedure has not yet been completed, meaning that NAS security (encryption and integrity protection) has not been activated; thus, all messages, including sensitive authentication responses, are sent in plain (unencrypted) form. According to the 3GPP 5G standard, the UE should only respond to a single Authentication Request and should not process or respond to repeated or unexpected Authentication Requests, especially if they are sent in plain text after an initial successful authentication exchange. By responding to a second, unexpected Authentication Request in plain text, the UE exposes itself to potential replay or downgrade attacks, as an attacker could exploit this behavior to extract authentication responses or manipulate the authentication process. Therefore, the UE's action of responding to a repeated Authentication Request in plain text before security activation is not compliant with 3GPP security recommendations and is considered insecure. Insecure

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 5G-AKA authentication procedure, which had not yet been completed, meaning that a secure NAS security context was not yet established. 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) form. The UE then responded with an "Authentication failure (MAC failure)" message, indicating that it detected an integrity failure in the received authentication request, specifically a MAC (Message Authentication Code) mismatch. According to the 3GPP 5G security standards, the UE is required to verify the integrity of authentication messages using the MAC and to reject any message where the MAC does not validate, as this could indicate a replay attack, tampering, or an otherwise invalid authentication attempt. The UE's action to reject the authentication request and report a MAC failure is the correct and secure behavior as per the standard, as it prevents the establishment of a security context based on potentially compromised or manipulated messages. Therefore, the UE's response demonstrates adherence to 3GPP security requirements and protects against possible attacks during the authentication phase. 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 was not yet established. Upon receiving this plain authentication request, the UE responded with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, the UE is required to reject authentication requests that do not conform to 5G security requirements, especially if the message is not protected and the context is not valid for 5G authentication. The UE's action to reject the unprotected authentication request is in line with the 3GPP specifications, as it prevents potential downgrade or replay attacks and ensures that only properly protected authentication procedures are accepted. Therefore, the UE's behavior in this scenario demonstrates adherence to the 5G security standards and is considered secure. 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 and 128-5G-IA2 for integrity protection, with the security header indicating "integrity protected with new security context." Upon receiving this command, the UE responded with a Security Mode Reject message, citing "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after authentication, the Security Mode Command is used to establish NAS security, and the use of 5G-EA0 (null ciphering) means that no encryption will be applied to NAS messages, only integrity protection. The 3GPP standard (TS 33.501) allows the UE to reject a Security Mode Command if it deems the proposed security algorithms insufficient or insecure, especially if ciphering is not enabled (i.e., 5G-EA0 is selected), as this could expose sensitive information. The UE's rejection of the Security Mode Command in this context demonstrates a secure behavior, as it avoids operating with no encryption, which would be a security risk. Therefore, the UE's action aligns with best security practices and the intent of the 3GPP standard to protect user data confidentiality. 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, after the initial NAS procedures, the UE sent an authentication response to the AMF, which then replied with another authentication request in plain (unencrypted) form. The UE subsequently responded again with an authentication response. According to the 3GPP 5G standard, specifically TS 33.501, the 5G-AKA authentication and key agreement procedure must be completed before any NAS messages can be securely encrypted and integrity protected. Until the authentication is successfully completed, messages are exchanged in plain text, which is expected behavior. However, the critical point here is that the UE, after already sending an authentication response, accepted and responded to a subsequent authentication request from the AMF, which was sent in plain text. This is not standard-compliant behavior: once the UE has sent an authentication response, it should not accept or respond to further authentication requests unless the procedure is restarted from the beginning (e.g., after a failure or explicit abort). Accepting and responding to repeated or unexpected authentication requests, especially in plain text, could expose the UE to replay or downgrade attacks, as it may allow an attacker to manipulate the authentication process. Therefore, the UE's action of responding to a second, plain authentication request after already completing its part of the authentication procedure is not secure and does not align with the 3GPP security requirements. 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 and, after completing the initial steps, sent an Authentication Response to the AMF as part of the 5G-AKA procedure. However, before the 5G-AKA authentication and key agreement could be completed (i.e., before security context establishment and NAS message encryption), the AMF sent an Authentication Reject message to the UE in plain (unencrypted) form. The UE, upon receiving this Authentication Reject, did not attempt to continue the registration or authentication process; instead, it immediately sent a Deregistration Request to the AMF, also in plain text, and ceased further communication. According to the 3GPP 5G standard, if the UE receives an Authentication Reject before security is activated, it must not proceed with registration and should not respond to the reject with any sensitive information or attempt to continue the authentication process. The UE's action—terminating the registration attempt and sending a Deregistration Request without exposing any sensitive data—aligns with the security requirements of the standard, as all messages prior to security activation are expected to be in plain text and the UE must not proceed further after an authentication failure. Therefore, the UE's behavior in this scenario is considered secure and compliant with 3GPP specifications. 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 to the AMF, indicating that NAS security (integrity protection and ciphering) was now active. The AMF, under test control, then sent a "deregistration request" message 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, after 5G-AKA and security mode command/complete, all subsequent NAS messages must be integrity protected and ciphered to ensure confidentiality and authenticity. The packet capture confirms that the UE only sent protected messages after security activation, and responded appropriately to a valid, protected deregistration request. There is no evidence of the UE accepting or responding to unprotected or invalid messages, nor of any deviation from the expected secure behavior as per the standard. Therefore, based on the observed actions and adherence to 3GPP security requirements, the UE's behavior in this interaction was 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, 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 now active for subsequent messages. 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, also protected, thereby completing the deregistration process. According to the 3GPP 5G standard, after 5G-AKA and security mode command/complete, all subsequent NAS messages must be integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions—waiting for security activation before accepting and responding to the deregistration request, and ensuring all messages were protected—align with these requirements. There is no indication that the UE accepted or processed any unprotected NAS messages after security activation, nor did it respond to any deregistration request before security was established. Therefore, the UE's behavior in this interaction was secure and compliant with 3GPP standards. 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 the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters negotiated during the initial NAS security setup. However, the AMF then sent a subsequent "security mode command" message, which was protected, specifying the use of ciphering algorithm 128-5G-EA2 and the null integrity algorithm 5G-IA0, 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 there is a valid reason, such as a change in security context or a handover. Additionally, 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 critical security requirement. The UE's decision to reject the security mode command, especially when it requests null integrity protection after security has already been established, aligns with the security principles of the 5G standard, as it prevents potential downgrade attacks or misconfigurations that could compromise the integrity of the communication. Therefore, the UE's action was secure and in accordance with 3GPP security guidelines. 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 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 a new security context. However, the AMF subsequently sent another "security mode command" message, this time protected with the new security context but specifying null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms. Upon receiving this, the UE responded with a "security mode reject" message, indicating that it rejected the security mode command for an unspecified reason. According to the 3GPP 5G standard, after the security context is established, the use of null algorithms (EA0/IA0) is only permitted under very specific 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 downgrade security to null algorithms, as this would expose user data and signaling to potential interception or tampering. The UE's action to reject the security mode command that attempted to set null algorithms, even though the message was integrity protected, aligns with the security requirements of the 5G standard and demonstrates that the UE is enforcing proper security policies to prevent downgrade attacks. Therefore, the UE's behavior 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 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). However, the AMF, under test control, responded with a "security mode command" message after the security mode was already completed, which is not the expected sequence according to the 3GPP 5G NAS protocol. The UE then responded again with a "security mode complete" message. According to the 3GPP standard (TS 24.501), once the security mode procedure is completed and the UE has sent "security mode complete," the AMF should not send another "security mode command" unless a new security context is being established (e.g., due to a context loss or re-authentication). The UE, upon receiving an unexpected "security mode command" after already completing the procedure, should have rejected or ignored the message to prevent potential replay or downgrade attacks. By accepting and responding to a redundant "security mode command," the UE exposes itself to possible security vulnerabilities, as this behavior could be exploited by an attacker to interfere with the security context. Therefore, the UE's action in this scenario does not align with the secure behavior expected by the 3GPP standard. 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 the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the negotiated security algorithms (5G-EA4 for ciphering and 5G-IA0, which is null, for integrity protection). Subsequently, the AMF sent a "security mode command" message, which was protected (ciphered) and used the new security context, as indicated by the security header. The UE then sent a "deregistration request (UE originating)" message. According to the 3GPP 5G standard, after the security mode command is completed and the security context is established, all subsequent NAS messages from the UE should be both ciphered and integrity protected, except in specific cases (such as emergency services or when null algorithms are negotiated). In this test, the integrity algorithm selected was 5G-IA0 (null), meaning that while messages were encrypted, they were not integrity protected. This is generally not recommended, as it leaves the communication vulnerable to certain attacks (e.g., message modification or replay), and the 3GPP standard strongly discourages the use of null integrity protection except for specific, limited scenarios. The UE's acceptance and use of a null integrity algorithm in a normal registration and deregistration context is therefore not secure according to the standard's intent, as it does not provide the required level of protection for NAS signaling. 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 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-EA4 for ciphering and 128-5G-IA3 for integrity protection) and was ready to proceed with protected NAS communication. However, the AMF then sent another "security mode command" message, which was integrity protected and ciphered, as indicated by the security header and the use of the agreed algorithms. The UE did not respond to this subsequent security mode command. According to the 3GPP 5G standard, once the security context is established and the UE has sent "security mode complete," the UE should not expect another security mode command unless there is a valid reason, such as a context re-establishment or a handover. Receiving an unexpected, protected security mode command after already completing the security mode procedure could indicate a protocol anomaly or a potential attack (such as a replay or downgrade attempt). The UE's lack of response in this situation demonstrates adherence to the 3GPP standard, as it avoids engaging in potentially insecure or undefined behavior. By refusing to respond to an unexpected security mode command after security activation, the UE maintains the integrity of the security context and prevents possible exploitation. Therefore, the UE's action in this scenario was secure. Secure
33	33	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 6 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.160211086273193 36 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, 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. Immediately following this, the AMF sent a protected GMM Status message with a 5GMM cause value of 6, which corresponds to "Illegal ME" (Mobile Equipment). Upon receiving this status, the UE responded by sending a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G standard, after security mode is established, all subsequent NAS messages must be integrity protected and, if required, ciphered. The packet capture confirms that the downlink GMM Status message was protected, and the UE's response (Deregistration Request) was sent after receiving an "Illegal ME" cause, which is a valid and expected behavior as per the standard—when the UE is informed that it is considered illegal, it should deregister itself from the network. The UE did not continue with any further registration or service requests, which would have been insecure. Therefore, the UE's actions were in line with 3GPP security requirements, as it only communicated over protected NAS messages after authentication and responded appropriately to the network's status indication. Secure

34	34	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15963101387023926 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15987801551818848 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.360584020614624 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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" message 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 process. According to the 3GPP 5G standard, after the security context is established (post-5G-AKA and security mode complete), all subsequent NAS messages between the UE and AMF must be integrity protected and ciphered to ensure confidentiality and authenticity. The packet capture confirms that the deregistration request from the AMF was protected, and the UE responded appropriately with a deregistration accept message. Since the UE only responded to a properly protected and ciphered deregistration request after security was established, and did not accept or process any unprotected or insecure messages, the UE's actions align with the security requirements of the 5G standard. Therefore, the UE's behavior in this interaction was secure. 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 completed, establishing the necessary security context for protected NAS communication 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 security algorithms and was ready to use the agreed-upon encryption and integrity protection for subsequent NAS messages. The AMF then responded with a "service accept" message, which was sent as a protected (encrypted and integrity-protected) NAS message. According to the 3GPP 5G standard, after the security mode is completed, all subsequent NAS messages must be protected. The UE, upon receiving the protected "service accept" message, did not respond, which is acceptable if no further action is required from the UE for this procedure. There is no indication that the UE sent any unprotected messages after the security context was established, nor did it accept or process any unprotected messages from the AMF post-security mode completion. This behavior aligns with the 3GPP security requirements, as the UE only communicated using protected messages after the security context was in place and did not compromise the security of the NAS communication. Secure

36	36	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5051651000976562 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5054340362548828 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7091829776763916 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 registration process was finalized. Immediately following this, the AMF (under test control) sent a "Deregistration Request (UE terminated)" message to the UE, which was protected with both integrity and ciphering, as indicated by the security header (2). The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, also protected, thereby acknowledging the deregistration request. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF must be integrity protected and ciphered to ensure confidentiality and authenticity. The packet capture confirms that the UE only sent protected messages after security was established, and it correctly processed and responded to the protected deregistration request from the AMF. There is no indication that the UE accepted or responded to any unprotected or suspicious messages after security activation. Therefore, the UE's actions were in line with 3GPP security requirements, maintaining the integrity and confidentiality of the NAS signaling. 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 the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration process was finalized. The AMF then responded with a "Service Accept" message, which was sent as a protected (i.e., integrity protected and/or ciphered) NAS message, confirming that security context was established and NAS security was active. Subsequently, the UE sent a "Deregistration Request (UE originating)" message to the AMF. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected using the established security context. The packet capture shows that the AMF's downlink message was protected, and since the UE sent the deregistration request after security activation, it is expected that this message was also protected, as per the standard. There is no indication in the summary or packet capture that the UE sent any unprotected NAS messages after security was established. Therefore, the UE's actions align with the 3GPP security requirements, and the communication can be considered secure. 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 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 registration process was finalized. Subsequently, the AMF sent a "Security Mode Command" message to the UE, which was protected with integrity using the new security context established during 5G-AKA. The message specified the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm, with the security header indicating "integrity protected with new security context." Notably, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after 5G-AKA, the AMF must initiate NAS security mode control to establish ciphering and integrity protection for subsequent NAS messages. The UE is expected to respond to the Security Mode Command, even if the null ciphering algorithm is selected, to confirm the security context and proceed with secure communication. By not responding, the UE failed to follow the standard protocol, which could leave the session in an undefined or insecure state, as the security context was not confirmed or activated. This lack of response could expose the UE to potential security risks, such as replay or downgrade attacks, since the security context negotiation was not completed. Therefore, the UE's action in this scenario was not secure according to the 3GPP 5G standard. Insecure
39	39	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.2683730125427246 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2686209678649902 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.476357936859131 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 context was established. Following this, the AMF sent a "Configuration Update Command" 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 "Configuration Update Complete" message. According to the 3GPP 5G standard, after establishing a 5G-AKA procedure, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture confirms that the downlink message from the AMF was indeed protected, and the UE responded appropriately within the secure context. Since the UE only sent messages after the security context was established and responded to protected messages as required by the standard, the actions taken by the UE align with 3GPP security requirements. Therefore, the UE's communication in this scenario was 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 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 was established. 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, as required by the 3GPP 5G security standards after authentication. The UE then responded with a "configuration update complete" message, also sent over the protected NAS security context. According to 3GPP TS 33.501, after the 5G-AKA procedure, all subsequent NAS messages between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The actions taken by the UE—responding only after the security context was established and using protected messages—align with these requirements. Therefore, based on the observed behavior 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, indicating that the initial NAS security context establishment was finished. The AMF then sent a "Security Mode Command" message, which was properly protected (integrity protected with a new security context) and specified the use of 128-5G-EA2 for ciphering and 128-5G-IA2 for integrity protection. However, the UE did not respond to this Security Mode Command, which is a deviation from the expected 3GPP 5G standard behavior. According to 3GPP TS 24.501, upon receiving a valid Security Mode Command, the UE must process the command, establish the new security context, and respond with a Security Mode Complete message. The absence of any response from the UE means it did not acknowledge or accept the new security context, which is a security risk because it leaves the NAS signaling unprotected or in an undefined state. This could potentially expose the UE to replay or man-in-the-middle attacks, as the security context is not properly established. Therefore, the UE's action in this scenario is not compliant with the 5G security requirements and 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 the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the NAS security context should now be active and all subsequent NAS messages should be integrity protected and, where required, encrypted. The AMF then sent a protected Deregistration Accept message to the UE, indicating that the message was integrity protected and/or encrypted as per 3GPP standards. The UE, upon receiving this protected Deregistration Accept, did not respond further, which is also compliant with the 3GPP specification, as the Deregistration Accept is a terminal message and does not require an acknowledgment or further action from the UE. The packet capture confirms that the sequence of messages and their protection status align with the expected secure behavior post-5G-AKA. Therefore, based on the observed actions and the 3GPP requirements for NAS message protection after authentication, the UE's behavior in this scenario was 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 sent an Uplink NAS Transport message to the AMF, indicating that the security context was established and subsequent NAS messages should be protected. The AMF then sent a Configuration Update Command to the UE, which was correctly protected with both integrity and ciphering, as indicated by the security header (2). The UE responded with a Deregistration Request (UE originating), which was also sent after the security context was established. 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 ciphered to ensure confidentiality and integrity of the signaling. The packet capture confirms that the downlink message from the AMF was protected, and the UE's actions—sending messages only after security activation and responding appropriately to protected messages—align with the expected secure behavior as per the standard. There is no indication that the UE sent any unprotected or insecure messages after the security context was established. Therefore, based on the observed interaction and adherence to 3GPP security requirements, the UE's actions were secure. 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 proceeded to send uplink NAS messages, including a PDU session establishment request, to the AMF. The AMF, under test control, responded with a series of downlink NAS messages, including a deregistration request (UE terminated), which was sent with integrity protection and ciphering enabled, as indicated by the security header (2). The UE, upon receiving this protected deregistration request, responded appropriately with a deregistration accept message, indicating that it processed the request as per the 3GPP 5G NAS protocol. According to the 3GPP standards, after the security context is established via 5G-AKA, all subsequent NAS messages, especially those related to registration and deregistration, must be integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions—processing only protected messages and responding with the correct protocol message—demonstrate adherence to these security requirements. There is no indication that the UE accepted or acted upon any unprotected or malformed messages, nor did it deviate from the expected protocol behavior. Therefore, based on the observed interaction and compliance with 3GPP security standards, the UE's actions in this scenario were secure. 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, 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 a Configuration Update Command to the UE, which was observed in the packet capture as being integrity protected and ciphered, indicating that NAS security had been activated following 5G-AKA. The UE then responded with a Configuration Update Complete message. According to the 3GPP 5G standard, after the 5G-AKA procedure, all subsequent NAS messages exchanged between the UE and the AMF must be protected by both integrity and ciphering to ensure confidentiality and authenticity. The packet capture confirms that the downlink Configuration Update Command from the AMF was indeed protected, and the UE responded appropriately. Since the UE only sent or responded to messages after security activation, and all its actions adhered to the expected secure communication procedures as per 3GPP standards, 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 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 is now established. The AMF then sent a Configuration Update Command to the UE, and the packet capture shows that this downlink message was both integrity protected and ciphered, as indicated by the security header (2), which aligns with 3GPP 5G security requirements for NAS messages after authentication. The UE responded with a Configuration Update Complete message, also sent as an Uplink NAS Transport, which, given the established security context, would also be protected. The sequence of messages and the use of security headers indicate that the UE correctly enforced NAS security procedures by only sending and accepting protected messages after 5G-AKA completion. This behavior is compliant with the 3GPP 5G standard, which mandates that all NAS signaling after authentication must be integrity protected and ciphered to prevent interception or tampering. Therefore, the actions taken by the UE in this interaction were secure and in accordance with the 5G standard. 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 to the AMF, which then responded with a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating both integrity protection and ciphering (security header type 2). The UE then responded with a Configuration Update Complete message, indicating it processed the command. According to the 3GPP 5G security standards, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions—accepting and responding to a protected Configuration Update Command only after 5G-AKA was completed—align with these requirements. The packet capture confirms that the UE did not process any unprotected or insecure messages after authentication, and its response was appropriate and secure as per the standard. Therefore, the UE's behavior in this interaction was secure. 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 that it was ready for further NAS communication. The AMF, under test control, responded with a Security Mode Command message that was marked as "protected" and specified the use of ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA2, with the security header indicating "integrity protected with new security context." Upon receiving this Security Mode Command, the UE responded with a Security Mode Reject message, citing "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept a valid Security Mode Command if the parameters and context are correct and the message is properly protected. However, if the UE detects any anomaly—such as an unsupported or mismatched algorithm, an invalid security context, or any other inconsistency—it is required by the standard to reject the Security Mode Command to prevent potential security breaches or misconfigurations. Since the UE rejected the Security Mode Command with an unspecified reason, it suggests that the UE detected something abnormal or non-compliant in the message or its context, and thus refused to proceed with potentially insecure communication. This behavior aligns with the security principles of the 3GPP standard, which prioritize the integrity and confidentiality of NAS signaling. Therefore, the UE's action in this scenario was secure, as it prevented the establishment of a potentially insecure security context. Secure

49	49	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 17.321523904800415 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.322353839874268 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Security mode command 17.532354831695557 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm, with the security header set to "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, the use of the null ciphering algorithm (5G-EA0) means that user data would not be encrypted, which is generally only allowed in specific, controlled scenarios (such as emergency services or when explicitly permitted by policy). In normal operation, the UE is expected to reject security mode commands that attempt to establish a security context with no encryption, as this would expose user data to potential interception. The UE's action to reject the security mode command under these circumstances aligns with the security requirements of the 5G standard, as it prevents the establishment of an insecure communication channel. Therefore, the UE's behavior in this test 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 procedure, the UE sent a Service Request message to the AMF, which is a standard step to resume or establish a session. In response, the AMF sent a Deregistration Accept message, encapsulated within a protected Downlink NAS Transport message, indicating that the message was integrity protected and/or encrypted as per 3GPP security requirements post-authentication. The UE, upon receiving this protected Deregistration Accept, did not respond further. According to the 3GPP 5G NAS protocol, after receiving a Deregistration Accept message, especially one that is properly protected, the UE is expected to terminate its NAS signaling and release any related resources, without sending any further NAS messages unless a new registration or service request is initiated. The lack of response from the UE in this context is therefore compliant with the standard and demonstrates that the UE did not process or respond to any unprotected or unexpected messages, nor did it continue communication after being deregistered. This behavior aligns with the security expectations of the 5G standard, as the UE only acted after successful authentication and did not respond to any potentially malicious or out-of-sequence messages. Thus, the UE's actions in this scenario were secure. Secure

51	51	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 25.642455101013184 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 25.642899990081787 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Message type not compatible with the protocol state) 25.85011601448059 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 requesting network services. In response, the AMF sent a deregistration request (UE terminated) to the UE, and this message was integrity protected and ciphered, indicating that NAS security was active and the message was both encrypted and authenticated. The UE then responded with a deregistration accept message, also as expected per the 3GPP protocol. According to 3GPP standards, after 5G-AKA is completed and NAS security is established, the UE must only accept and process protected (integrity protected and ciphered) NAS messages. In this test, the deregistration request from the AMF was properly protected, and the UE responded appropriately by sending a deregistration accept message. There is no indication that the UE accepted or processed any unprotected or invalid messages, nor did it behave in a way that would violate the security requirements of the 5G standard. Therefore, the UE's actions were in line with 3GPP security requirements, as it only processed protected messages after security activation and responded correctly to the deregistration request. 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, which is a standard step for requesting network services. The AMF then responded with a configuration update command, which was sent as a protected NAS message—specifically, it was both integrity protected and ciphered, as indicated by the security header (2). This means the message was encrypted and its integrity was ensured, in line with 3GPP security requirements for NAS signaling after authentication. Following this, the UE sent a deregistration request (UE originating) to the AMF, also as an uplink NAS message. Since the 5G-AKA was completed prior to these exchanges, all subsequent NAS messages, including the service request and deregistration request, would be expected to be protected (integrity protected and ciphered) according to 3GPP TS 33.501. The packet capture does not indicate any deviation from this process, nor does it show the UE sending any unprotected or out-of-spec messages after security was established. Therefore, based on the sequence of events and the security protections in place, the UE's actions were in accordance with the 5G security standards and did not expose any vulnerabilities or insecure behavior. 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) (Integrity protected) 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 to the AMF, indicating that the NAS security context was established and subsequent NAS messages should be protected. In response, the AMF sent a deregistration request (UE terminated) message, which was integrity protected and ciphered, as indicated by the security header (2). The UE then responded with a deregistration accept message, also sent within the protected NAS context. According to the 3GPP 5G standard, once the 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The UE, in this case, correctly followed the standard by only sending and responding to protected messages after the security context was established, and it did not process or respond to any unprotected or insecure messages. Therefore, the UE's actions were in line with the security requirements of the 5G standard, and there is no indication of insecure behavior in its communication during this test. 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 sent a Service Request message to the AMF, which is a standard step to request access to network services. The AMF then responded with a GMM Status message indicating a "Conditional IE error" (5GMM Cause: 100), and this message was sent as a protected (encrypted and integrity-protected) NAS message, as expected after 5G-AKA completion. The UE, upon receiving this protected GMM Status message, did not respond further. According to the 3GPP 5G standards (TS 24.501), when a UE receives a GMM Status message with an unrecognized or unexpected cause value, or if the message indicates an error that the UE cannot recover from, it is permissible for the UE to take no further action and not respond, especially if the message is protected and the integrity is verified. This behavior prevents the UE from engaging in potentially insecure or undefined communication, and avoids leaking information or reacting to possibly malicious or malformed messages. Therefore, the UE's action of not responding to the protected GMM Status message is consistent with secure behavior as outlined by the 3GPP standard. 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 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, the UE should only accept certain NAS messages (such as Authentication Reject) in plain form prior to the completion of 5G-AKA, as encryption and integrity protection are not yet established at this stage. The UE, upon receiving the plain Authentication Reject, did not respond further, which aligns with the expected behavior: the UE should treat this as a failed authentication and abort the registration procedure. This prevents the UE from proceeding with potentially insecure or unauthorized network access. Therefore, the UE's action—no response to a plain Authentication Reject before security context establishment—demonstrates compliance with 3GPP security requirements and does not expose the UE to additional risk in this context. 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 and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should not process or respond to NAS messages that are not integrity protected or encrypted after the security context is established. However, before 5G-AKA is completed, messages are necessarily sent in plain text, and the UE must be able to handle certain messages, such as Authentication Reject, in the clear. The critical security requirement is that the UE must not proceed with registration or provide sensitive information in response to an unauthenticated or unprotected Authentication Reject. In this test, the UE did not respond to the plain Authentication Reject message, which is the correct and secure behavior as per 3GPP standards, since it prevents further interaction that could be exploited by an attacker. The UE's lack of response ensures that it does not act on potentially spoofed or malicious messages before a secure context is established. Therefore, the UE's action in this scenario was secure. 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, the UE should not process or respond to NAS messages that are not integrity protected or encrypted after the security context is established. However, before 5G-AKA is completed, messages are allowed to be sent in plain text, and the UE must be able to handle certain messages, such as Authentication Reject, in plain form. The UE's action—providing no response to the plain Authentication Reject—aligns with the standard, as it prevents further interaction in an unauthenticated and potentially insecure state, thereby mitigating the risk of downgrade or spoofing attacks. This behavior demonstrates that the UE does not proceed with registration or send further messages when authentication fails or is rejected before security is established. Therefore, the UE's action in this scenario is consistent with 3GPP security requirements and is considered 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 before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should not accept or act upon any NAS messages that are not integrity protected and ciphered after the security context is established. However, before the 5G-AKA procedure is completed, messages such as Authentication Reject are allowed to be sent in plain text, as no security context exists yet. The UE, upon receiving the plain Authentication Reject, did not respond further, which is the expected and secure behavior as per the standard: the UE should cease further NAS communication upon receiving an Authentication Reject before security activation. This prevents the UE from being tricked into further actions by a potentially malicious AMF before mutual authentication and key establishment. Therefore, the UE's action in this scenario aligns with 3GPP security requirements and demonstrates secure behavior. Secure

59	59	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002620220184326172 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 (TS 33.501), messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are not protected by NAS security, and the UE must be cautious in processing such messages. Specifically, the standard mandates that the UE should ignore or silently discard any plain (unencrypted) Authentication Reject messages received before security activation, as these could be sent by an attacker to prematurely terminate the registration process or cause denial of service. In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the 3GPP security requirements and demonstrates that the UE is not vulnerable to this type of attack. Therefore, the UE's action was secure. 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. 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, the UE should only accept certain NAS messages in plain text prior to the completion of authentication and security context establishment. The Authentication Reject message is one of the few messages that the UE is permitted to process in plain text before security activation, as it is necessary to inform the UE that authentication has failed or is not possible. In this test, the UE did not respond to the plain Authentication Reject message, which is a secure and compliant behavior, as the UE should not proceed with further communication or registration attempts after receiving such a message in this context. This prevents potential security vulnerabilities such as replay or downgrade attacks. Therefore, the UE's action in this scenario aligns with the 3GPP security requirements and is considered secure. 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 initial registration request to the AMF. The AMF, under test control, responded with a registration reject message using a plain (unencrypted) NAS message, with 5GMM Cause 111 (Protocol error, unspecified). Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that a security context had not been established and thus NAS messages were not yet encrypted or integrity protected. According to the 3GPP 5G standard (TS 24.501), before the completion of 5G-AKA, it is expected and permitted that initial NAS messages, including registration requests and registration rejects, are sent in plain text, as security procedures have not yet been negotiated. The UE, upon receiving the registration reject in plain text before security activation, did not respond further, which is compliant with the standard and prevents unnecessary or insecure communication. Therefore, the UE's actions—sending the initial registration request in plain, accepting the plain registration reject, and not responding further—are in line with 3GPP security requirements for this stage of the NAS procedure. The UE did not expose itself to any additional risk or violate protocol expectations. 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 procedure, the UE initiated a service request to the AMF, which is a standard step for requesting network services. In response, the AMF sent a "deregistration accept" message to the UE, and this message was protected (i.e., integrity protected and/or encrypted), as expected after 5G-AKA completion. However, the UE did not respond to the protected "deregistration accept" message from the AMF. According to the 3GPP 5G standards, after receiving a protected deregistration accept message, the UE is expected to process it and, if required, perform any necessary follow-up actions such as releasing resources or sending a confirmation. The lack of response from the UE could indicate that it did not process the protected message correctly, which may be a deviation from the expected secure behavior. However, since the message was protected and the UE did not respond to an unexpected or potentially malicious deregistration accept, this could also be interpreted as the UE refusing to process an unsolicited or suspicious message, which is a secure behavior. Given that the message was protected and the UE did not take any insecure action (such as accepting an unprotected or unexpected message), the UE's behavior can be considered secure in this context, as it did not compromise its security state or credentials. 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 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, which was protected using the negotiated ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and the security header indicated that the message was integrity protected with a new security context, as per 3GPP standards. Upon receiving the Security Mode Command, the UE did not proceed with the expected Security Mode Complete message, but instead immediately sent a Deregistration Request (UE originating). According to 3GPP TS 24.501, after receiving a Security Mode Command, the UE should respond with a Security Mode Complete message to confirm the activation of the new security context before initiating any further NAS procedures, such as deregistration. By sending a Deregistration Request before completing the security mode procedure, the UE bypassed the confirmation of the new security context, which could potentially expose the deregistration message to security risks, such as being sent without the full protection of the negotiated security algorithms. This behavior does not align with the secure communication flow mandated by the 3GPP standard, as it may allow for vulnerabilities in the NAS signaling. Therefore, the action taken by the UE is considered insecure. Insecure
64	64	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.12326717376709 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.123653173446655 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 provide any response to this protected downlink message from 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 integrity protected and, where required, ciphered to ensure confidentiality and authenticity. The fact that the UE did not respond to a properly protected service accept message from the AMF suggests that the UE either failed to process the protected message or did not recognize it as valid, which is not compliant with the expected secure behavior as per 3GPP standards. This lack of response could indicate a security flaw or a failure in the UE's NAS message handling, as it should be able to process and respond to protected messages after authentication. Therefore, based on the observed behavior, the UE's action 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. However, the AMF, under test control, sent another "security mode command" message to the UE, this time with the security header set to "integrity protected with new security context" and using the agreed cipher and integrity algorithms. Upon receiving this unexpected or potentially invalid security mode command after already completing the security mode procedure, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, once the security mode procedure is successfully completed, the UE should not expect another security mode command unless there is a valid context change or re-authentication event. Receiving a redundant or out-of-sequence security mode command could indicate a protocol error or a potential security attack (such as a replay or downgrade attempt). By rejecting the second security mode command, the UE demonstrated correct and secure behavior, as it did not accept an unexpected change in security context, thereby protecting itself from possible security risks. This response aligns with the 3GPP standard's security principles, which require the UE to maintain the integrity and consistency of the security context. 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 further NAS communication. The AMF, under test control, responded with a Security Mode Command message, which was properly protected (integrity protected with a new security context) and specified the use of 128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection, with ABBA value 0322. Upon receiving this Security Mode Command, 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 a valid Security Mode Command if the message is correctly protected and the algorithms are supported. A Security Mode Reject is only expected if the UE detects an issue such as an unsupported algorithm, an invalid or unprotected message, or a mismatch in the security context. Since the Security Mode Command was sent with proper protection and standard algorithms, and there is no indication of an error in the message itself, the UE's rejection without a specified reason suggests a deviation from expected secure behavior. This could indicate a potential vulnerability or misconfiguration in the UE, as it should not reject a valid, protected Security Mode Command after successful authentication. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. 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 0.8142230510711167 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 1.0217480659484863 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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, under test control, responded with a protected (i.e., encrypted and integrity-protected) GMM Status message containing a 5GMM Cause value of 98. According to 3GPP TS 24.501, a GMM Status message is typically used to indicate protocol errors or abnormal conditions, and the cause value 98 ("Message type not compatible with the protocol state") suggests that the AMF sent a message that was not expected in the current protocol state of the UE. The UE, upon receiving this, responded with its own GMM Status message, echoing the same cause value, which is the correct behavior as per the standard: when a UE receives a message that is not compatible with its protocol state, it should respond with a GMM Status message indicating this incompatibility. The fact that the messages were protected after 5G-AKA further confirms that the UE maintained the required security context. Therefore, the UE's actions were in line with 3GPP security and protocol requirements, correctly handling an unexpected or erroneous message from the network in a secure manner. 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 message with integrity protection, as indicated by the security header. The UE then replied with a Configuration Update Complete message, acknowledging the configuration update, and also sent a Registration Request. According to the 3GPP 5G security standards, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected, and, where required, encrypted. The packet capture shows that the Configuration Update Command from the AMF was integrity protected, and the UE responded appropriately. There is no indication that the UE sent any unprotected or unencrypted NAS messages after the security context was established. Therefore, the UE's actions align with the 3GPP security requirements, as it only sent messages after the security context was in place and responded to protected messages as expected. Based on this analysis, the UE's behavior in this interaction was secure. 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 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 and indicated the use of the 5G-EA0 (null) ciphering algorithm and 128-5G-IA2 for integrity protection. The security header specified 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 security standards, after authentication, the UE and network must agree on both ciphering and integrity algorithms to protect subsequent NAS messages. The selection of 5G-EA0 (null ciphering) means that no encryption would be applied to the NAS messages, leaving them vulnerable to eavesdropping. The 3GPP standard (TS 33.501) allows the UE to reject a Security Mode Command if it deems the proposed security algorithms insufficient or insecure, especially if only null encryption is offered when stronger algorithms are available and supported. The UE's action to reject the Security Mode Command under these circumstances demonstrates adherence to security best practices by refusing to operate without encryption, thereby protecting the confidentiality of its communications. Therefore, the UE's behavior in this scenario is consistent with the 3GPP security requirements and is considered secure. 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 protected (integrity protected and ciphered with a new security context) as per the 3GPP 5G standard. The security algorithms indicated were 5G-EA0 (null ciphering) and 128-5G-IA2 (integrity protection), and the security header showed that the message was both integrity protected and ciphered with the new context. However, the UE did not respond to the Security Mode Command. According to 3GPP standards, after receiving a Security Mode Command that is properly protected and after 5G-AKA is completed, the UE is expected to process the command and respond with a Security Mode Complete message. The lack of response from the UE suggests that it either rejected the security context or failed to process the message, which could be due to the use of the null ciphering algorithm (5G-EA0) or other security policy reasons. From a security perspective, if the UE refused to proceed because the ciphering algorithm was set to null (thus not providing confidentiality), this behavior aligns with secure practices, as it avoids operating in an insecure state. Therefore, the UE's action of not responding can be considered secure, as it did not accept a potentially insecure security context. 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 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 registration and session establishment. The AMF then responded with a Security Mode Command, which was protected using the negotiated ciphering algorithm (128-5G-EA3) and a null integrity algorithm (5G-IA0), and the security header indicated that the message was both integrity protected and ciphered. However, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after 5G-AKA, the Security Mode Command is used to activate NAS security, and the UE is required to respond with a Security Mode Complete message if it accepts the proposed security algorithms. The use of a null integrity algorithm (5G-IA0) is generally not recommended for normal operation, as it means that the integrity of NAS messages is not protected, which could expose the communication to certain attacks. The UE's lack of response to the Security Mode Command in this context can be interpreted as a security-conscious action, as it may be refusing to proceed with a configuration that does not provide integrity protection, which aligns with best security practices and the intent of the 3GPP standard to ensure both confidentiality and integrity. Therefore, the UE's action of not responding to the Security Mode Command when only ciphering and no integrity protection was offered is considered secure behavior. Secure

72	72	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 6.590965032577515 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.591464042663574 AMF to UE SACK (Ack=25, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.5918920040130615 AMF to UE DownlinkNASTransport, Security mode command 6.7950029373168945 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message, and the AMF responded with a Security Mode Command message that was integrity protected and indicated the use of ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA2, with the security header set to "integrity protected with new security context." The UE then responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard (TS 24.501), the Security Mode Command is used to establish NAS security, and the UE is expected to accept the command if the parameters are valid and supported. A Security Mode Reject is only expected if the UE cannot support the proposed algorithms or has other issues with the security context. Since the Security Mode Command was sent after 5G-AKA completion and was properly protected, the UE's rejection without a specific cause ("unspecified") suggests that it did not provide a clear, standards-based reason for rejecting the security context. This behavior could be considered insecure, as it may indicate that the UE is not properly handling the security mode negotiation or is failing to provide diagnostic information necessary for secure operation and troubleshooting. In a secure implementation, the UE should only reject the Security Mode Command for well-defined reasons and should specify the cause, as per 3GPP requirements, to avoid ambiguity and potential security loopholes. Insecure

73	73	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1599750518798828 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602010726928711 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3605461120605469 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 a new security context. However, the AMF subsequently sent another "security mode command" message, this time protected with integrity but specifying the use of the null ciphering algorithm (5G-EA0), which means no encryption would be applied to subsequent NAS messages, while integrity protection was still enabled (128-5G-IA2). Upon receiving this command, the UE responded with a "security mode reject" message, indicating that it rejected the security mode command for an unspecified reason. According to the 3GPP 5G security standards, after the security context is established, the use of the null ciphering algorithm (5G-EA0) is only permitted in very specific scenarios (such as emergency services or when explicitly allowed by policy), and generally, the UE is expected to reject any attempt to downgrade security by disabling encryption unless it is justified. The UE's rejection of the security mode command that attempted to set the ciphering algorithm to null, despite integrity protection, demonstrates that the UE is adhering to the security requirements by not accepting a lower level of protection than what was negotiated and expected after authentication. This behavior prevents potential downgrade attacks and ensures the confidentiality of NAS signaling. Therefore, the UE's action in this scenario is consistent with the 3GPP 5G security standards and is considered secure. 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, which then responded with a Security Mode Command message. This Security Mode Command was sent as a protected message, specifying the use of ciphering algorithm 128-5G-EA3 and integrity algorithm 128-5G-IA2, with the security header indicating "integrity protected with new security context." Upon receiving this, the UE replied with a Security Mode Reject message, citing "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept the Security Mode Command if the parameters (algorithms, ABBA, etc.) are valid and the message is properly protected. However, if the UE detects any inconsistency, unsupported algorithms, or issues with the security context, it is permitted—and in fact required—to reject the Security Mode Command to prevent the establishment of an insecure or compromised security context. Since the Security Mode Command was integrity protected and the algorithms specified are standard, the UE's rejection (with an unspecified cause) suggests it detected something abnormal or unsupported, which is a secure behavior as per the standard: the UE should not proceed with security establishment if it cannot guarantee the integrity and confidentiality of subsequent communications. Therefore, the UE's action in rejecting the Security Mode Command, rather than accepting potentially insecure parameters, aligns with secure behavior as defined by 3GPP. 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, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Security Mode Command message. The Security Mode Command was sent as a protected message, using the cipher algorithm 5G-EA5 and integrity algorithm 128-5G-IA1, with the security header indicating "Integrity protected with new security context (3)." According to the 3GPP 5G standard, after 5G-AKA is completed, the AMF initiates the Security Mode Command 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 to the Security Mode Command. This lack of response is not compliant with the 3GPP standard, as the UE is required to acknowledge and activate the security context for secure NAS communication. The absence of a response could indicate a failure in the UE's security handling or an inability to process the protected message, which could leave the communication channel vulnerable or incomplete. Therefore, based on the 3GPP standard and the observed behavior, the UE's action in this scenario is considered insecure. 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 UE completed the initial NAS procedures and sent an authentication response to the AMF, the AMF responded with an identity request for the SUCI (Subscription Concealed Identifier). Importantly, this identity request was sent in plain (unencrypted) NAS, as the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security context was not established. According to the 3GPP 5G standard (TS 24.501), the SUCI is a privacy-protected identifier that should only be sent by the UE in response to an identity request if the request is protected by NAS security (i.e., after 5G-AKA is completed and NAS encryption is active). Since the AMF requested the SUCI in plain NAS before security activation, the UE correctly did not respond, thereby protecting the subscriber's privacy and adhering to the 3GPP security requirements. This behavior demonstrates that the UE is following the standard and is not exposing sensitive information over an unprotected channel. Therefore, the UE's action in this scenario was secure. 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 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 were sent in plain (unencrypted) form. According to the 3GPP 5G security standard, it is expected and required that the initial NAS messages, including the identity request and response, may be sent unencrypted 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 subscriber's identity even when sent over an unprotected channel. Therefore, the UE's action of providing 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. The UE did not send the SUPI or any other sensitive identifier in the clear, and the use of SUCI ensures privacy. Based on this analysis, the UE's behavior in this scenario was secure and in line with 3GPP requirements. 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 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 a new security context. However, the AMF then sent another "security mode command" message, this time protected with integrity but specifying the use of the null ciphering algorithm (5G-EA0) and a valid integrity algorithm (128-5G-IA2). The UE responded by rejecting this security mode command with a "security mode reject" message, citing an unspecified reason. According to the 3GPP 5G standard, after the security context is established and the security mode is completed, the UE expects all subsequent NAS messages to be protected using the agreed-upon security algorithms. If the network attempts to downgrade security (e.g., by requesting the use of the null ciphering algorithm after security has been established), the UE is expected to reject such requests to prevent potential security vulnerabilities such as ciphering algorithm downgrade attacks. The UE's action to reject the security mode command that attempted to use the null ciphering algorithm, even though the message was integrity protected, aligns with the security requirements of the 5G standard and demonstrates proper security behavior by not accepting a lower level of protection after security establishment. Therefore, the UE's response was secure and in accordance with 3GPP specifications. 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 to the UE, specifying the use of the 5G-EA0 (null) ciphering algorithm and 128-5G-IA2 for integrity protection, with the security header indicating "integrity protected with new security context." Upon receiving this command, the UE responded with a Security Mode Reject message, citing "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after authentication, the AMF should select appropriate ciphering and integrity algorithms to protect NAS signaling. The use of 5G-EA0 (null ciphering) means that no encryption would be applied to the NAS messages, which is generally only allowed in exceptional cases (e.g., for emergency services or if the UE does not support any other ciphering algorithm). In normal operation, the UE is expected to reject a Security Mode Command that requests null encryption when it supports stronger algorithms, as accepting null ciphering would expose NAS messages to potential eavesdropping and compromise user privacy. Therefore, the UE's action to reject the Security Mode Command under these circumstances aligns with the security requirements of the 3GPP standard and demonstrates secure behavior by refusing to operate without encryption when it is not appropriate. 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 to resume or establish a session. The AMF, under test control, responded with a Configuration Update Command, which was sent as a protected message with integrity protection and a new security context, indicating that NAS security procedures were properly established. Upon receiving this message, the UE replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to 3GPP standards, the UE is required to check the validity and compatibility of received NAS messages with its current protocol state. If the UE receives a message that is not compatible with its current state, it should respond with a 5GMM Status message, as was observed in this test. This behavior demonstrates that the UE is correctly enforcing protocol state checks and is not processing potentially invalid or malicious messages, which is a critical aspect of secure NAS communication. The UE's actions align with the security and protocol requirements defined by 3GPP, as it did not accept or process an unexpected or out-of-sequence message, and instead reported the protocol error as specified. Therefore, the UE's response in this scenario was secure. Secure

81	81	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 2222 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.1596660614013672 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1599440574645996 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 as a protected message, but the selected ciphering and integrity algorithms were both set to null (5G-EA0 and 5G-IA0), meaning that neither encryption nor integrity protection was actually applied to subsequent NAS messages. The security header indicated "integrity protected," but with the null algorithm, this protection is effectively absent. According to the 3GPP 5G standard, after authentication, the UE is expected to only accept Security Mode Commands that require at least integrity protection with a non-null algorithm, and ideally, ciphering should also be enabled unless there is a specific reason (such as emergency services) to use null algorithms. The UE, in this case, did not respond to the Security Mode Command, which is the correct and secure behavior as per the standard, since accepting null algorithms would expose the communication to potential interception and tampering. By refusing to proceed with insecure security settings, the UE demonstrated compliance with 3GPP security requirements. 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, the use of a null integrity algorithm (5G-IA0) is generally not recommended for user plane or NAS signaling protection, as it leaves the communication vulnerable to integrity attacks. The UE, by rejecting the security mode command that proposed a null integrity algorithm, is acting in accordance with best security practices and the intent of the standard, which expects UEs to reject insecure security configurations. Therefore, the UE's action in this scenario is secure, as it refused to proceed with a security context that would have left its communications unprotected against integrity threats. 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 5G-AKA authentication, 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. However, the UE did not provide any response to this protected downlink message from 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 integrity protected and, where required, ciphered to ensure confidentiality and authenticity. The UE is expected to process protected messages from the AMF and respond appropriately. 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 the 3GPP security requirements. This behavior could expose the UE to potential denial of service or downgrade attacks if it does not handle protected messages as specified. Therefore, based on the observed interaction and the 3GPP standard, the action taken by the UE is considered insecure. 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, the 5G standalone User Equipment (UE) completed the 5G-AKA authentication procedure and sent an authentication response to the Access and Mobility Management Function (AMF). Following this, the AMF sent a Security Mode Command to the UE, which was protected using the negotiated ciphering (128-5G-EA2) and integrity (128-5G-IA2) algorithms, and included a security header indicating "Integrity protected with new security context." Upon receiving this command, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after successful authentication, the UE is expected to accept the Security Mode Command if the parameters (algorithms, ABBA, etc.) are valid and supported. A Security Mode Reject is only expected if the UE detects an issue such as an unsupported algorithm, an invalid or unexpected security context, or a protocol error. In this test, the Security Mode Command was sent with standard parameters and proper protection, and the UE did not specify a clear reason for rejection. The use of "unspecified" as the cause, without a clear protocol or security justification, suggests that the UE did not follow the expected secure behavior as outlined by 3GPP, where it should only reject for specific, valid reasons. Therefore, the action taken by the UE in this scenario is considered insecure, as it could indicate a vulnerability or misconfiguration that prevents the establishment of a secure NAS security context. 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 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, this time protected, but specifying the use of 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, indicating that it refused to accept the proposed security configuration. According to the 3GPP 5G standard, the use of null algorithms is only permitted under very specific circumstances (such as emergency services or when explicitly allowed by the UE's security policy), and UEs are expected to reject security mode commands that attempt to downgrade security without valid justification. The UE's action to reject the security mode command with null algorithms, especially after a secure context had already been established, demonstrates adherence to the standard and a secure behavior, as it prevents potential security downgrades or attacks. Therefore, the UE's response was appropriate and secure according to 3GPP specifications. 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 begin protected NAS communication. However, the AMF, under test control, responded with another "security mode command" message, which is not the expected behavior according to the 3GPP 5G standard. Normally, after the UE sends "security mode complete," the security context is established, and all subsequent NAS messages should be protected (integrity protected and ciphered) using the agreed algorithms. The UE, upon receiving a second "security mode command," responded again with a "security mode complete" message. According to 3GPP TS 24.501, the UE should not accept a new security mode command after security has already been activated, unless there is a valid reason (such as a security context re-establishment or a handover). The UE's acceptance and response to a repeated security mode command, without any context change, indicates that it did not properly enforce the expected security state machine and allowed a potentially malicious or erroneous re-negotiation of security parameters. This behavior could be exploited to downgrade or disrupt the security context, which is a violation of the 5G security requirements. Therefore, the UE's action in this scenario was not secure according to the 3GPP standard. Insecure

87	87	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7935822010040283 UE to AMF UplinkNASTransport, Service request 0.793781042098999 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.9976592063903809 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information), InitialUEMessage, Service request, Service request, RRCEstablishmentCause=mo-Data] 0.9985220432281494 AMF to UE DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes security context for NAS message protection), the UE sent a Service Request to the AMF. In response, the AMF sent a Deregistration Request message, which was integrity protected and ciphered, indicating that the NAS security context was active and messages were encrypted as per 3GPP requirements. Upon receiving the Deregistration Request, the UE responded 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 correct and secure behavior as per 3GPP TS 24.501, which specifies that the UE should send a 5GMM Status message if it receives a NAS message with invalid or missing mandatory information, especially when the message is protected. The UE did not process the deregistration or take any insecure action; instead, it reported the protocol error as required. Therefore, the UE's actions adhered to the 3GPP security standards, maintaining the integrity and confidentiality of the communication and properly handling protocol errors. 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 UE sent an authentication response to the AMF, the AMF issued an identity request for the SUCI (Subscription Concealed Identifier), which the UE responded to with an identity response. Notably, the AMF sent the identity request as a plain (unencrypted) message, and 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, specifically TS 24.501, the UE is permitted to respond to identity requests sent in plain NAS messages prior to the completion of 5G-AKA, as this is necessary for the network to obtain the SUCI and proceed with authentication. The SUCI itself is a privacy-preserving identifier, designed to protect the subscriber's permanent identity (SUPI) even when sent in the clear. Therefore, the UE's action of responding to a plain identity request with a SUCI before NAS security is established is compliant with the 3GPP standard and does not expose sensitive information. Based on this, the UE's behavior in this interaction is considered 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, after the initial NAS procedures, the UE sent an authentication response to the AMF, but the 5G-AKA authentication procedure was not yet completed. The AMF then sent an identity request for the SUCI (Subscription Concealed Identifier) to the UE in plain (unencrypted) NAS, and the UE responded with an identity response. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should only send sensitive identifiers such as the SUCI or SUPI in cleartext before the NAS security context is established, which occurs after successful completion of 5G-AKA. The SUCI is designed to be a privacy-preserving, encrypted form of the SUPI, and it is acceptable for the UE to send the SUCI in response to a plain identity request before security activation, as the SUCI itself does not reveal the SUPI directly. Therefore, the UE's action of providing 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. The UE did not send the SUPI or any other sensitive identifier in cleartext, and thus its behavior is considered secure in this context. 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 the 5G-AKA authentication procedure was not yet completed. The AMF then sent an identity request for the SUCI (Subscription Concealed Identifier) to the UE in plain (unencrypted) NAS, and the UE responded with an identity response. According to the 3GPP 5G security standard, NAS messages are only protected (encrypted and integrity protected) after the successful completion of the 5G-AKA procedure, which establishes the security context. Before this, messages—including identity requests and responses—are sent in plain text. However, the SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) even when sent over an unprotected channel, as it is a concealed, privacy-preserving identifier. Therefore, the UE's action of sending the SUCI in response to a plain identity request before security activation is compliant with the 3GPP standard and does not expose sensitive information. Based on this, 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, the UE initiated a Service Request to the AMF, which is a standard procedure to request network services. In response, the AMF sent a Deregistration Request (UE terminated) message, which was integrity protected and ciphered, indicating that NAS security was active and the message was both encrypted and authenticated. Upon receiving this protected deregistration request, the UE responded with a 5GMM Status message indicating "Invalid mandatory information." According to 3GPP standards (TS 24.501), when a UE receives a NAS message with invalid or missing mandatory information, it is expected to respond with a 5GMM Status message, and this response should also be protected if security is active. The packet capture confirms that the UE's response was sent after security activation, and the content of the response aligns with the expected behavior as per the standard. Therefore, the UE's actions—responding with a protected status message upon detecting an error in a protected NAS message—demonstrate adherence to 3GPP security requirements and proper error handling. 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 and key agreement procedure, the UE initiated a Service Request to the AMF, which is a standard step to request access to network services. 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 requirements. The UE then responded with a Deregistration Accept message, also sent under NAS security protection. Throughout this exchange, the UE only sent messages after the security context was established (post-5G-AKA), and all subsequent NAS messages were protected, ensuring confidentiality and integrity. According to the 3GPP 5G security standards, this behavior is correct: the UE did not send any unprotected NAS messages after security activation, and it properly responded to a valid, protected deregistration request. Therefore, the UE's actions adhered to the expected security procedures and did not expose itself to any known vulnerabilities in this context. 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 its acceptance of the previously negotiated security parameters. However, the AMF then sent another "security mode command" message, this time protected and 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 reject security mode commands that attempt to establish a security context with algorithms or parameters that do not match its declared capabilities, especially if the integrity protection is set to null (5G-IA0), which is generally not permitted for user plane or NAS signaling except in very specific, controlled scenarios. The UE's action to reject the security mode command in this context is a secure and standards-compliant response, as it prevents the establishment of a potentially insecure security context that could expose the UE to attacks or eavesdropping. The UE correctly identified the mismatch and refused to proceed, thereby upholding the security requirements of the 5G system. 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 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 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 standard, it is expected and required that the UE provides the SUCI (and not the cleartext SUPI) in response to an identity request before NAS security is activated. 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 of providing the SUCI in plain text prior to 5G-AKA completion is compliant 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, thus maintaining the intended level of security and privacy as per the standard. 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: Deregistration Request (UE terminated)) 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 UplinkNASTransport message. In response, the AMF sent a Deregistration Request (UE terminated) as a DownlinkNASTransport message, which was integrity protected and ciphered, indicating that NAS security was active. The UE then responded with a Deregistration Accept (UE terminated), also as an UplinkNASTransport message. According to 3GPP 5G standards, after security activation, all subsequent NAS messages must be protected, and the UE must process and respond to valid, protected messages from the network. Although the Deregistration Request was received in this protocol state (as indicated by "Message type not compatible with the protocol state"), the UE still processed the protected message and responded appropriately with a Deregistration Accept, as required by the standard. The UE did not process or respond to any unprotected or invalid messages, and all communication after 5G-AKA was encrypted and integrity protected. Therefore, the UE's actions adhered to the security requirements of the 5G standard, as it only accepted and responded to protected messages and did not exhibit any insecure behavior in this context. 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 UE completed the initial NAS steps and sent an identity response to the AMF. The AMF, under test control, then sent another identity request to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), and this message was sent in plain (unencrypted) form because the 5G-AKA authentication procedure had not yet been completed. The UE responded to this request by sending another identity response, again in plain text, as encryption is not yet established prior to the completion of 5G-AKA. According to the 3GPP 5G standard, it is expected and required that the UE respond to identity requests from the AMF even before security (ciphering and integrity protection) is activated, as the network needs to identify the subscriber before authentication and key agreement can be performed. The use of SUCI, which is a privacy-preserving, encrypted version of the SUPI (permanent identifier), is specifically designed to protect the subscriber's identity even when sent in the clear before security activation. Therefore, the UE's action of responding with the SUCI in plain text prior to 5G-AKA completion is compliant with the 3GPP standard and does not expose the permanent identity. Based on this, the UE's behavior in this interaction is secure according to the 5G standard. 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 this test scenario, the UE completed the initial NAS steps and sent an identity response to the AMF, which then issued another identity request for the SUCI (Subscription Concealed Identifier). The UE responded with another identity response, all before the 5G-AKA authentication procedure was completed. According to the 3GPP 5G security standard, sensitive information such as the SUCI is designed to protect the subscriber's permanent identifier (SUPI) and should be sent in a way that prevents exposure, even if the NAS security context is not yet established. The SUCI itself is a privacy-preserving identifier, encrypted with the home network's public key, and is specifically intended to be sent in the clear before NAS security is activated, as it does not reveal the SUPI directly. Therefore, the UE's action of responding to the identity request with a SUCI in plain NAS, prior to the completion of 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, and the use of SUCI in this context is secure by design. Thus, the UE's behavior in this interaction is considered secure. 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 a standard procedure to initiate communication. The AMF then responded with a Configuration Update Command, which was sent as a protected message with integrity protection and a new security context, indicating that the NAS security context was active and the message was properly secured according to 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 and compatibility of received NAS messages with its current protocol state. If the UE receives a message that is not compatible with its current state, it should respond with a 5GMM Status message, as was observed in this test. This behavior demonstrates that the UE correctly validated the message and did not process an unexpected or potentially malicious command, thereby adhering to the security requirements of the 5G standard. The UE's actions ensured that only valid and expected messages are processed, which is a critical aspect of maintaining protocol security and integrity. Therefore, the UE's response was secure and compliant with 3GPP specifications. 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 5G-AKA authentication, the UE sent an Uplink NAS Transport message (specifically, a 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" (i.e., integrity protected and/or ciphered as per 3GPP standards). However, after receiving this protected Service Accept message, the UE did not provide any response. According to the 3GPP 5G NAS protocol (TS 24.501), once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered. The UE is expected to process protected messages and respond appropriately, such as acknowledging the Service Accept or proceeding with the next protocol step. The lack of response from the UE after receiving a properly protected Service Accept message indicates that the UE did not handle the message as specified by the standard. This could be due to a failure to process protected messages, a failure to recognize the message type, or another implementation issue. Since the UE did not continue the protocol as required, this behavior is not compliant with the 3GPP security requirements and could expose the UE to potential security or interoperability issues. Insecure
100	100	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 92 UE provided: No response The packet capture during the test using wireshark is: 0.4685640335083008 UE to AMF UplinkNASTransport, Registration complete 0.4687800407409668 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Insufficient user-plane resources for the PDU session) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). The AMF then sent a "GMM Status" message with a 5GMM cause value of 92 ("Insufficient user-plane resources for the PDU session"), and this message was sent as a protected (encrypted and integrity-protected) NAS message. The UE, upon receiving this protected status message, did not respond. According to the 3GPP 5G standards (TS 24.501), after the completion of 5G-AKA and the establishment of NAS security, the UE is required to process protected NAS messages and is not required to respond to a GMM Status message unless it is necessary for further procedures. The lack of response from the UE is compliant with the standard, as the GMM Status message is informational and does not require an acknowledgment or further action from the UE. Furthermore, the UE only sent and received protected messages after security activation, which is in line with 5G security requirements. Therefore, the UE's actions in this scenario were secure and compliant with the 3GPP 5G standard. 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) NAS message, indicating that the AMF was enforcing the negotiated security context (Cipher Algorithm: 128-5G-EA3, Integrity Algorithm: 128-5G-IA2) as per 3GPP standards. The Security Mode Command is a critical step, as it instructs the UE to activate the agreed-upon security algorithms for subsequent NAS message protection. However, the UE did not respond to this Security Mode Command. According to 3GPP TS 24.501, upon receiving a Security Mode Command with a new security context, the UE is required to verify the message integrity, activate the specified security algorithms, and respond with a Security Mode Complete message if the command is valid. The absence of any response from the UE indicates a failure to comply with the standard security procedure, which could leave the communication vulnerable or indicate a malfunction in the UE's security handling. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure, as it did not properly acknowledge or activate the required security context after the Security Mode Command. 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 initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the null cipher (5G-EA0) and null integrity (5G-IA0) algorithms, but with the security header indicating "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 Security Mode Command should negotiate and activate non-null ciphering and integrity algorithms to ensure confidentiality and integrity of NAS messages. The use of null algorithms (EA0/IA0) means that messages are not actually encrypted or integrity protected, which is only allowed in very limited scenarios (e.g., for emergency services or specific test cases). The UE correctly identified that the Security Mode Command was invalid due to the use of null algorithms in a context where security should be enforced, and responded with an error status. This behavior aligns with the 3GPP standard, as the UE should reject or flag such insecure security mode commands. Therefore, the UE's action was secure, as it did not accept insecure security parameters and properly reported the issue. 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 followed by the AMF sending a Deregistration Request (UE terminated) message back to the UE. The Deregistration Request from the AMF was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered, as required by the 3GPP 5G security standards after authentication is complete. The UE, upon receiving this protected Deregistration Request, did not respond. According to 3GPP specifications, when a UE receives a protected Deregistration Request from the network, it is expected to process the message and respond appropriately, typically with a Deregistration Accept message. The lack of response from the UE could indicate a failure to process the protected message or a non-compliance with the expected behavior as per the standard. This absence of response could be considered insecure, as it may leave the UE in an undefined state and could potentially be exploited in certain scenarios. Therefore, based on the 3GPP standard and the observed behavior, the UE's action in this interaction is considered 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 procedure, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Deregistration Request (UE terminated) message back to the UE. The Deregistration Request from the AMF was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered, as required by the 3GPP 5G security standards after authentication is complete. The UE, upon receiving this protected deregistration request, did not respond. According to the 3GPP specifications, when a UE receives a valid, integrity protected, and ciphered Deregistration Request from the AMF, it is expected to process the request and deregister itself, typically sending a Deregistration Accept message in response. However, the UE in this test did not respond at all. From a security perspective, the UE did not process or respond to a properly protected network-initiated deregistration request, which could be interpreted as a failure to comply with the expected secure behavior defined by the standard. This lack of response could potentially leave the UE in an inconsistent state and may expose it to security or operational risks, such as remaining registered when it should not be. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered 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 5G-AKA authentication, the UE initiated an Uplink NAS Transport message, which was followed by the AMF sending a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating both integrity protection and ciphering (security header type 2). The UE then responded with a Configuration Update Complete message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The UE's actions—sending the initial message after authentication, receiving a protected configuration update command, and responding appropriately—demonstrate adherence to the security procedures mandated by the standard. The fact that the UE accepted and responded to a protected message, and that all communication post-authentication was secured, indicates that the UE's behavior was 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 ciphering (5G-EA4) and integrity (128-5G-IA3) algorithms, and indicated a new security context in the security header. Upon receiving this command, 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 in the Security Mode Command are among those it supports and has previously indicated in its security capabilities. If there is a mismatch—meaning the network requests algorithms the UE does not support—the UE must reject the security mode command to prevent the establishment of an insecure or unsupported security context. This behavior is explicitly defined in the standard to protect the UE from being forced into using weak or unsupported security algorithms, which could compromise the confidentiality or integrity of its communications. Therefore, the UE's action to reject the security mode command due to a capabilities mismatch is in strict compliance with the 3GPP security requirements and demonstrates secure behavior in this 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 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. The AMF then sent a "Deregistration Request (UE terminated)" message, which was integrity protected and ciphered, as indicated by the security header (2), meaning both confidentiality and integrity protection were applied according to 3GPP TS 24.501 and TS 33.501. The UE responded with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to the 3GPP 5G standards, after 5G-AKA is completed, all subsequent NAS messages must be protected using the established security context. The UE's actions—sending and receiving protected messages only after security activation—align with these requirements. There is no indication that the UE accepted or processed any unprotected or improperly protected NAS messages after security was established. Therefore, based on the observed behavior and adherence to the 3GPP security requirements, the UE's actions were secure. 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 the successful completion of 5G-AKA (authentication and key agreement), the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Configuration Update Command. This downlink message from the AMF was integrity protected and used a new security context, as indicated by the security header. 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 standards, after security activation (i.e., after 5G-AKA), all subsequent NAS messages must be integrity protected and, where required, ciphered. The UE's action to reject the Configuration Update Command with a 5GMM Status message is in line with the standard if the message is unexpected or not allowed in the current protocol state. This behavior is a security feature to prevent protocol state confusion or exploitation by malicious actors. The UE did not process or accept the potentially invalid or out-of-sequence message, but instead reported the incompatibility, which is the correct and secure behavior as per 3GPP TS 24.501. Therefore, the UE's actions demonstrate adherence to the 5G security requirements 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 authentication (which establishes security context for NAS message protection), the UE sent an Uplink NAS Transport message to the AMF, likely as part of a PDU session establishment request. The AMF, under test control, responded with a protected GMM Status message containing a 5GMM cause value of 98. According to 3GPP TS 24.501, cause 98 indicates "Message type not compatible with the protocol state," which is typically used by the UE to indicate receipt of an unexpected or invalid message for its current state. The UE, upon receiving this protected GMM Status message from the AMF, responded with its own GMM Status message, explicitly stating "Message type not compatible with the protocol state." This behavior aligns with the 3GPP standard, which specifies that the UE should respond with a GMM Status message when it receives a message 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 or act upon the invalid message beyond reporting the protocol error, thereby maintaining the integrity of its state machine and not exposing itself to potential attacks or state confusion. This demonstrates that the UE correctly adhered to the 3GPP security procedures by not accepting or acting on an unexpected message, and by reporting the protocol error in a secure, standards-compliant manner. 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 the 5G-AKA authentication 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). Following this, the AMF 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), after security activation, the UE is required to process only protected NAS messages and should ignore or silently discard any unprotected NAS messages. Furthermore, the standard specifies that upon receiving a "5GMM Status" message with cause 101, the UE is not required to respond, as this message is primarily for diagnostic purposes and does not require an acknowledgment or further action from the UE. In this test, the UE did not respond to the protected "5GMM Status" message, which is compliant with the 3GPP specification and does not expose any security vulnerability. Therefore, the UE's actions were secure and in accordance with the 5G standard. 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 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 integrity protected and indicated the use of ciphering algorithm 5G-EA5 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 reject a security mode command if the proposed security algorithms do not match its capabilities or if the integrity protection algorithm is set to null (5G-IA0) when the UE does not support null integrity or when the network requests ciphering without integrity protection. This is a critical security measure to prevent downgrading attacks or the use of weak/null integrity protection, which could expose the UE to security risks. The UE's action to reject the security mode command under these circumstances demonstrates adherence to the 3GPP security requirements and protects the integrity and confidentiality of its communications. Therefore, the UE's behavior in this interaction 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 ciphering (5G-EA5) and integrity (128-5G-IA2) algorithms, and indicated 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 standard, the UE is required to verify that the security algorithms proposed by the network in the Security Mode Command are among those it supports and has previously indicated during capability exchange. If there is a mismatch—meaning the network requests algorithms the UE does not support—the UE must reject the security mode command to prevent the establishment of an insecure or unsupported security context. This behavior is explicitly defined to protect the UE from being forced into using weak or unsupported security algorithms, which could compromise the confidentiality or integrity of its communications. Therefore, the UE's action to reject the security mode command upon detecting a capabilities mismatch is in strict compliance with 3GPP security requirements and demonstrates secure behavior in the context of the 5G standard. 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 ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and marked as "integrity protected with new security context." Upon receiving this message, the UE responded with a Security Mode Reject, citing an unspecified reason for rejection. According to the 3GPP 5G standard (TS 24.501), the UE is expected to accept the Security Mode Command if the message is valid, properly protected, and the negotiated algorithms are supported. However, the standard also allows the UE to reject the command if it detects any issues, such as unsupported algorithms, invalid security context, or other security concerns. Since the Security Mode Command was sent with the correct security protections and the 5G-AKA was completed, the UE's rejection—especially with an "unspecified" cause—suggests either a misconfiguration, an implementation issue, or a deliberate security policy to reject certain conditions. Without evidence of a protocol violation or exposure of sensitive information, the UE's cautious approach to reject the command does not constitute insecure behavior; rather, it may reflect a conservative security posture. Therefore, based on the information provided and adherence to 3GPP standards, the UE's actions can be considered secure. Secure
114	114	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5208940505981445 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215411186218262 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7234148979187012 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated an Uplink NAS Transport message, which was followed by the AMF sending a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating both integrity protection and ciphering (security header type 2). The UE then responded with a Configuration Update Complete message. According to the 3GPP 5G security 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 align with this requirement: it accepted and processed a protected Configuration Update Command and responded appropriately. There is no indication that the UE accepted or processed any unprotected or improperly protected messages after security activation. Therefore, based on the observed behavior and adherence to the 3GPP security requirements, the UE’s actions in this interaction were secure. 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, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF. The AMF responded with a Security Mode Command, which was sent as a protected message using the negotiated cipher (5G-EA4) and integrity (128-5G-IA3) algorithms, and with the security header indicating "Integrity protected with new security context (3)". This means the AMF expected the UE to process the command under the new security context established after 5G-AKA. However, instead of responding with a Security Mode Complete message (as required by 3GPP TS 24.501, section 7.2.7), the UE replied with a 5GMM Status message indicating "Invalid mandatory information". This suggests that the UE either could not process the Security Mode Command or detected an issue with the message content or its protection. According to the 3GPP standard, the correct and secure behavior for the UE is to verify the integrity and validity of the Security Mode Command and, if it is valid, respond with Security Mode Complete. If the message is invalid or cannot be processed, the UE is permitted to send a 5GMM Status message indicating the error, as a security measure to avoid accepting potentially malicious or malformed commands. Therefore, the UE's action to reject the Security Mode Command and report the error, rather than proceeding with an insecure or incomplete security context, aligns with secure behavior as defined by the standard. 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, which then responded with a Security Mode Command. The Security Mode Command from the AMF was sent as a protected message, indicating that it was integrity protected and ciphered using the negotiated algorithms (128-5G-EA2 for ciphering and 128-5G-IA2 for integrity), and the security header indicated the use of a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after 5G-AKA is completed, the UE is expected to accept the Security Mode Command if the message is valid and protected with the correct security context. However, if the UE detects any anomaly—such as an invalid or unexpected security context, mismatched algorithms, or any integrity/ciphering issues—it is required to reject the Security Mode Command to prevent potential security breaches. Since the Security Mode Reject cause is "unspecified," it suggests the UE detected something abnormal but did not provide a specific reason, which is a conservative and secure approach to avoid proceeding with potentially compromised security parameters. This behavior aligns with the 3GPP security principles, where the UE must not accept security contexts or commands that it cannot fully verify as authentic and correct. Therefore, the UE's action in this scenario is considered secure, as it refused to proceed under uncertain security conditions, thereby protecting itself and the network from possible attacks or misconfigurations. Secure

117	117	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.5606789588928223 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5618300437927246 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 protected using the negotiated security algorithms (ciphering with 5G-EA5 and integrity protection with 128-5G-IA1), and the security header indicated that the message was both integrity protected and ciphered with the new security context established during 5G-AKA. 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 uses the correct security context, the UE is expected to verify the message, apply the indicated security algorithms, and respond with a Security Mode Complete message if everything is valid. The lack of response from the UE means it did not acknowledge or accept the new security context, which is not compliant with the standard and could indicate a security or implementation issue. This behavior is considered insecure because the UE failed to complete the security procedure as required, potentially leaving 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 an Uplink NAS Transport message, which was followed by the AMF sending a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating both integrity protection and ciphering (security header type 2). The UE then responded with a Configuration Update Complete message. According to the 3GPP 5G security standards, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions—sending and receiving protected NAS messages after authentication—align with these requirements. The UE only responded to a properly protected (integrity protected and ciphered) Configuration Update Command, and its own response would also be protected under the established security context. Therefore, based on the observed behavior and adherence to 3GPP security procedures, the UE's actions were secure. 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 5G-EA0 (null) ciphering algorithm, meaning no encryption would be applied to subsequent NAS messages, while integrity protection was set to 128-5G-IA1. The Security Mode Command was sent as a protected message, and the security header indicated that a new security context was being established. Upon receiving this, the UE responded with a Security Mode Reject message, indicating "Security mode rejected, unspecified." According to 3GPP standards (TS 33.501 and TS 24.501), the use of 5G-EA0 (null ciphering) is only permitted under specific, limited circumstances (such as emergency services or when explicitly allowed by the operator policy). In normal operation, the UE is expected to reject security mode commands that attempt to establish a null ciphering algorithm, as this would leave user and signaling data unencrypted and vulnerable to interception. The UE's rejection of the Security Mode Command in this context demonstrates adherence to 3GPP security requirements, as it refused to proceed with insecure ciphering settings. Therefore, the UE's action was secure and in line with the 5G standard. 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 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 was established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). The AMF then sent a "Deregistration Accept" message to the UE, which was correctly protected as per the packet capture. However, the UE did not respond to this protected "Deregistration Accept" message from the AMF. According to the 3GPP 5G standard (TS 24.501), upon receiving a protected "Deregistration Accept" message, the UE is not required to send any further response; the deregistration procedure is considered complete from the UE's perspective. The key security consideration is that all NAS messages after 5G-AKA must be protected, and the UE must not process unprotected messages that require security. In this case, the UE only sent and received protected messages after authentication, and its lack of response to the "Deregistration Accept" is compliant with the standard. Therefore, the UE's actions were secure and in line with 3GPP requirements. Secure

121	121	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 1.719182014465332 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 1.7194299697875977 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Authentication Response to the AMF, but the 5G-AKA authentication procedure was not yet completed. Immediately after, the AMF sent a Service Reject message with 5GMM Cause 111 (Protocol error, unspecified) in plain (unencrypted) NAS, as expected since security context establishment (via 5G-AKA) had not yet occurred. The UE, upon receiving this plain Service Reject message, did not respond further. According to the 3GPP 5G standard, NAS messages are only protected (integrity and ciphering) after successful completion of the authentication and security mode procedures. Before this, messages are exchanged in plain text, and the UE is expected to process certain messages, such as Service Reject, even if they are unprotected, provided that authentication has not been completed. The UE's lack of response to the Service Reject is compliant with the standard, as it indicates the UE did not proceed with any further actions or accept the service in an insecure state. Therefore, the UE's behavior in this scenario aligns with 3GPP security requirements and does not expose itself to additional risk by acting on unauthenticated or unprotected messages before security context establishment. 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 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 Service Reject message, specifically indicating "UE identity cannot be derived by the network" (5GMM Cause 9). Importantly, this Service Reject message was sent in plain (unencrypted) form, which is expected because the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning no security context or encryption keys had been established. According to the 3GPP 5G standard, until the 5G-AKA is successfully completed, NAS messages between the UE and the AMF are permitted to be sent in plain text. The UE, upon receiving the Service Reject, did not respond further, which is also compliant with the standard, as the Service Reject is a terminal message for the registration attempt. The UE did not send any sensitive information after receiving the reject, nor did it attempt to proceed with registration or authentication in an insecure manner. Therefore, the UE's actions were in line with 3GPP security requirements, as it did not expose itself to additional risk and followed the expected protocol behavior. 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, the UE and AMF engaged in a NAS communication sequence where, after the UE sent an identity response, the AMF issued a Security Mode Command with the security header set to "integrity protected with new security context" and specified ciphering and integrity algorithms. However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for protecting NAS messages was not yet established. According to the 3GPP 5G standard, the Security Mode Command should only be sent after successful completion of the authentication procedure (5G-AKA), which establishes the keys required for integrity and ciphering protection. Since the AMF sent a protected Security Mode Command before authentication was complete, the UE correctly rejected the command with a Security Mode Reject message, as it could not securely process the command without an established security context. This behavior aligns with the 3GPP standard, as the UE must not accept security procedures initiated out of sequence or without proper key material. Therefore, the UE's action was secure and compliant with the standard. 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 are engaged in NAS communication prior to the completion of the 5G-AKA authentication procedure. The UE first sends an identity response to the AMF, after which the AMF issues another identity request, specifically requesting the SUCI (Subscription Concealed Identifier). The AMF sends this request in plain (unencrypted) form, as the 5G-AKA procedure—which establishes NAS security and enables encryption—has not yet been completed. The UE responds to this request with another identity response, also in plain text. According to the 3GPP 5G standard, before the completion of 5G-AKA, all NAS messages, including identity requests and responses, are transmitted in plain text because the necessary security context for encryption has not yet been established. The use of SUCI, which is a privacy-preserving, encrypted form of the subscriber identity (SUPI), is specifically designed to protect the subscriber's identity even when sent over an unprotected channel. Therefore, the UE's action of responding with a SUCI in plain text prior to NAS security activation is compliant with the 3GPP standard and does not expose sensitive information. The UE did not send a cleartext SUPI or other sensitive identifiers, and thus its behavior is considered secure within the context of the standard. 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, the initial NAS messages (including registration requests and authentication challenges/rejects) are permitted to be sent in plain text before security context establishment, as encryption and integrity protection are only activated after successful authentication and key agreement. The UE, upon receiving an Authentication Reject message before security context establishment, is expected to silently discard the message and not respond, as a security measure to prevent downgrade or spoofing attacks. In this test, the UE did not respond to the plain Authentication Reject, which aligns with the 3GPP security recommendations and demonstrates correct, secure behavior. Therefore, the UE's action 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) (Undecipher) 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 security setup, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration procedure was finalized. Immediately following this, 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 (2). The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture confirms that the deregistration request from the AMF was protected, and the UE responded as expected by the standard. There is no indication that the UE accepted or processed any unprotected or suspicious messages, nor did it deviate from the expected protocol behavior. Therefore, based on the observed actions and adherence to the 3GPP security requirements, the UE's actions in this scenario were secure. 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 is a standard step before authentication. However, before the 5G-AKA authentication and key agreement procedure was completed, the AMF sent a Deregistration Accept message to the UE in plain (unencrypted) form. The UE did not respond to this message. According to the 3GPP 5G security standards, NAS 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 activated after successful authentication and key agreement. The UE's lack of response to the plain Deregistration Accept message is consistent with the standard, as the UE is not required to respond to a deregistration accept, especially if it did not initiate the deregistration. Furthermore, the UE did not proceed with any further actions that could compromise security, such as sending sensitive information before security activation. Therefore, based on the 3GPP standard and the observed behavior, the UE's actions were secure and compliant with expected procedures. 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 initial NAS procedures, the UE sent an identity response to the AMF, which then replied with an authentication request. Notably, the authentication request from the AMF was sent in plain (unencrypted) form and contained invalid values for the RAND and AUTN fields (all zeros), which are critical for the 5G-AKA authentication procedure. The UE, upon receiving this malformed authentication request, did not proceed with the authentication process but instead responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, the UE is required to validate the integrity and correctness of mandatory fields in received messages, especially before the security context is established (i.e., before 5G-AKA is completed and NAS messages are encrypted). If the UE detects missing or invalid mandatory information, it should not proceed with authentication and should notify the network of the error, which is exactly what occurred here. This behavior prevents the UE from processing potentially malicious or malformed authentication requests, thereby protecting itself from possible security threats or protocol exploits. Therefore, the UE's action aligns with the security requirements of the 5G standard and demonstrates proper protocol compliance. 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. The AMF then issued a Security Mode Command to the UE, specifying the use of the null ciphering algorithm (5G-EA0) 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 security standards, the use of the null ciphering algorithm (5G-EA0) means that user data and NAS signaling would not be encrypted, only integrity protected. Many UEs are designed to reject security mode commands that request null encryption after authentication, as this would expose user data to potential eavesdropping and compromise confidentiality. The UE's decision to reject the security mode command under these circumstances aligns with best security practices and the intent of the 3GPP standard, which expects UEs to protect user data confidentiality unless there is a valid reason not to. Therefore, the UE's action in rejecting the command was secure and appropriate, as it prevented the establishment of an insecure communication channel. 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, the AMF replied with an authentication request message that was sent in plain (unencrypted) form, as the 5G-AKA procedure had not yet been completed and thus no NAS security context was established. The UE, upon receiving this authentication request, responded with an "Authentication failure" message, specifically indicating "Non-5G authentication unacceptable." According to the 3GPP 5G standard, the UE is required to verify that the authentication procedure is appropriate for 5G and that the security context is valid before proceeding. If the authentication request is not compliant with 5G-AKA or is sent in an insecure manner (such as in plain text when it should be protected), the UE should reject the authentication attempt to prevent potential security breaches. In this case, the UE correctly identified that the authentication request was not acceptable for 5G authentication and refused to proceed, thereby protecting itself from a potentially insecure or non-standard authentication process. This behavior aligns with the security requirements of the 5G standard, as it prevents the establishment of a security context based on an insecure or non-5G-compliant authentication procedure. Therefore, the UE's action was secure. 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 encryption and integrity protection of NAS messages are only established after successful completion of the 5G-AKA authentication and key agreement procedure. The UE, upon receiving the registration reject, did not respond further, which is also acceptable with the standard, as the UE is expected to abort the registration attempt upon receiving such a reject cause. Therefore, the UE's actions—sending the initial registration request in plain, accepting the plain registration reject, and not responding further—are all in line with 3GPP security requirements for this stage of the NAS procedure. The UE did not expose itself to any security risk in this interaction, as it did not proceed with any sensitive operations before security context establishment. 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 the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected behavior when the network requests the UE's identity. However, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed at this point, meaning that the NAS security context (encryption and integrity protection) was not yet established. Subsequently, the AMF sent a Service Reject message to the UE in plain (unencrypted) form, with a 5GMM cause code of 99 ("Information element non-existent or not implemented"). The UE did not respond further after receiving this message. According to the 3GPP 5G standard, it is permissible for certain initial NAS messages, such as Identity Request/Response, to be exchanged in plain text before authentication and security activation, as the security context is not yet available. The UE's behavior—sending the Identity Response in plain text before 5G-AKA and not responding to a Service Reject—aligns with the standard and does not expose the UE to additional risk in this context. The UE did not proceed with any further actions that could compromise its security. Therefore, based on the 3GPP standard and the sequence of events, the UE's actions 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 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 crucially, this authentication request was sent in plain (unencrypted) form before the 5G-AKA procedure was completed. The UE, upon receiving this plain authentication request, replied with an authentication failure message, specifically indicating "Non-5G authentication unacceptable." According to the 3GPP 5G security standards, sensitive NAS messages such as authentication requests should only be sent after a secure context is established via the 5G-AKA procedure, ensuring confidentiality and integrity protection. The UE's action to reject the authentication request because it was not protected by 5G security (i.e., sent in plain text before 5G-AKA completion) aligns with the expected secure behavior as defined by the standard. This response prevents potential security vulnerabilities such as interception or replay attacks on unprotected authentication messages. Therefore, the UE's behavior in this scenario demonstrates adherence to 5G security requirements 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 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). The UE, after completing the initial NAS steps, responded to an identity request by sending an Identity Response message to the AMF. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the security context for NAS message encryption and integrity protection was not yet established. Subsequently, the AMF sent a Service Reject message with a 5GMM Cause value of 3 ("Illegal UE") in plain (unencrypted) form, as is permitted by the 3GPP standard prior to the completion of 5G-AKA. The UE did not respond further to the Service Reject. According to 3GPP TS 24.501, before the security context is established (i.e., before 5G-AKA is completed), NAS messages, including Identity Response and Service Reject, are allowed to be sent in plain text. The UE's behavior—sending the Identity Response in plain text before security activation and not responding further to the Service Reject—aligns with the expected and secure operation as defined by the standard. Therefore, the UE's actions in this scenario were secure and compliant with 3GPP requirements. 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, under test control, responded with a Security Mode Command, specifying null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, and marked the message as "integrity protected with new security context." However, the 5G-AKA authentication procedure, which is required to establish a valid security context and derive keys for encryption and integrity protection, had not yet been completed. Upon receiving the Security Mode Command with null algorithms and without a valid security context, the UE responded with a Security Mode Reject, citing an unspecified reason. According to the 3GPP 5G security standards, the UE must not accept security mode commands that attempt to establish null security (EA0/IA0) unless explicitly allowed (e.g., for emergency services), and must also reject any security mode command that is not properly protected or is received before authentication is complete. The UE's rejection of the security mode command in this context demonstrates correct and secure behavior, as it prevents the establishment of an insecure connection and adheres to the 3GPP security requirements. Therefore, the UE's actions in this scenario were 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 message that was integrity protected using a new security context, but specified the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA3 integrity algorithm. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for establishing encryption and integrity protection was not yet in place. According to the 3GPP 5G security standards (TS 33.501), the Security Mode Command should only be accepted by the UE after successful completion of authentication (5G-AKA), and the use of the null ciphering algorithm (EA0) is only permitted under specific, controlled circumstances (e.g., emergency services or regulatory requirements). In this case, the UE correctly rejected the Security Mode Command with an unspecified reason, as accepting it would have resulted in unprotected NAS signaling and a potential security vulnerability. The UE's refusal to proceed with security mode setup before authentication and with null ciphering aligns with 3GPP security requirements, demonstrating secure behavior in the face of a potentially insecure or non-standard request from the network. 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. After the initial NAS steps, the UE sends an Authentication Response to the AMF, which is expected behavior after receiving a valid Authentication Request. However, the AMF, under test control, sends another Authentication Request to the UE, and the UE responds again with an Authentication Response. Notably, the downlink Authentication Request from the AMF is sent in plain (unencrypted) form, which is expected at this stage because the 5G-AKA procedure, which establishes NAS security, has not yet been completed. According to the 3GPP 5G standard, all NAS messages prior to the completion of authentication and security mode command are sent in plain text, and only after successful authentication and security mode setup are messages encrypted and integrity protected. The UE's action—responding to a plain Authentication Request with a plain Authentication Response before security context establishment—is compliant with the standard. There is no indication that the UE sent any protected messages before security was established, nor did it accept protected messages before the security context was in place. Therefore, based on the 3GPP standard and the sequence of events, the UE's actions were secure and in line with expected behavior during the authentication phase. Secure

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 requested 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 and security procedures, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration process was finalized. Immediately following this, the AMF 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, acknowledging the request. According to the 3GPP 5G standards, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and authenticity. The packet capture confirms that the deregistration request from the AMF was indeed protected, and the UE responded as specified by the standard. The UE did not process or respond to any unprotected or unexpected messages, and its actions were in line with the expected secure behavior as per 3GPP TS 24.501 and TS 33.501. Therefore, the UE's actions in this interaction were secure and compliant with the 5G security requirements. 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 registration procedure 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 zeroed authentication parameters (e.g., AUTN: 00000000000000000000000000000000). The UE, upon receiving this malformed authentication request, did not proceed with the 5G-AKA authentication procedure. Instead, it responded with a 5GMM status message indicating "Invalid mandatory information," signaling that the authentication request was not valid or did not meet the expected format as per 3GPP standards. According to the 3GPP 5G security architecture, the UE should not proceed with authentication or provide sensitive information if the authentication request is invalid or incomplete, especially before a secure context is established. By refusing to process the invalid authentication request and instead reporting an error, the UE demonstrated correct and secure behavior, as it did not expose itself to potential security risks or protocol downgrades. This response aligns with the security requirements of the 5G standard, which mandates that the UE must validate the integrity and correctness of authentication messages before proceeding. 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 registration procedure by sending an initial registration request to the AMF. The AMF responded with an authentication request message, which was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. Upon receiving this plain authentication request, the UE did not proceed with the authentication process; instead, it immediately sent a deregistration request (UE originating) back to the AMF. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are allowed to be sent in plain text, as there is no shared key yet for encryption. However, the UE is expected to process the authentication request and attempt to complete the 5G-AKA procedure unless it detects an anomaly or security concern (such as an invalid or suspicious authentication challenge). The UE's action to deregister immediately after receiving a plain authentication request, without attempting authentication, suggests that it either detected something abnormal or was configured to avoid proceeding in the absence of security. This conservative behavior is in line with a secure implementation, as it avoids exposing sensitive information or proceeding with potentially insecure communication. Therefore, the UE's action in this scenario can be considered secure, as it did not proceed with authentication or further communication until a secure context was established. Secure
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 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 authentication response to the AMF, which then replied with an authentication reject message. Notably, the authentication reject was sent as a plain (unencrypted) message, which is expected since the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed—meaning that security context and encryption keys had not been established. According to the 3GPP 5G standard, until the 5G-AKA is successfully completed, NAS messages are transmitted in plain text, and the UE is required to accept and process an authentication reject message even if it is unprotected. The UE, in this case, did not respond further after receiving the authentication reject, which aligns with the standard behavior: upon receiving an authentication reject, the UE should abort the registration and not proceed with further NAS communication. Therefore, the UE's actions were consistent with 3GPP security requirements, as it did not accept any insecurely delivered messages beyond what is permitted prior to authentication, nor did it continue communication after rejection. 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 responded with another authentication request, but crucially, this request was sent in plain (unencrypted) form, and the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should only accept authentication requests that are part of the expected authentication flow and should reject any authentication requests that are not protected by the established security context, especially if they are sent in plain text after the authentication procedure has already started. The UE correctly identified that the authentication request was not in line with 5G security requirements (as it was sent in plain and after an authentication response had already been provided), and responded with an "Authentication failure (Non-5G authentication unacceptable)" message. This behavior demonstrates that the UE is adhering to the 5G security standards by refusing to process potentially insecure or replayed authentication requests that could compromise the security of the communication. Therefore, the UE's action was secure and in compliance with the 3GPP 5G security 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, Registration request (UE originating) 0.5048840045928955 AMF to UE SACK (Ack=7, Arwnd=106334) , 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, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration process was finalized. 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), meaning the message was both encrypted and authenticated according to 3GPP security requirements. The UE, upon receiving this protected deregistration request, did not respond. According to the 3GPP 5G standard, after the security context is established (post-5G-AKA), all NAS messages must be protected, and the UE is expected to process valid, protected messages. However, if the UE receives an unexpected or suspicious message—such as a deregistration request immediately after registration—it is within the UE's security design to ignore or not respond to such messages to prevent potential security breaches or denial-of-service attacks. The lack of response from the UE in this context suggests that it did not blindly accept or process a potentially malicious or out-of-sequence command, thereby adhering to a secure behavior as per 3GPP guidelines. This cautious approach helps protect the UE from unauthorized or unexpected network actions, especially when the message flow does not align with normal procedures. Secure

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 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 registration process was finalized. Following this, the AMF sent a "Configuration Update Command" to the UE, which was protected with both integrity and ciphering, as indicated by the security header (2). The UE then responded with a "Configuration Update Complete" message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected using the established security context, ensuring both integrity and confidentiality. The packet capture confirms that the downlink message from the AMF was indeed protected, and the UE responded appropriately within the secure context. Since the UE only sent messages after the security context was established and responded to protected messages as required by the standard, the actions taken by the UE align with 3GPP security requirements. Therefore, the UE's behavior in this interaction was secure. 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 that it had accepted the security parameters (ciphering and integrity algorithms) negotiated during the security mode command. However, the AMF, under test control, responded with another "security mode command" message, which is not the expected behavior according to the 3GPP 5G standard. The UE, upon receiving this second security mode command, again sent a "security mode complete" message. According to 3GPP TS 24.501, once the security context is established and the UE has responded with "security mode complete," the AMF should not send another security mode command unless the security context is being re-established or updated for a valid reason. The UE, by accepting and responding to a second, unexpected security mode command, is not strictly following the standard, as it should have rejected or ignored the redundant command to prevent potential security downgrades or replay attacks. This behavior could expose the UE to security vulnerabilities, such as repeated security context re-establishment or exploitation by a malicious AMF. Therefore, the UE's action in this scenario is considered insecure according to the 3GPP standard, as it does not properly validate the sequence and legitimacy of security mode commands after the initial security context is established. 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 protected NAS communication 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 proceed with protected NAS signaling. The AMF then sent a "deregistration accept" message, which was transmitted as a protected (i.e., integrity protected and/or ciphered) NAS message. The UE, upon receiving this protected deregistration accept message, did not respond further, which is expected behavior since the deregistration procedure is initiated by the network and the deregistration accept is the final message in this sequence. According to the 3GPP 5G standard, after the security context is established and NAS messages are protected, the UE should not respond to a properly protected deregistration accept message unless further action is required. The UE's actions—completing the security mode procedure, accepting only protected messages, and not responding unnecessarily—align with the security requirements of the 5G standard, ensuring that sensitive signaling is not exposed and that the UE does not process or respond to unprotected or unexpected messages. Therefore, the UE's behavior in this scenario was secure. 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 use the new security context for NAS message protection. The AMF then sent a "configuration update command" to the UE, which was properly 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, indicating "Message type not compatible with the protocol state." This response suggests that the UE detected that the configuration update command was not expected or valid in its current protocol state, and it reported this protocol error as specified in the 3GPP standards (TS 24.501, section 8.2.25). The UE did not process the invalid message further, nor did it accept or act on the configuration update command, but instead reported the error to the AMF. This behavior aligns with the security and robustness requirements of the 5G standard, which expects the UE to reject or report unexpected or out-of-sequence messages, especially after security activation, to prevent protocol misuse or attacks. Therefore, the UE's actions were secure and compliant with 3GPP specifications. Secure

148	148	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.11970210075378418 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.11996603012084961 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Congestion) 0.3268871307373047 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 use integrity protection and ciphering for subsequent NAS messages. The AMF then sent a "deregistration request" message 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, also protected, thereby completing the deregistration process. According to the 3GPP 5G standard, after the security context is established (post-5G-AKA and security mode complete), all subsequent NAS messages must be integrity protected and, where required, ciphered. The UE's actions—accepting the security mode, responding only to protected messages, and sending its own protected messages—are fully compliant with these requirements. There is no indication that the UE accepted or responded to any unprotected or improperly protected messages after security activation. Therefore, the UE's behavior in this interaction was secure and in line with 3GPP standards. 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 had accepted the negotiated security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity protection) and was ready to begin protected NAS communication. However, the AMF, under test control, responded with another "security mode command" message, which is not the expected behavior according to the 3GPP 5G standard. 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 UE, upon receiving a second "security mode command" after already completing the security mode procedure, should recognize this as an abnormal or potentially malicious event (such as a replay or downgrade attack) and, according to 3GPP TS 24.501, should reject the message or ignore it, rather than proceeding as if it were a valid new command. In this test, the UE responded again with "security mode complete," which suggests it accepted the repeated security mode command and did not enforce the expected security checks. This behavior is insecure because it exposes the UE to potential attacks where an adversary could attempt to disrupt or downgrade the security context by injecting additional security mode commands after the procedure should have been completed. Therefore, the UE's action did not conform to the security requirements of the 5G standard. 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 it had accepted the negotiated security algorithms and was ready to communicate securely. The AMF then sent a "deregistration request" message, which was integrity protected and ciphered, as indicated by the security header (2), meaning that both integrity protection and encryption were applied to the message. The UE responded with a "deregistration accept" message, also within the protected NAS security context. According to the 3GPP 5G standards, after the security context is established (post-5G-AKA and security mode complete), all subsequent NAS messages between the UE and AMF must be protected by integrity and, where required, ciphering. The UE's actions—accepting the security mode, responding only after security was established, and sending its deregistration accept message within the protected context—are fully compliant with these requirements. There is no indication that the UE accepted or responded to any unprotected or improperly protected messages after security activation. Therefore, the UE's behavior in this interaction was secure and in line with 3GPP 5G security standards. 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, after the UE initiated a registration request to the AMF, the AMF responded with an identity request for the GUTI (Globally Unique Temporary Identifier). 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 security standards (TS 33.501), the UE should not respond to identity requests for sensitive identifiers (such as the GUTI, SUCI, or SUPI) over unprotected NAS messages, as this could expose the UE to privacy and security risks, such as IMSI catching or tracking attacks. In this case, the UE did not respond to the plain identity request, which aligns with the security recommendations of the 5G standard to protect the user's identity until a secure channel is established. Therefore, the UE's action was secure and compliant with 3GPP security guidelines. 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 a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. At this point, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that security context establishment (i.e., mutual authentication and key derivation for NAS message protection) was not in place. Despite this, the AMF responded with a DownlinkNASTransport message carrying a Configuration Update Command, which was marked as "Protected" with an unknown security header. According to the 3GPP 5G standard (TS 24.501), NAS message protection (integrity and/or ciphering) must not be applied before the security context is established via 5G-AKA. The UE, upon receiving a protected NAS message before security activation, is expected to discard the message and not respond, as processing such messages could expose it to security risks like replay or spoofing attacks. In this test, the UE did not respond to the protected Configuration Update Command, which aligns with the 3GPP security requirements and demonstrates correct, secure behavior by refusing to process or acknowledge a prematurely protected message. 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 InitialUEMessage containing a Registration Request to the AMF. The AMF responded with a Security Mode Command, which was sent as a protected message using the cipher algorithm 128-5G-EA3 and the integrity algorithm 5G-IA0 (null), with the security header indicating "Integrity protected with new security context." However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for encryption and integrity protection was not fully established. Upon receiving the Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information," suggesting that the UE detected an issue with the received message—likely because the AMF attempted to enforce security before the authentication and key agreement (5G-AKA) was completed. According to the 3GPP 5G standard, security procedures such as ciphering and integrity protection should only be applied after successful authentication and key establishment. The UE's action to reject the Security Mode Command and not proceed with unprotected or improperly protected communication aligns with the standard's security requirements, as it prevents the establishment of a potentially insecure session. Therefore, the UE's behavior in this scenario was secure and compliant with 3GPP specifications. 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 initial registration request to the AMF. The AMF, under test control, responded with a configuration update command 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 at this point in the exchange. According to the 3GPP 5G security standards, 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 for encryption and integrity protection. Since the AMF sent a protected message before 5G-AKA was completed, the UE, following the standard, did not respond to this message, as it had not yet established the security context required to process protected NAS messages. This behavior by the UE is correct and secure, as responding to or accepting protected messages before authentication and key agreement would expose the UE to potential security risks, such as replay or man-in-the-middle attacks. Therefore, the UE's lack of response demonstrates adherence to the 3GPP security requirements and proper handling of NAS message protection. 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 a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. At this point, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that security context establishment (including encryption and integrity protection of NAS messages) was not yet in place. The AMF, under test control, responded with a DownlinkNASTransport message carrying a Deregistration Accept, which was sent as a "protected" message (i.e., with NAS security applied). According to the 3GPP 5G standard (TS 24.501), the UE should only process protected NAS messages after a security context has been established via 5G-AKA. If the UE receives a protected NAS message before security activation, it must discard the message and not respond, as it cannot verify the integrity or decrypt the message. In this test, the UE did not respond to the protected Deregistration Accept message sent before security activation, which is the correct and secure behavior as per the standard. This prevents potential security vulnerabilities such as replay or spoofing attacks before mutual authentication and key establishment. 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, the UE initiated a 5G standalone registration by sending an initial 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 a new security context. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that no valid security context or keys had been established between the UE and the network. Upon receiving the Security Mode Command with null algorithms and without a completed authentication, the UE responded with a Security Mode Reject, citing an unspecified reason. According to the 3GPP 5G security standards, the UE is expected to reject security procedures that attempt to establish a security context with null algorithms or before authentication is complete, as this would leave the communication unprotected and vulnerable to attacks. The UE's action to reject the security mode command under these circumstances aligns with the security requirements of the standard, as it prevents the establishment of an insecure connection. Therefore, the UE's behavior in this scenario was secure. Secure
157	157	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006291866302490234 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 deregistration request message 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 NAS message protection (integrity and ciphering) was not yet established between the UE and the network. According to the 3GPP 5G standard, the UE should only accept and process protected NAS messages (i.e., those with integrity protection and ciphering) after the 5G-AKA procedure is successfully completed and the security context is in place. Since the AMF sent a protected deregistration request before security activation, the UE correctly did not respond to this message, as it could not verify its authenticity or decrypt it without the established security context. This behavior aligns with the 3GPP security requirements, as processing protected messages before security context establishment could expose the UE to security risks such as replay or spoofing attacks. Therefore, the UE's action in this scenario was secure. 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, 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 IMEISV, in plain (unencrypted) NAS signaling. 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 protect sensitive information, such as the IMEISV, and should not transmit it in plain text before NAS security is activated. In this test, the UE did not respond to the AMF's plain (unencrypted) request for the IMEISV, which aligns with the security requirements of the standard, as sending the IMEISV in the clear would expose the UE to privacy and security risks. Therefore, the UE's action of withholding the IMEISV until NAS security is established demonstrates compliance with 3GPP security guidelines and is considered secure behavior. 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 test scenario, the UE and AMF engaged in NAS communication where, after the initial 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) was not yet established, and messages were exchanged in plain text. The AMF then sent a GMM Status message with cause 13 ("Roaming not allowed in this tracking area") in plain text, to which the UE did not respond. According to the 3GPP 5G standard (TS 24.501), before the completion of 5G-AKA, it is expected that certain NAS messages, including identity procedures and status messages, may be sent unprotected, as security context is not yet available. The UE's lack of response to the plain GMM Status message is also compliant, as the standard does not require a response to a status message, especially when it is received before security activation. Therefore, the UE's actions—sending the identity response in plain text before security activation and not responding to the status message—are consistent with the 3GPP standard and do not introduce additional security risk in this context. 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 5G standalone User Equipment (UE) completed the initial NAS procedures and sent an Identity Response message 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) was not yet established. The AMF then sent a Configuration Update Command to the UE as a plain (unencrypted and unauthenticated) NAS message, which is not permitted by the 3GPP 5G standard (TS 24.501). According to the standard, the UE must not process or respond to any NAS messages that require security protection (such as Configuration Update Command) if they are received in plain text after the initial registration steps, and before security has been activated. The UE correctly did not respond to the plain Configuration Update Command, thereby preventing a potential security vulnerability where sensitive configuration could be manipulated by an attacker before security is established. This behavior aligns with the 3GPP security requirements, as the UE must ignore such messages until NAS security is in place. Therefore, the UE's action in this scenario was secure. 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, the UE completed the initial NAS procedures and sent an Identity Response message to the AMF, which is a typical step before authentication. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed, the AMF sent a Deregistration Accept message to the UE, and this message was marked as "Protected." According to the 3GPP 5G standard, NAS message protection (integrity and encryption) is only possible after the successful completion of the 5G-AKA procedure, as this is when the necessary security context and keys are established. Since the 5G-AKA was not completed, the UE should not have accepted or processed any protected NAS messages, nor should it have responded to them, as it would not have the required keys to verify or decrypt the message. The UE's action of providing no response to the protected Deregistration Accept message from the AMF is therefore correct and aligns with the 3GPP security requirements, as it avoids processing potentially unauthenticated or malicious messages before security is established. This behavior demonstrates that the UE is adhering to the security principles outlined in the 5G standard. 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 test scenario, the 5G standalone User Equipment (UE) completed the initial NAS procedures and sent an Identity Response message to the Access and Mobility Management Function (AMF). The AMF, under test control, then sent a Service Accept message back to the UE, and this message was marked as "Protected" (i.e., integrity protected and/or encrypted). However, the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed at this point in the exchange. According to the 3GPP 5G security standards, NAS message protection (encryption and integrity protection) can only be applied after successful completion of 5G-AKA, as this procedure establishes the necessary security context and keys for protecting subsequent NAS messages. Since the Service Accept message from the AMF was sent as "Protected" before 5G-AKA was completed, the UE correctly did not respond to this message. This behavior aligns with the 3GPP standard, which requires the UE to ignore or reject protected NAS messages if a security context has not yet been established. Therefore, the UE's action in this scenario 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 UE and AMF engaged in NAS communication where, after the initial steps, the UE sent an Identity Response message to the AMF. Immediately following this, the AMF sent a Deregistration Request message to the UE, which was integrity protected and ciphered (security header type 2). However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for encryption and integrity protection had not been established between the UE and the network. 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 is when the keys for securing NAS messages are derived. Since the AMF sent a protected message before 5G-AKA was completed, the UE, following the standard, did not respond to this message because it could not verify or decrypt it without the security context. This behavior demonstrates that the UE correctly adhered to the 3GPP security requirements by not processing or responding to a protected message before security activation. Therefore, the UE's action was secure. 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, after the UE sent an identity response to the AMF, the AMF responded with a Security Mode Command message that was marked as "protected" and indicated the use of specific ciphering and integrity algorithms, but the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G standard, the Security Mode Command should only be sent after the successful completion of the 5G-AKA authentication, which establishes the necessary security context for protecting NAS messages. Since the 5G-AKA was not completed, the UE had not yet established the required security keys and context to process a protected Security Mode Command. The UE responded by rejecting the Security Mode Command with an unspecified reason, which is the correct and secure behavior as per the standard, because accepting or processing protected messages without a valid security context could expose the UE to security vulnerabilities such as replay or man-in-the-middle attacks. Therefore, the UE's action to reject the Security Mode Command before authentication was completed demonstrates adherence to the 3GPP security requirements and protects the integrity of the communication. Secure
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, 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, the AMF sent a Configuration Update Command to the UE, which was integrity protected but not encrypted, as indicated by the security header and the fact that 5G-AKA was not yet completed. According to the 3GPP 5G standard, NAS message encryption and integrity protection should only be applied after successful completion of the authentication and key agreement (5G-AKA), which establishes the necessary security context. Since the AMF sent a protected message before 5G-AKA completion, the UE correctly did not respond to this message, as it had not yet established the security context required to process protected NAS messages. If the UE had accepted or responded to this prematurely protected message, it would have violated the 3GPP security procedures and potentially exposed itself to security risks. Therefore, the UE's action of not responding was in line with the 5G standard and demonstrated secure behavior. 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 crucially, this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should only be transmitted after the establishment of NAS security, which is achieved by completing the 5G-AKA authentication and key agreement procedure. Since the AMF sent the identity request before security was activated, the UE was correct in not responding to this request, as sending the IMEISV in plain text would expose sensitive device information to potential interception. The UE's refusal to respond in this situation demonstrates adherence to 3GPP security guidelines, as it avoids leaking sensitive information before a secure channel is established. Therefore, the UE's action was secure and in line with the 5G standard. 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 sent an authentication response to the AMF, after which the AMF replied with a service accept message that was marked as "Protected." However, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, which means that the necessary security context for NAS message encryption and integrity protection was not yet established. Despite this, the UE proceeded to send a deregistration request (UE originating) to the AMF. According to the 3GPP 5G security standards, specifically TS 33.501, NAS message protection (encryption and integrity) must only be applied after successful completion of the 5G-AKA procedure, which establishes the security context. Since the AMF sent a protected (i.e., encrypted/integrity-protected) message before 5G-AKA was completed, and the UE accepted and responded to this message, the UE's behavior is not compliant with the standard. The UE should have rejected or ignored protected messages until the security context was established. This could potentially expose the UE to security risks, such as accepting spoofed or manipulated messages. Therefore, the action taken by the UE in this scenario is considered insecure according to the 3GPP 5G security requirements. 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, indicating it was participating in 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 the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are expected 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 GMM Status message in plain text, did not respond, which is appropriate because the message indicated an authentication failure and the session could not proceed securely. The UE did not attempt to continue communication or send sensitive information before security was established. Therefore, the UE's actions were in line with 3GPP security requirements, as it did not expose itself to unnecessary risk or violate protocol expectations. 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 this test scenario, the UE completed the initial NAS steps and sent an authentication response to the AMF, but the 5G-AKA (Authentication and Key Agreement) procedure was not yet 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 procedure, as this is when the necessary security keys are established between the UE and the network. Since the 5G-AKA was not completed, the UE should not have the required keys to decrypt or verify the integrity of the protected message. The UE did not respond to the protected deregistration request, which indicates that it did not process a message that was protected before security context establishment. This behavior aligns with 3GPP security requirements, as the UE must ignore or reject protected messages if security has not been activated. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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 now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message for the IMEISV in plain (unencrypted) form, which is not compliant with 3GPP security requirements. According to 3GPP TS 33.501, once NAS security is established, sensitive information such as the IMEISV must only be requested and transmitted over a protected (encrypted and integrity-protected) NAS connection. The UE, upon receiving an unprotected identity request after security activation, did not respond, thereby refusing to send its IMEISV in the clear. This behavior aligns with 3GPP security guidelines, as the UE is expected to protect its identity information and not disclose it over an unprotected channel after security is established. Therefore, the UE's action in this scenario was secure and in accordance with the 5G standard. 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 requesting the GUTI, but this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after "security mode complete"), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if required, 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 any NAS messages received in plain format after security activation, as responding to such messages could expose sensitive information to potential attackers. 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, the UE and AMF completed the 5G-AKA authentication, establishing a security context for subsequent NAS message encryption and integrity protection. After this, the UE sent a "security mode complete" message, indicating it was ready to use the negotiated security algorithms. However, the AMF responded with a "service reject" message (5GMM Cause 111: Protocol error, unspecified), and crucially, this message was sent in plain (unencrypted) form. Upon receiving this, the UE responded with a "deregistration request (UE originating)," which, according to the 3GPP 5G standard, is the expected behavior when the UE receives a service reject with certain causes, as it should deregister itself from the network. The key security consideration here is whether the UE should have accepted and acted upon a plain (unencrypted) service reject message after security activation. According to 3GPP TS 24.501, after security mode is complete, all subsequent NAS messages (except a few exceptions like "Service Reject" with certain causes) must be integrity protected and, if possible, encrypted. However, the standard does allow for "Service Reject" messages to be sent in plain under some error conditions, and the UE is expected to process them. Therefore, the UE's action—accepting the plain "service reject" and deregistering—aligns with the standard and does not represent a security vulnerability, as it is explicitly permitted by 3GPP for this message type and cause. Secure
174	174	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: c2ada16de5afa04c9abbf0b2aba327aa AUTN: 3030303030303000ee55922b5d550000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.15995287895202637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016292572021484 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 an "authentication request" message to the UE in plain (unencrypted) form, which is not the expected behavior according to the 3GPP 5G security standards. Once the security mode is complete, all subsequent NAS messages between the UE and the AMF should be integrity protected and, if required, encrypted. The UE, upon receiving a plain (unencrypted) authentication request after security mode completion, did not respond. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore or silently discard any NAS messages that are not properly protected after security mode is established, as responding to 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 authentication request was secure and compliant with the 5G standard. 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 NAS security algorithms and was ready to begin secure (encrypted and integrity-protected) NAS communication. However, the AMF then sent a "service accept" message to the UE in plain (unencrypted) form, which is not compliant with the 3GPP 5G standard. According to 3GPP TS 24.501, after the security mode procedure is completed, all subsequent NAS messages between the UE and the AMF must be protected using the agreed-upon security context. The UE, upon receiving a plain (unencrypted) NAS message after security activation, is required by the standard to discard the message and not respond, as accepting or processing such a message could 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 standard. The UE's refusal to process or acknowledge the insecure message ensures the integrity and confidentiality of the NAS signaling. 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 completed and that 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. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), after the completion of the 5G-AKA and the establishment of NAS security, the UE is required to only accept and respond to NAS messages that are integrity protected and ciphered. If the AMF sends a plain (unencrypted) NAS message after security has been established, the UE should ignore it and not respond, 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" message after security was established is in strict compliance with the 3GPP security requirements and demonstrates secure behavior. 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 successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior as per the 3GPP 5G NAS protocol. 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 following the completion of 5G-AKA. According to the 3GPP standards (TS 24.501), after 5G-AKA is completed and security is activated, 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) authentication request after security activation, did not respond to this message. This behavior aligns with the 3GPP security requirements, as the UE is expected to ignore or reject any NAS messages that are not properly protected once a security context is in place. By not responding, the UE avoided a potential downgrade or replay attack, thereby maintaining the integrity and confidentiality of the communication. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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 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 should have been established and all subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 33.501. However, the AMF then sent an "Identity Request" message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. Upon receiving this request, the UE did not respond with the requested identity; instead, it sent a "Deregistration Request (UE originating)" message, effectively terminating its registration. According to the 3GPP standard, after 5G-AKA is completed and security is activated, the UE must not accept or respond to any NAS messages that are not integrity protected and ciphered. The UE's action to deregister rather than respond to a plain (unprotected) identity request demonstrates correct and secure behavior, as it avoids exposing sensitive information (such as SUCI) over an unprotected channel and adheres to the security requirements of the standard. Therefore, the UE's response in this scenario was secure. 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 context should have been established and that subsequent NAS messages should be protected (i.e., integrity protected and 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 the 3GPP standard, since after 5G-AKA, all NAS messages must be protected. The UE, upon receiving this unprotected message, responded by sending a "Deregistration Request (UE originating)" to the AMF. This action by the UE demonstrates that it detected the security anomaly (the receipt of a plain NAS message after security context establishment) and took protective action by deregistering itself from the network, rather than accepting or processing the insecure message. According to 3GPP standards, the UE is expected to reject or ignore unprotected NAS messages after security activation, and deregistration is a valid defensive response. Therefore, the UE's behavior aligns with the security requirements of the 5G standard and demonstrates secure handling of the situation. 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 (which establishes security context for NAS message encryption and integrity protection), the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent a Configuration Update Command to the UE, but this message was sent as a plain (unencrypted and unprotected) NAS message, as indicated by the security header value of 0. Upon receiving this plain message, the UE responded by sending a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G standard (TS 24.501), after 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, encrypted. If the UE receives a plain NAS message from the AMF after security activation, it is required by the standard to treat this as a protocol error and should initiate a deregistration procedure to protect itself from potential security threats, such as replay or man-in-the-middle attacks. In this test, the UE correctly identified the protocol violation (receiving a plain NAS message after security was established) and responded by deregistering itself, thereby adhering to the security requirements of the 5G standard. This demonstrates that the UE's actions were secure and compliant with 3GPP specifications. 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 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 this message was sent in plain (unencrypted) form, and the UE did not respond to it. According to the 3GPP 5G security standards, once 5G-AKA is completed, a security context should be established, and all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. The fact that the AMF sent an Authentication Request after 5G-AKA is unusual, as authentication should not be repeated unless the security context is lost or invalid. More importantly, the UE's refusal to respond to a plain (unencrypted) Authentication Request after security context establishment is the correct and secure behavior, as responding to such a message could expose the UE to replay or downgrade attacks. Therefore, the UE's action of not responding to the insecure message aligns with 3GPP security requirements and demonstrates secure behavior. 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, Deregistration request (UE originating) 0.5084729194641113 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Configuration update command 0.5085830688476562 AMF to UE DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which should indicate that a security context was established and subsequent NAS messages should be integrity protected and ciphered according to 3GPP standards (TS 33.501). However, the AMF responded with a Service Reject message sent in plain (unencrypted and non-integrity protected) form, with a 5GMM cause code 111 (Protocol error, unspecified). The UE, upon establishing this plain Service Reject message, did not respond (UE originating) 3GPP security requirements, after 5G-AKA is completed, the UE must only accept NAS messages that are integrity protected and ciphered; any plain (unencrypted) NAS messages received after security activation should be ignored or treated as suspicious. In this case, the UE did not respond to the plain Service Reject message, which aligns with the security requirements to prevent downgrade or replay attacks. Therefore, the UE's action—refusing to process or respond to a plain NAS message after security context establishment—demonstrates secure behavior as per the 3GPP 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 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. The UE, upon receiving this unexpected plain Authentication Request after 5G-AKA completion, responded by sending a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G security standards, 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, where required, encrypted. The fact that the AMF sent a plain (unencrypted) Authentication Request after security context establishment is a protocol violation and could indicate a security attack or misconfiguration. The UE's action to deregister itself upon receiving such a message demonstrates that it correctly detected the security anomaly and took protective action to avoid further insecure communication. This behavior aligns with 3GPP security requirements, which expect the UE to reject or ignore messages that do not meet security expectations after authentication. Therefore, the UE's response was secure and compliant with the 5G standard. 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, the UE sent an Uplink NAS Transport message, after which the AMF issued an Identity Request message in plain (unencrypted) form, specifically requesting the IMEI. Instead of responding with the requested identity, the UE immediately sent a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages, especially those carrying sensitive information such as device identity (IMEI), must be protected with NAS security (i.e., encrypted and integrity protected). The AMF's request for the IMEI in plain text after security activation is a violation of the standard, as it exposes the UE to potential privacy and security risks. The UE, by refusing to respond to the unprotected identity request and instead deregistering, demonstrated correct and secure behavior as per 3GPP guidelines, which recommend that the UE should not disclose sensitive information over unprotected channels after security has been established. This action helps prevent potential IMEI catching or tracking attacks. Therefore, the UE's response was secure and in line with 3GPP 5G security requirements. 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, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Registration Reject message with 5GMM Cause 62 ("No network slices available"). Notably, the Registration Reject message from the AMF was sent in plain (unencrypted) NAS, and the UE did not respond to this message. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed and NAS security is established, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where applicable, ciphered. However, the standard also specifies that certain messages, such as Registration Reject, may be sent in plain NAS under specific conditions, particularly if the AMF cannot establish security or if the reject is due to a cause that prevents further communication. The UE's lack of response to a plain Registration Reject after security context establishment is a secure and recommended behavior, as responding to unauthenticated or unprotected messages could expose the UE to security risks such as spoofing or denial-of-service attacks. Therefore, the UE's action of not responding to the unprotected Registration Reject message aligns with 3GPP security guidelines and demonstrates secure behavior in this context. 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, 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 3GPP 5G security standards (TS 33.501), after 5G-AKA is completed, all subsequent NAS messages that carry sensitive information, such as the Security Mode Command, must be integrity protected and, where applicable, ciphered. The UE, upon receiving a Security Mode Command in plain text after authentication, did not proceed with the security procedure and instead sent a Deregistration Request, effectively refusing to continue the session under insecure conditions. This behavior aligns with 3GPP security requirements, which state that the UE must not accept security-related NAS messages in plain text after authentication is complete, as this could expose the session to interception or manipulation. Therefore, the UE's action to not respond to the insecure Security Mode Command and to deregister is compliant with the 5G security standard and demonstrates secure behavior. 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 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 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, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where applicable, encrypted. The IMEISV is considered sensitive information, and the 3GPP standard (TS 33.501) explicitly states that the UE must not send its IMEISV in response to a plain (unencrypted) Identity Request after security has been activated. By refusing to respond to the AMF's plain Identity Request for the IMEISV after 5G-AKA completion, the UE correctly adhered to the security requirements, thereby protecting its sensitive information from potential interception. This behavior demonstrates compliance with the 5G security standard and shows that the UE acted securely in this scenario. 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, 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 establishing NAS communication. However, the AMF responded with a Deregistration Accept message sent in plain (unencrypted) NAS, and the UE did not respond to this message. 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 must be integrity protected and, where possible, encrypted. The Deregistration Accept message is a NAS message that, after security context establishment, should be sent with NAS security (i.e., not in plain). The UE, upon receiving a plain (unencrypted) NAS message after security context establishment, is expected to treat this as a protocol error and should not process or respond to such messages, as processing them 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 aligns with the 3GPP security requirements and demonstrates correct and secure behavior by the UE in rejecting insecure communication. 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 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 to initiate further communication. The AMF then responded with a Security Mode Command, which is intended to establish NAS security by activating the agreed ciphering and integrity algorithms (in this case, 5G-EA6 for ciphering and 128-5G-IA2 for integrity). However, the Security Mode Command from the AMF 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), the Security Mode Command is always sent as a plain NAS message, since it is the message that establishes NAS security context and activates encryption and integrity protection for subsequent messages. The UE, upon receiving this plain Security Mode Command, did not respond. This lack of response could indicate that the UE either rejected the message due to a perceived security issue or failed to process it for another reason. However, since the Security Mode Command is expected to be sent in plain text before security is activated, the UE should have accepted and responded to it as per the standard. By not responding, the UE did not proceed with the security context establishment, which is not compliant with the 3GPP standard and could be considered insecure behavior, as it prevents the activation of NAS security for subsequent messages. Therefore, based on the 3GPP standard and the expected behavior, the UE's action in this scenario was not secure. 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, which then responded with an Authentication Request message. Notably, this Authentication Request was sent in plain (unencrypted) form, even though the 5G-AKA had already been completed and a native security context was established. According to the 3GPP 5G security standards, once the 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 required, encrypted to prevent interception or tampering. The UE, upon receiving a plain (unencrypted) Authentication Request after security context establishment, did not respond to the AMF. This behavior aligns with 3GPP security requirements, as the UE is expected to reject or ignore messages that do not meet the required security protections after a security context is active. By not responding, the UE avoided a potential downgrade or replay attack, thereby maintaining the integrity and confidentiality of its communication. Therefore, the UE's action in this scenario was secure. 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 successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. The AMF, instead of proceeding with the expected secured communication, sent another authentication request message to the UE in plain (unencrypted) form, reusing the same ngKSI (Key Set Identifier) that was already in use and associated with an established native security context. Upon receiving this, the UE responded with an "Authentication failure (ngKSI already in use)" message, indicating that it detected the reuse of an ngKSI for which a security context was already active, and refused to proceed with the authentication. According to the 3GPP 5G security standards, once a security context is established and the ngKSI is in use, the UE must not accept further authentication requests for the same ngKSI, especially if they are sent in plain text, as this could be an attempt to downgrade or replay attacks. The UE's action to reject the authentication request and not proceed with unprotected communication demonstrates adherence to the 5G security requirements and protects against potential security threats. Therefore, the UE's behavior in this scenario was secure. 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 the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF issued an identity request for the TMSI, but crucially, this message was sent in plain (unencrypted) form. The UE did not respond to this identity request. According to the 3GPP 5G security standards, once 5G-AKA is completed, NAS signaling messages between the UE and the AMF must be integrity protected and, where possible, encrypted to prevent exposure of sensitive information and to protect against various attacks, such as identity interception or replay attacks. The TMSI, while a temporary identifier, is still considered sensitive and should not be transmitted in response to a plain (unencrypted) identity request after security has been established. The UE's refusal to respond to an unprotected identity request after 5G-AKA is therefore in line with 3GPP security requirements, as it prevents the potential exposure of its identity in an insecure context. This behavior demonstrates that the UE is correctly enforcing the security policy mandated by the standard. 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 5G-AKA authentication, the UE sent a Service Request to the AMF, which is a standard procedure to resume or establish a connection for data or signaling. The AMF then responded with a Configuration Update Command, which was sent as a protected (secured) NAS message. However, the security header of the downlink message was marked as "Unknown," and the UE did not provide any response to this message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. 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 respond, as a security measure to prevent potential attacks or protocol violations. In this case, the UE's lack of response to a downlink message with an unknown security header aligns with the expected secure behavior as per 3GPP specifications, as it avoids processing potentially unprotected or tampered messages. Therefore, the UE's action in this scenario was secure. 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 standard step to resume or establish a connection. In response, the AMF sent an Authentication Reject message to the UE, and notably, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standards, after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where possible, encrypted to ensure confidentiality and prevent tampering or replay attacks. The UE, upon receiving a plain (unencrypted) Authentication Reject message after security context establishment, did not respond further. This behavior aligns with 3GPP security requirements, which specify that the UE must ignore or silently discard any NAS messages that are not integrity protected or encrypted after security has been activated. By not responding to the unprotected message, the UE demonstrated correct and secure behavior as per the standard, thereby preventing potential security breaches such as downgrade or spoofing attacks. 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), which was sent in plain (unencrypted) NAS signaling. The UE then responded with an identity response. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where possible, encrypted. The SUCI is specifically designed to protect the subscriber's permanent identifier (SUPI) from exposure, even if sent in the clear, but the expectation is that after authentication, the NAS security context is established and all further NAS messages, including identity requests and responses, should be protected. In this case, the UE responded to a plain (unencrypted) identity request after 5G-AKA was completed, which is not compliant with the 3GPP security requirements. The UE should have rejected or ignored the request, or at least not responded with sensitive information over an unprotected channel. Therefore, the action taken by the UE was insecure according to the 5G standard. 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 procedure, the UE sent 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) NAS message. However, the security header of the downlink 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 is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. 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 expected to discard the message and not respond, as a security measure to prevent potential attacks or protocol violations. In this case, the UE's lack of response to a downlink message with an unknown security header aligns with the expected secure behavior as per 3GPP standards, as it avoids processing potentially unprotected or malicious messages. Therefore, the UE's action in this scenario 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)(5G-AKA, 3) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on 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 and key agreement procedure had not yet been completed, meaning that security context establishment (i.e., mutual authentication and key derivation for integrity and ciphering) was not yet in place. The AMF, under test control, responded with a deregistration request message that was integrity protected and ciphered, as indicated by the security header. 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 via 5G-AKA. Since the 5G-AKA was not completed, the UE would not have the necessary keys to decrypt or verify the integrity of the protected message. The UE's lack of response to the protected deregistration request is therefore correct and secure behavior, as it prevents the processing of potentially malicious or out-of-sequence messages before security is established. This behavior aligns with 3GPP security requirements, which mandate that UEs ignore protected NAS messages if a security context is not yet in place. 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 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) form, requesting the UE's GUTI. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), once NAS security is established (i.e., after the security mode complete message), all subsequent NAS messages must be integrity protected and, if required, encrypted. The UE is expected to ignore or silently discard any NAS messages received in plain format after security activation, as responding to such messages could expose sensitive information to potential attackers. Therefore, the UE's action of not responding to the plain identity request after security activation is compliant with the 5G security standard and demonstrates secure behavior. 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 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 standard (TS 24.501), once NAS security is established (i.e., after the security mode complete), all subsequent NAS messages, including identity requests, must be protected (encrypted and integrity protected). The UE, upon receiving an unprotected identity request after security activation, is expected to ignore the message and not respond, as responding would risk exposing sensitive information (such as the IMEISV) over an unprotected channel. 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. 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 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) form, requesting the SUCI (Subscription Concealed Identifier). The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after the security mode complete), all subsequent NAS messages, including identity requests, must be protected (encrypted and integrity protected). The SUCI is a privacy-sensitive identifier, and sending it in response to an unprotected (plain) identity request after security activation would expose the UE to privacy and security risks. By refusing to respond to an unprotected identity request after security mode activation, the UE is adhering to the 3GPP security requirements and protecting the subscriber's privacy. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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 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 for the IMEI in plain (unencrypted) form, which is not compliant with 3GPP standards. According to 3GPP TS 24.501, once NAS security is established, all subsequent NAS messages, including identity requests, must be protected. The UE, upon receiving an unprotected (plain) 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 unprotected NAS messages after security mode is complete, as responding could expose sensitive information and compromise user privacy. Therefore, the UE's action of not responding to the unprotected identity request was secure and in accordance with the 5G security requirements. 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 (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 SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) form rather than being protected by the established NAS security context. According to the 3GPP 5G standard (TS 24.501), once the security mode is complete, all subsequent NAS messages must be integrity protected and, if required, encrypted. The UE, upon receiving a plain (unprotected) identity request after security activation, is expected to ignore or silently discard such messages to prevent potential security breaches, such as replay or interception attacks. In this test, the UE did not respond to the unprotected identity request, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by refusing to transmit sensitive information (SUCI) over an unprotected channel. Therefore, the UE's action was secure. 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 in plain (unencrypted) form, requesting the UE's GUTI (Globally Unique Temporary Identifier). The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after "security mode complete"), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if required, encrypted. The UE is expected to ignore or silently discard any NAS messages received in plain form after security activation, as responding to such messages could expose sensitive information to potential attackers. Therefore, the UE's action of not responding to the plain identity request after security mode activation is compliant with the 3GPP standard and demonstrates secure behavior in this context. 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 3GPP 5G standards (TS 24.501), once NAS security is established (i.e., after "security mode complete"), all subsequent NAS messages, especially those requesting sensitive information such as IMEISV, must be protected (encrypted and integrity protected). The UE, upon receiving an unprotected 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 requests for sensitive information if they are not properly protected after security activation. Therefore, the UE's action of not responding to the unprotected identity request was secure and compliant with the 5G standard. 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, 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, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard, once 5G-AKA is completed and a security context is established, all subsequent NAS messages, especially those involving sensitive information such as identity requests, must be protected using NAS security (i.e., encrypted and integrity protected). The UE, upon receiving an unprotected identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore or reject unprotected NAS messages that require security after the security context is active, to prevent potential security breaches such as identity interception or replay attacks. Therefore, the UE's action of not responding to the plain identity request after security activation was correct and secure according to the 5G standard. 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 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, requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) NAS. According to the 3GPP 5G standard (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, where required, encrypted. The UE, upon receiving a plain (unencrypted) identity request after security activation, is expected to reject the message or ignore it, as responding to such a request would expose sensitive information and violate the security procedures mandated by the standard. 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 enforced the security policy by refusing to process or respond to insecure messages after security activation. Therefore, the UE's action was secure. 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 the security context should now be established and all subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 33.501. However, the AMF, under test control, sent an "Identity Request" message in plain (unencrypted) NAS format, requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE did not respond to this request. According to the 3GPP 5G security standards, after the security context is established (post-5G-AKA), the UE must only accept and respond to NAS messages that are integrity protected and ciphered; it must ignore or silently discard any plain NAS messages received after this point. By not responding to the plain "Identity Request" message, the UE correctly followed the 3GPP security requirements, thereby preventing potential exposure of sensitive information in an unprotected message. This behavior demonstrates that the UE's actions were secure and compliant with 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 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, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) NAS, despite the security context being available. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed and a security context is established, all subsequent NAS messages, including identity requests, must be sent with NAS security (i.e., encrypted and integrity protected). The UE is required to ignore or silently discard any NAS messages received in plain text after security activation, as responding to such messages could expose sensitive information and compromise user privacy. Therefore, the UE's action of not responding to the plain identity request after security activation is in strict compliance with the 3GPP standard and demonstrates secure behavior in this context. 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 successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context should now be established and all subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF, under test control, 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), once the 5G-AKA is completed and security context is established, the UE must only accept and respond to NAS messages that are integrity protected and ciphered; it must ignore or silently discard any subsequent plain (unencrypted) NAS messages. 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 and maintaining the integrity of the secure channel. Therefore, the UE's action in this scenario was secure. 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 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. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) form. 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 between the UE and the AMF must be integrity protected and, where applicable, encrypted. The SUCI is a privacy-sensitive identifier, and the standard mandates that it should not be transmitted in the clear after security activation. By refusing to respond to an identity request sent in plain text after security activation, the UE is adhering to the 3GPP security requirements and protecting the subscriber's privacy. Therefore, the UE's action in this scenario is secure and compliant with the 5G standard. 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 the security context had been established and NAS security should be active. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the TMSI, but crucially, this message was sent in plain (unencrypted) NAS format rather than being protected by the established security context. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed and security is activated, 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, is expected to ignore or silently discard such messages to prevent potential security risks such as identity exposure or replay attacks. In this test, the UE did not respond to the unprotected identity request, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by refusing to process or respond to insecure messages after security activation. 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 a Downlink NAS Transport message containing an Identity Request for the IMEISV. Notably, this Identity Request was sent in plain (unencrypted) NAS, despite the fact that 5G-AKA had already been completed, meaning that NAS security (encryption and integrity protection) should have been activated for all subsequent NAS messages, as per 3GPP TS 33.501 and TS 24.501. The UE, upon receiving this unprotected Identity Request, did not respond. According to 3GPP standards, after NAS security is established, the UE must ignore any subsequent NAS messages that are not integrity protected and encrypted, especially those requesting sensitive information such as IMEISV. By refusing to respond to the unprotected Identity Request, the UE correctly adhered to the security requirements of the 5G standard, thereby protecting its sensitive identity information from potential interception or replay attacks. This behavior demonstrates that the UE's actions were secure and compliant with 3GPP security guidelines. 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 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 SUCI (Subscription Concealed Identifier). 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 security context and NAS encryption should have been established. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed and a security context is in place, all subsequent NAS messages containing sensitive information, such as identity requests and responses, must be protected (i.e., integrity protected and, where applicable, encrypted). The UE, upon receiving an unprotected (plain) Identity Request after security context establishment, did not respond. This behavior aligns with 3GPP security requirements, as the UE is expected to ignore or reject requests for sensitive information if they are not properly protected, to prevent exposure of subscriber identity over the air. Therefore, the UE's action of not responding to the unprotected Identity Request was secure and compliant with the 5G standard. 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 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a plain (unencrypted) Identity Request message asking for the TMSI. 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 AMF's Identity Request was sent in plain text, which is a security risk, but the focus here is on the UE's behavior. The UE, upon receiving a plain (unencrypted) Identity Request after security context establishment, did not respond. This is the correct and secure behavior as per 3GPP standards, which specify that the UE must not respond to requests for sensitive information (such as TMSI) unless the NAS security context is active and the message is integrity protected (and encrypted if possible). By refusing to respond to an unprotected identity request after 5G-AKA, the UE prevented potential exposure of its identity, demonstrating compliance with the security requirements. Therefore, the UE's action in this scenario was secure. 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 issued an Identity Request message, 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 (TS 33.501), 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, where applicable, encrypted. Sensitive information such as the IMEISV should not be transmitted in plain text after security activation. The UE's refusal to respond to a plain (unencrypted) Identity Request for the IMEISV after security activation is in line with 3GPP security requirements, as responding would expose sensitive device information over an unprotected channel. Therefore, the UE's action of not responding to the unprotected request demonstrates adherence to the 5G security standard and protects the user's privacy and device identity. 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 0.5513196975708010 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 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), and this message was sent in plain (unencrypted) form. The UE did not respond to this request. 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 applicable, encrypted to prevent exposure of sensitive information. The SUCI is designed to protect the subscriber's permanent identity (SUPI) and should only be transmitted in a secure manner after authentication and security mode establishment. By refusing to respond to a plain (unencrypted) Identity Request after 5G-AKA completion, the UE is adhering to the 3GPP security requirements, as responding in plain would expose sensitive information and violate the standard. Therefore, the UE's action in this scenario was secure and compliant with 5G security specifications. 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 the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message, specifically requesting the IMEISV, and this message was sent in plain (unencrypted) NAS. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages, especially those requesting sensitive information such as the IMEISV, must be protected by NAS security (i.e., integrity protected and ciphered). The AMF's request for the IMEISV in plain text is a violation of this standard, as it exposes sensitive device information to potential interception. The UE, by refusing to respond to an unprotected identity request after security context establishment, is acting in accordance with 3GPP security guidelines, which recommend that the UE should not disclose sensitive identifiers unless the NAS security context is active. Therefore, the UE's action of not responding to the plain identity request is 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 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 TMSI, and this message was sent in plain (unencrypted) form. The UE did not respond to this 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 and to protect against various attacks. The TMSI, while not as sensitive as the SUPI, is still considered privacy-relevant information. The UE's refusal to respond to an unprotected (plain) Identity Request after security context establishment is in line with 3GPP security recommendations, which state that the UE should not send identity information in response to a plain request once security has been activated. Therefore, the UE's action of not responding to the unprotected Identity Request was secure and compliant with the 5G standard. 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, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a plain (unencrypted) Identity Request asking for the TMSI. 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 applicable, encrypted to prevent exposure of sensitive information. The AMF's Identity Request was sent in plaintext, which is a security risk, but since the focus is on the UE's behavior, it is important to note that the UE did not respond to this unprotected request. This is the correct and secure behavior as per 3GPP standards, which specify that the UE must not respond to identity requests that are not integrity protected after security mode is established. By refusing to respond to an unprotected identity request, the UE prevented potential exposure of its TMSI and adhered to the security requirements of the standard. Therefore, the UE's action in this scenario was secure. 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 the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a plain (unencrypted) Identity Request message asking for the TMSI. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed, NAS security (encryption and integrity protection) should be activated, and all subsequent NAS messages, especially those requesting sensitive information such as the TMSI, must be protected. The UE, upon receiving an unprotected (plain) Identity Request after security activation, is expected to ignore the request 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 security requirements of the 5G standard. This behavior demonstrates that the UE correctly enforced the security policy by refusing to send potentially sensitive information in the clear after security activation. Therefore, the UE's action was 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, 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 service accept message, but crucially, this downlink message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, specifically TS 33.501, once 5G-AKA is completed, both NAS signaling integrity and encryption should be activated before any further NAS messages are exchanged, except for a few explicitly allowed exceptions (such as the initial registration or authentication messages). The service accept message is not one of these exceptions and should be protected. The UE, upon receiving a plain (unencrypted) service accept message after security context establishment, is expected to reject or ignore the message, as accepting or acting upon unprotected NAS messages after security activation would expose the UE to potential security threats such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected service accept message, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by not accepting or processing insecure messages after 5G-AKA completion. 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 procedure, the UE sent a Service Request message to the AMF, which is a standard step to request access to network services. The AMF then responded with a Service Accept message, but crucially, this downlink message was sent in plain (unencrypted) text. According to the 3GPP 5G security standards, once 5G-AKA is completed, both the UE and the AMF are expected to establish NAS security, which includes encryption and integrity protection for subsequent NAS messages. The Service Accept message, being a NAS message sent after authentication, should have been protected. The UE, upon receiving an unprotected (plain) Service Accept message after security context establishment, is expected to either ignore the message or respond with a security mode reject or similar error, as accepting unprotected messages at this stage could 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 aligns with the security expectations of the 3GPP standard, as it did not accept or process an insecure message. Therefore, the UE's action 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 after authentication. 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 reject message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, after the completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted to ensure confidentiality and prevent tampering or eavesdropping. The UE, upon receiving the plain (unencrypted) Service Reject message after security context establishment, did not respond further, which aligns with the 3GPP security recommendations: the UE should ignore or silently discard any unprotected NAS messages received after security activation, as processing such messages could expose the UE to security risks such as spoofing or denial-of-service attacks. Therefore, the UE's action of not responding to the unprotected Service Reject message demonstrates adherence to the 5G security standard and is considered secure behavior. 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 is the expected behavior for initiating a service in a 5G standalone network. The AMF, under test control, responded with a Service Reject message, specifically indicating the cause "UE identity cannot be derived by the network" (5GMM Cause: 9). Notably, this Service Reject message was sent in plain (unencrypted) form, even though the 5G-AKA procedure had already been completed, which means that both the UE and the network should have established security contexts for NAS message encryption and integrity protection. According to 3GPP standards (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages, including Service Reject, must be integrity protected and, where possible, encrypted. The UE, upon receiving the unprotected Service Reject message, did not respond further. This behavior aligns with the 3GPP security recommendations, which state that the UE should ignore or silently discard any NAS messages that are not integrity protected after security activation, as processing such messages could expose the UE to security risks such as spoofing or denial-of-service attacks. Therefore, the UE's action of not responding to the unprotected Service Reject message demonstrates adherence to the 5G security standard and is considered secure. 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 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 request access to network services. The AMF, under test control, responded with a Service Reject message, indicating a protocol error (5GMM Cause 111), and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards (TS 33.501), after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where applicable, encrypted to ensure confidentiality and prevent tampering or eavesdropping. In this test, the UE received a plain (unencrypted and possibly unauthenticated) Service Reject message from the AMF and, as observed, did not respond to it. This behavior aligns with the 3GPP security requirements, which specify that the UE should ignore or discard any NAS messages that are not integrity protected after security context establishment, as accepting such messages could expose the UE to security risks such as spoofing or denial of service. Therefore, the UE's action of not responding to the unprotected Service Reject message demonstrates adherence to the 5G security standard and is considered 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 for initiating a service. The AMF then responded with a Service Reject message, indicating a 5GMM Cause 21 (synchronization failure), and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where possible, encrypted to ensure confidentiality and prevent tampering or eavesdropping. 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, which specify that the UE should ignore or silently discard any NAS messages that are not integrity protected or encrypted after security has been activated. By not responding to the unprotected Service Reject message, the UE demonstrated correct and secure behavior as per the standard, thereby preventing potential security risks such as replay or downgrade attacks. 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, which is expected behavior as the UE continues with NAS signaling. 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. According to the 3GPP 5G standard, after receiving a Security Mode Command, the UE is required to verify the message, apply the indicated security algorithms, and 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 proceed with the security context activation, which is a deviation from the standard. This lack of response could be due to the UE not recognizing the security header, an unsupported algorithm, or a failure to process the protected message. Regardless of the reason, the UE's failure to respond means it did not establish a secure NAS signaling context as required, potentially leaving the communication session incomplete or vulnerable. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. 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, 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 registration and session establishment. The AMF then responded with a Security Mode Command, which is a critical step where the AMF instructs the UE to activate specific ciphering and integrity protection algorithms for subsequent NAS messages. However, the Security Mode Command from the AMF specified the use of 5G-EA0 and 5G-IA0 algorithms, which are "null" algorithms, meaning no encryption or integrity protection would be applied to the NAS messages. Additionally, the security header in the message was marked as "Unknown," and the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, the use of null algorithms is only permitted in very specific, controlled scenarios (such as emergency services or when explicitly allowed by policy), and generally, 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 interception or tampering. The UE's lack of response in this context indicates that it did not accept the insecure security configuration, which aligns with the security requirements of the 5G standard. Therefore, the UE's action was secure, as it refused to proceed with unprotected communication. 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 to resume or establish a connection. 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 security specifications (TS 33.501), 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 prevent tampering or eavesdropping. The UE, upon receiving a plain (unencrypted) NAS message after security context establishment, is expected to discard the message and not respond, as processing such messages could 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 Configuration Update Command, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by refusing to process or acknowledge insecure messages after authentication. Therefore, the UE's action 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 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 context establishment and registration process had concluded. Subsequently, the AMF sent a "Security Mode Command" message to the UE, but this message was transmitted as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard, after the 5G-AKA procedure is completed and a security context is established, all subsequent NAS messages exchanged between the UE and the AMF must be protected using the negotiated ciphering and integrity algorithms (in this case, 5G-EA4 and 5G-IA5). The UE, upon receiving a Security Mode Command in plain text after security context establishment, did not respond to the message. This behavior aligns with the 3GPP security requirements, as the UE is expected to reject or ignore any unprotected NAS messages once a security context is in place, to prevent potential security breaches such as replay or man-in-the-middle attacks. Therefore, the UE's action of not responding to the unprotected Security Mode Command was secure and compliant with the 5G standard. 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. Subsequently, the AMF responded with a Security Mode Command message, which was sent as a plain (unencrypted) 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 next step is for the AMF to initiate NAS security by sending a Security Mode Command in plain text, since NAS security (ciphering and integrity protection) is not yet activated at this point. The UE is expected to respond to this command, after which NAS security is established and subsequent messages are protected. 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 the UE is required to process and respond to the Security Mode Command to establish NAS security. By failing to respond, the UE did not proceed to activate NAS security, leaving the communication channel unprotected and potentially vulnerable. Therefore, the action taken by the UE was insecure, as it did not follow the required security procedure to establish a protected communication channel after authentication. 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 a normal step 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 standard (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted. The Authentication Reject message sent in plain text after security context establishment is a protocol violation by the AMF, as the message should have been protected. The UE, upon receiving an unprotected (plain) NAS message after security has been established, is required by the standard to discard the message and not respond, as a security measure to prevent downgrade or replay attacks. The UE's lack of response indicates that it correctly identified the protocol violation and protected itself by not processing or acknowledging the unprotected message. Therefore, the UE's behavior aligns with the 3GPP security requirements 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, which is the expected behavior for initiating further communication or requesting services. The AMF, under test control, responded with an Authentication Reject message, which was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, once 5G-AKA is completed, both the UE and the network are expected to establish NAS security, meaning that subsequent NAS messages should be integrity protected and, where applicable, encrypted. The Authentication Reject message is a security-critical message, and per 3GPP TS 24.501, after security mode is established, the UE should only accept such messages if they are integrity protected. In this test, the UE did not respond to the plain (unencrypted) Authentication Reject message, which aligns with the 3GPP security requirements: the UE must ignore unauthenticated or unprotected critical messages after security activation to prevent security attacks such as downgrades or spoofing. Therefore, the UE's action—providing no response to the unprotected Authentication Reject—demonstrates secure behavior as per the 5G standard. 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 completed the initial NAS procedures and sent an authentication response to the AMF, the AMF responded with an identity request for the TMSI, sent as a plain (unencrypted) 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, the UE should not respond to identity requests sent in plain text after the authentication response, as this could expose sensitive information (such as the TMSI) to potential interception or replay attacks. The UE's action of not responding to the plain identity request is therefore in line with the security requirements of the 5G standard, as it avoids disclosing potentially sensitive information before a secure channel is established. This behavior demonstrates that the UE is correctly implementing the security procedures specified by 3GPP for 5G NAS communication. 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, but this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA 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 cleartext before the NAS security context is established, which only occurs after successful completion of 5G-AKA. The UE, upon receiving an unprotected identity request for the IMEISV before security activation, did not respond. This behavior aligns with the security recommendations in the standard, which state that the UE should not disclose sensitive identifiers in the clear prior to NAS security activation. By refusing to respond to the unprotected request, the UE protected its IMEISV from potential interception or misuse, demonstrating adherence 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 successful completion of the 5G-AKA authentication procedure, 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 test summary, was transmitted as a plain (unencrypted and unauthenticated) NAS message. The Security Mode Command is critical because it instructs the UE to activate NAS security (ciphering and integrity protection) using the negotiated algorithms (5G-EA4 for ciphering and 128-5G-IA2 for integrity). According to the 3GPP 5G standard (TS 24.501), the Security Mode Command must be sent as a plain NAS message, as security context is not yet established at this point. However, after receiving the Security Mode Command and activating security, all subsequent NAS messages from the UE should be protected (i.e., integrity protected and, if required, ciphered). In this test, the UE responded to the Security Mode Command by sending a Deregistration Request, but the capture does not indicate that this message was protected (the security header is not specified, but the summary suggests the previous message was plain). If the Deregistration Request was sent as a plain message after security activation, this would be a violation of the 3GPP standard, as the UE is expected to protect all subsequent NAS messages after security mode is activated. This exposes the UE to potential security risks, such as message tampering or interception. Therefore, based on the information provided and the expected behavior per 3GPP, the UE's action 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 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 as a protected message, specifying the use of ciphering algorithm 5G-EA5 and integrity algorithm 5G-IA0 (null integrity protection). Notably, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after authentication, the AMF should select both ciphering and integrity algorithms, and the Security Mode Command should be integrity protected to ensure the authenticity and integrity of the message. The use of 5G-IA0 (null integrity) means that the Security Mode Command was not integrity protected, which is not compliant with the standard, as integrity protection is mandatory for this message. The UE, by not responding to a Security Mode Command that lacks integrity protection, is acting securely and in accordance with 3GPP specifications, as accepting such a command could expose it to security risks such as man-in-the-middle attacks. Therefore, the UE's refusal to respond is a secure action. 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, and the AMF subsequently sent another Identity Request, specifically requesting the TMSI, in plain (unencrypted) NAS signaling. 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 send sensitive information such as the TMSI or SUPI in response to an Identity Request if NAS security has not been activated, to prevent exposure of subscriber identity over the air in plain text. 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 and helps protect the subscriber's identity from potential interception. Therefore, the UE's action of withholding a response in this context 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 engaged in NAS communication where, after the initial NAS steps, 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 procedure had not yet been completed. According to the 3GPP 5G security standards, sensitive information such as the IMEISV should only be transmitted after the NAS security context is established, which occurs after successful completion of 5G-AKA. In this case, the UE did not respond to the AMF's plain (unencrypted) identity request for the IMEISV, thereby refusing to send sensitive information before a secure channel was established. This behavior aligns with the security requirements outlined by 3GPP, as it prevents exposure of sensitive identifiers over an unprotected channel. Therefore, the UE's action was secure and compliant with the 5G standard. 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 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. Notably, the 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 standard (TS 24.501), the Security Mode Command is always sent as a plain NAS message, since at this stage, NAS security (ciphering and integrity protection) has not yet been activated; the purpose of this message is to establish the NAS security context. The UE, upon receiving this plain Security Mode Command, is expected to respond with a Security Mode Complete message, which should be the first NAS message protected with the newly agreed security algorithms. However, in this test, the UE did not respond at all to the Security Mode Command. This lack of response could indicate that the UE rejected the plain Security Mode Command, which would be non-compliant with the 3GPP standard, as the UE is expected to accept and process this message in plain form. If the UE refused to process the Security Mode Command because it was not encrypted, this would be an incorrect implementation, as the standard explicitly requires this message to be sent in plain text. Therefore, the UE's action in this scenario is considered insecure, as it does not comply with the expected secure behavior defined by the 5G standard. Insecure

241	241	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.16009092330932617 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1604149341583252 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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, once the security mode complete message is sent, both the UE and the AMF should have established a secure NAS security context, and all subsequent NAS messages must be protected (i.e., integrity protected and, if required, ciphered). However, in this test, the AMF (under tester control) sent another "security mode command" message to the UE after the security mode complete, which is not a standard-compliant sequence; the security mode command should not be sent again after the security context is established. The UE, upon receiving this unexpected and potentially malicious message (which was protected but with an unknown security header), did not respond. This lack of response from the UE is the correct and secure behavior as per 3GPP standards, as it prevents possible downgrade or replay attacks and ensures that the UE does not process out-of-sequence or suspicious security messages. Therefore, the UE's action in this scenario was secure and compliant with the 5G security requirements. 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 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 sent a Security Mode Command to the UE, which was protected (i.e., integrity protected and/or ciphered) using the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity). The Security Mode Command is the first NAS message that should be protected after the security context is established. According to the 3GPP 5G standard (TS 24.501), upon receiving a protected Security Mode Command, the UE is expected to verify the integrity of the message and respond with a Security Mode Complete message if the verification is successful. In this test, the UE did not respond to the Security Mode Command, and the security header of the message was marked as "Unknown" in the test summary. This lack of response could indicate that the UE either failed to process the protected message, did not recognize the security header, or detected an issue with the message's integrity or ciphering. From a security perspective, the UE's refusal to respond to a message with an unknown or unrecognized security header is the correct and secure behavior, as responding to potentially malformed or tampered messages could expose the UE to security risks. Therefore, the UE's action aligns with the 3GPP security requirements, as it did not proceed with further communication when the security of the message could not be assured. Secure

243	243	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0293 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.15967893600463867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15994000434875488 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. Subsequently, the AMF sent a Security Mode Command to the UE, but this message was transmitted 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), the Security Mode Command is the message that establishes NAS security (ciphering and integrity protection) between the UE and the network. It is expected and compliant for the Security Mode Command itself to be sent as a plain NAS message, since security context is not yet established at this point. The UE, however, did not respond to the Security Mode Command. From a security perspective, the UE's lack of response is a cautious and secure action, as it avoids proceeding with further communication until a secure context is established. This behavior prevents the possibility of accepting a potentially tampered or replayed Security Mode Command, which could be a vector for certain attacks if the message was not received as expected or if the context was not valid. Therefore, the UE's action in this scenario aligns with secure practices as outlined by the 3GPP standard, as it does not proceed with insecure communication. 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 that it had accepted the negotiated security algorithms (ciphering: 5G-EA0/null, integrity: 128-5G-IA2). Subsequently, the AMF sent a "security mode command" message back to the UE, but this message was sent as a plain (unencrypted and unauthenticated) NAS message, even though the security context had already been established. According to the 3GPP 5G standard (TS 24.501), once the security mode is completed and the security context is active, all subsequent NAS messages between the UE and the AMF must be protected using the agreed-upon integrity and ciphering algorithms. 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 processing such a message could 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 "security mode command" from the AMF, which is the correct and secure behavior as per 3GPP specifications. Therefore, the UE's action was secure. 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 this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should only be transmitted after NAS security (ciphering and integrity protection) is activated, which occurs after successful completion of the 5G-AKA authentication and key agreement procedure. Since the AMF sent the identity request before security activation, the UE correctly did not respond with its IMEISV in the clear, thereby protecting its sensitive information from potential interception. This behavior aligns with the security requirements of the 5G standard, as the UE must not disclose its IMEISV or other sensitive identifiers over an unprotected channel. Therefore, the UE's action in this scenario was secure and compliant with 3GPP specifications. 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 replied with an identity request for the TMSI, but this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards, user identity information such as the TMSI should not be transmitted in cleartext after security has been established, and ideally, the network should avoid requesting sensitive identities in plain before security activation unless absolutely necessary. In this case, the UE did not respond to the AMF's plain identity request. This behavior aligns with the security principle of not exposing user identity information over an unprotected channel, as responding would have risked leaking the TMSI to potential eavesdroppers. Therefore, the UE's refusal to respond to an unprotected identity request demonstrates adherence to 3GPP security guidelines and is considered a secure action. 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 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. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should not be transmitted in cleartext before the establishment of NAS security, which is only activated after successful completion of the 5G-AKA authentication and key agreement procedure. The UE, upon receiving a plain (unencrypted) identity request for the IMEISV before NAS security was established, did not respond. This behavior aligns with the security requirements of the 5G standard, as the UE is expected to protect its sensitive identifiers and only provide them over a secure, encrypted channel. By refusing to send the IMEISV in response to an unprotected request, the UE demonstrated secure behavior in accordance with 3GPP guidelines. 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, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which is the expected behavior according to the 3GPP 5G security procedures. Following this, the AMF sent a Security Mode Command to the UE, which was indicated as being "Protected" and included the ABBA parameter, ciphering algorithm 128-5G-EA2, and integrity algorithm 128-5G-IA3. However, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard (TS 24.501 and TS 33.501), after receiving a Security Mode Command, the UE is expected to verify the integrity and correctness of the message, and if valid, respond with a Security Mode Complete message. If the security header is "Unknown" or the message fails integrity checks, the UE should discard the message and not respond, as a security measure to prevent potential attacks or protocol violations. In this case, since the Security Mode Command's security header was "Unknown," the UE's lack of response aligns with the 3GPP security requirements, as responding to a potentially invalid or tampered message could compromise security. Therefore, the UE's action was secure and in compliance with the 5G standard. 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 standard step to resume or establish a NAS signaling connection. 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 security specifications (TS 33.501), once 5G-AKA is completed, 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 (unprotected) NAS message after security context establishment, is required by the standard to discard the message and not respond, as accepting or processing such messages could 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 Configuration Update Command, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior. Therefore, the UE's action in this scenario was secure. 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 the initial NAS procedures, the UE sent an identity response to the AMF. Subsequently, the AMF issued another identity request, specifically requesting the IMEISV, and this message was sent in plain (unencrypted) NAS signaling because the 5G-AKA authentication and key agreement procedure had not yet been completed. The UE did not respond to this plain identity request. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should not be transmitted in cleartext over the air interface unless NAS security (encryption and integrity protection) has been established, which only occurs after successful completion of 5G-AKA. By refusing to respond to the AMF's request for the IMEISV in plain text, the UE adhered to the security requirements and protected its sensitive information from potential interception. This behavior demonstrates that the UE is compliant with 3GPP security guidelines and is acting securely in this context. 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, the 5G standalone User Equipment (UE) completed the initial NAS steps and sent an identity response to the AMF. Subsequently, the AMF, under test control, sent another identity request to the UE, specifically requesting the TMSI, 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, the UE should not disclose sensitive permanent or semi-permanent identifiers (such as SUPI or TMSI) in response to plain (unencrypted) identity requests after the initial identity exchange, especially before the security context is established via 5G-AKA. In this test, the UE did not respond to the second identity request sent in plain text, which aligns with the security requirements to prevent exposure of sensitive information over an unprotected channel. This behavior demonstrates that the UE correctly refused to transmit potentially sensitive identity information without an established security context, thereby adhering to the 3GPP security guidelines. 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, still before the completion of 5G-AKA (meaning NAS security context was not yet established), sent another identity request to the UE, specifically requesting the IMEISV, and this request was sent in plain (unencrypted) NAS. The UE did not respond to this request. According to the 3GPP 5G standard, sensitive information such as the IMEISV should not be transmitted in plain text before NAS security is activated, as this could expose the UE to privacy and security risks (e.g., device tracking or identification by an attacker). The UE's refusal to respond to a plain (unencrypted) identity request for IMEISV before the completion of 5G-AKA demonstrates adherence to the security requirements of the standard, as it avoids disclosing sensitive information without encryption. Therefore, the UE's action in this scenario was secure and in line with 3GPP security guidelines. 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 initiated a service request to the AMF. In response, the AMF sent an identity request message, specifically requesting the UE's GUTI (Globally Unique Temporary Identifier). Notably, this identity request was sent in plain (unencrypted) NAS signaling, despite the fact that 5G-AKA had already been completed, which means that NAS security (encryption and integrity protection) should have been activated for all subsequent NAS 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 AMF sends a NAS message in plain after security has been established, the UE must ignore it and not respond, to prevent potential security vulnerabilities such as identity exposure or replay attacks. Therefore, the UE's action of not responding to the unprotected identity request aligns with the 3GPP security requirements and demonstrates secure behavior in this context. 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 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which is a normal step in establishing a PDU session. The AMF then responded with a Service Accept message, but crucially, this downlink message was sent in plain (unencrypted) text, as indicated by the packet capture and the test summary. According to the 3GPP 5G security standards (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 applicable, encrypted to ensure confidentiality and prevent replay or man-in-the-middle attacks. The UE, upon receiving a plain (unencrypted) Service Accept message after 5G-AKA, did not respond further. This behavior aligns with the 3GPP security requirements, as the UE is expected to reject or ignore any NAS messages that are not properly protected after security activation. By not responding to the unprotected message, the UE demonstrated correct and secure behavior, refusing to process potentially insecure or malicious messages. Therefore, the UE's action in this scenario was secure. 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 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 message, specifically requesting the IMEI, and crucially, 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), after the completion of 5G-AKA, all subsequent NAS messages, including identity requests, must be integrity protected and, where possible, encrypted to prevent exposure of sensitive information such as the IMEI. The UE is expected to refuse to send its IMEI in response to a plain (unencrypted) identity request after security has been established, as responding would risk exposing its permanent equipment identity to potential interception or replay attacks. By not responding to the unprotected identity request, the UE adhered to the security requirements of the 5G standard, thereby protecting its IMEI from being transmitted in the clear. Therefore, the UE's action in this scenario was secure. 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 the initial NAS security context should have been established and all subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 24.501. However, the AMF then sent a "GMM Status" message with cause 97 ("Message type non-existent or not implemented") in plain (unencrypted and non-integrity protected) form. According to the 3GPP standard, after security mode command and 5G-AKA completion, the UE must only accept and process NAS messages that are integrity protected and ciphered (except for a very limited set of messages (such as Service Request in some cases). The UE, upon receiving a plain (unprotected) NAS message after security context establishment, is required to silently discard it and not respond, as a security measure to prevent downgrade or replay 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 standard. This demonstrates that the UE properly enforced NAS security requirements and did not process or acknowledge insecure messages after security activation. 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. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) NAS, despite the fact that 5G-AKA had already been completed. According to the 3GPP 5G security standards (TS 33.501), after the 5G-AKA procedure, 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 standard, which mandates that the UE should ignore or reject any NAS messages that are not protected after security has been activated, as responding to such messages could expose sensitive information or make the UE vulnerable to certain attacks. Therefore, the UE's action of not responding to the unprotected identity request was secure and compliant with the 5G standard. 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 successful 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 finished. Subsequently, the AMF sent a "Deregistration Request" message to the UE, which was transmitted as a plain (unencrypted) message but with a 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 between the UE and the AMF should be both integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The key point here is that the AMF sent a deregistration request in plain text, which is not compliant with the 3GPP security requirements; however, the focus is on the UE's actions. The UE, after receiving the deregistration request, responded with its own deregistration request, which is the expected behavior as per the standard. There is no indication that the UE sent any NAS message in plain text after security was established; its messages were sent after the security context was set up. Therefore, the UE's actions were in line with the 3GPP security requirements, as it did not send any unprotected NAS messages after 5G-AKA was completed and responded appropriately to the AMF's request. Secure
259	259	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 99 UE provided: No response The packet capture during the test using wireshark is: 0.5207638740539551 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.521324872970581 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Information element non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which is expected to be encrypted and integrity protected as per 3GPP standards once security has been established. The AMF then responded with a GMM Status message, indicating a 5GMM cause value of 99 ("Information element non-existent or not implemented"), and crucially, this message was sent in plain (unencrypted) form. According to 3GPP TS 24.501, after security mode is established (i.e., after 5G-AKA), all subsequent NAS messages, including status messages, must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) NAS message after security activation, is required by the standard to discard the message and not respond to it. In this test, the UE did not respond to the unprotected GMM Status message, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by the UE. Therefore, the UE's action in this scenario was secure. 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 NAS security procedures should have been established and subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent a "5GMM Status" message with cause 101 ("Message not compatible with the protocol state") in plain (unencrypted and unprotected) form. Upon receiving this unprotected message, the UE responded by sending a "Deregistration Request (UE originating)" to the AMF. According to the 3GPP 5G standard (TS 24.501), after security mode is established, the UE must ignore any NAS messages received in plain (unprotected) form, except for a few exceptions (such as Service Request and Deregistration Accept). The correct and secure behavior for the UE, upon receiving a plain "5GMM Status" message after security activation, would be to ignore the message and not act upon it. In this case, the UE instead initiated a deregistration procedure, which is not compliant with the standard and could be exploited by an attacker to force the UE to deregister by sending unauthenticated messages. Therefore, the UE's action in this scenario was insecure, as it did not adhere to the security requirements of the 5G standard and responded to an unprotected message in a way that could compromise service availability. 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 the 5G-AKA authentication procedure, the UE initiated a service request by sending an UplinkNASTransport message to the AMF. In response, the AMF sent a Security Mode Command message, which was protected (i.e., integrity protected and/or ciphered) using the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection), and included the ABBA parameter. However, the UE did not respond to the Security Mode Command, and no further messages were sent from the UE. According to the 3GPP 5G standard, after receiving a Security Mode Command, the UE is expected to verify the integrity of the message, apply the negotiated security algorithms, and 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 proceed with the security context activation, which is a deviation from the expected secure behavior. This lack of response could expose the session to potential security risks, such as denial of service or failure to establish a protected NAS communication channel. 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 to the AMF, which is a standard step to initiate or resume a session. The AMF then responded with a Security Mode Command, but crucially, this command was sent as a plain (unencrypted and unauthenticated) NAS message, with the ciphering algorithm set to 5G-EA0 (null ciphering) and the integrity algorithm set to 128-5G-IA2. According to the 3GPP 5G standard, after authentication, the Security Mode Command is used to establish NAS security (ciphering and integrity protection) between the UE and the AMF. The Security Mode Command itself is allowed to be sent in plain text, but the expectation is that the UE should only accept security algorithms that provide actual protection (i.e., not 5G-EA0 for ciphering, except in specific, limited scenarios such as emergency services). In this test, the AMF proposed null ciphering (5G-EA0), and the UE did not respond to the Security Mode Command. This lack of response indicates that the UE refused to proceed with insecure security settings, as accepting null ciphering would expose user data and signaling to potential interception and manipulation. By refusing to respond, the UE adhered to the security requirements of the 5G standard, which mandates that UEs should not accept insecure security configurations except in well-defined exceptional cases. Therefore, the UE's action was secure. 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 (specifically, a PDU Session Establishment Request) to the AMF. 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) form. According to the 3GPP 5G standard (TS 24.501), after 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 certain reject messages sent before security activation). However, in this case, since 5G-AKA was completed, the expectation is that the Registration Reject should have been protected. The UE, upon receiving an unprotected Registration Reject after security context establishment, did not respond further, which aligns with the 3GPP security recommendations: the UE should ignore unprotected messages that should have been protected, to prevent downgrade or spoofing attacks. Therefore, the UE's action—providing no response to an unprotected Registration Reject after 5G-AKA—was secure and compliant with the 5G standard. 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 the 5G-AKA authentication procedure, the UE sent an UplinkNASTransport message to the AMF, which is expected behavior as the UE proceeds with NAS signaling under the assumption that a secure context has been established. Subsequently, the AMF responded with a Registration Reject message, indicating a 5GMM Cause value of 6 (Illegal ME), 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, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where possible, encrypted to ensure confidentiality and authenticity. The UE, upon receiving a plain (unencrypted) Registration Reject message after security context establishment, did not respond further, which aligns with the 3GPP security requirements. The standard specifies that the UE should ignore or discard any NAS messages that are not integrity protected after security activation, as accepting such messages could expose the UE to security risks such as spoofing or denial of service. Therefore, the UE's lack of response to the unprotected Registration Reject message demonstrates correct and secure behavior as per the 5G standard. 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. The AMF, under test control, responded with a new authentication request message that was sent in plain (unencrypted) form, even though a native security context had already been established (as indicated by ngKSI_TSC: Native security context and ngKSI_KSI: 5). Upon receiving this unexpected authentication request, the UE replied with an "Authentication failure (ngKSI already in use)" message, indicating that it recognized the ngKSI (Key Set Identifier) was already in use and that a new authentication procedure was not appropriate or necessary. According to the 3GPP 5G security standards, once a security context is established, further NAS messages should be protected, and the UE should not accept a new authentication request for an already active security context. The UE's response demonstrates that it correctly detected a protocol anomaly and refused to proceed with a potentially insecure or replayed authentication procedure, thereby protecting itself from possible security threats such as replay or downgrade attacks. This behavior aligns with the security requirements of the 5G standard, as the UE did not accept an insecure or out-of-sequence authentication request. 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 to the AMF, which is expected behavior as the UE proceeds with further NAS signaling (such as a PDU session establishment request). The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form. According to the 3GPP 5G security standards, after the completion of 5G-AKA, both the UE and the network should establish NAS security (encryption and integrity protection) before exchanging further NAS messages. However, the Authentication Reject message is an exception in the standard: per 3GPP TS 24.501, section 9.11.3.3, the UE must accept an Authentication Reject message even if it is sent in plain (unencrypted) NAS, as this message is used to indicate that authentication has failed or is no longer valid, and the UE should not respond to it. In this test, the UE did not respond to the plain Authentication Reject message, which is the correct and secure behavior as per the standard, since responding could expose the UE to further attacks or protocol confusion. Therefore, the UE's action—providing no response to a plain Authentication Reject after 5G-AKA—aligns with 3GPP security requirements and does not introduce any security vulnerability. 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 (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent an Authentication Reject message to the UE, and this message was sent in plain (unencrypted) form. According to the 3GPP 5G standards, once 5G-AKA is completed, NAS security (encryption and integrity protection) should be activated for all subsequent NAS messages exchanged between the UE and the AMF. The Authentication Reject message is a security-critical message, and per 3GPP TS 24.501, after security mode is established, the UE should only accept such messages if they are integrity protected and, where applicable, encrypted. In this test, the UE did not respond to the plain (unencrypted) Authentication Reject message, which is the correct and secure behavior as per the standard. This prevents potential security attacks such as message injection or replay by ensuring that only protected messages are processed after security activation. Therefore, the UE's action in this scenario was secure. 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 procedure, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior as per the 3GPP 5G NAS protocol. Subsequently, the AMF sent a "Configuration Update Command" to the UE, and this message was marked as "Protected," but the security header was reported as "Unknown." Importantly, the UE did not respond to this message. According to the 3GPP 5G standards (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. If the UE receives a NAS message with an unknown or invalid security header, or if the message does not conform to the expected security protection (e.g., missing integrity protection or encryption), the UE is required 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 a downlink message with an unknown security header demonstrates that it correctly enforced the security requirements by refusing to process or acknowledge a potentially insecure or malformed message. Therefore, the UE's action was in line with the 3GPP security standards and protected the integrity of the communication. 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 the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior as per the 3GPP 5G NAS protocol. Subsequently, the AMF sent a "Deregistration Accept" message to the UE, but this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where required, encrypted to prevent interception or tampering. In this case, the UE did not respond to the unprotected "Deregistration Accept" message, which is the correct and secure behavior. The UE is expected to ignore or reject any NAS messages that are not properly protected after security activation, as accepting or acting on such messages could expose it to security risks such as spoofing or session hijacking. Therefore, the UE's action of not responding to the unprotected message aligns with the 3GPP security requirements and demonstrates secure behavior in this context. 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, after the initial NAS procedures, the UE sent an identity response to the AMF, and subsequently, the AMF issued another identity request, specifically requesting the IMEISV, in plain (unencrypted) NAS signaling. 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 protect sensitive information such as the IMEI or IMEISV and should not transmit these identifiers in plain text before NAS security is activated. 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, as sending such identifiers in the clear would expose the UE to privacy and security risks. Therefore, the UE's action of withholding the IMEISV until NAS security is established demonstrates adherence to 3GPP security guidelines and is considered secure behavior. 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 sent another Identity Request, specifically requesting the IMEI, in plain (unencrypted) NAS signaling. 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 send it in response to a plain (unencrypted) Identity Request before NAS security is activated. The UE's action of not responding to the AMF's plain Identity Request for the IMEI demonstrates compliance with the standard's security requirements, as it avoids exposing the IMEI over an unprotected channel. This behavior is considered secure because it prevents potential interception of the IMEI by unauthorized parties before a secure channel is 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, which was sent as a protected (encrypted or integrity-protected) NAS message. However, the 5G-AKA authentication procedure, which is required to establish NAS security (encryption and integrity protection), was not completed prior to this exchange. Despite this, the UE proceeded to send a Deregistration Request (UE originating) in uplink, which, according to the 3GPP 5G standard, should only be sent after NAS security has been established via 5G-AKA. Sending sensitive NAS messages, such as Deregistration Request, before completing 5G-AKA means these messages are sent unprotected, exposing them to potential interception or tampering. The 3GPP standard mandates that the UE must not send such messages in cleartext before security activation. Therefore, the UE's action of sending a Deregistration Request before 5G-AKA completion is a security flaw and does not comply with the 5G security requirements. Insecure

273	273	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11984086036682129 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12007284164428711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF immediately sent a deregistration request to the UE. Notably, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the security context necessary for NAS message encryption and integrity protection was not yet established. Despite this, the AMF sent the deregistration request as a protected (integrity protected and ciphered) message, which the UE did not respond to. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must only be applied after successful completion of the 5G-AKA procedure, as this is when the necessary security keys are derived and shared between the UE and the network. Since the UE did not respond to a protected message sent before security context establishment, it correctly followed the 3GPP standard by refusing to process or respond to a message that was inappropriately protected. This behavior prevents potential security vulnerabilities that could arise from processing protected messages without a valid security context. 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 procedure was not yet completed, meaning that the NAS security context (encryption and integrity protection keys) had not been established. Immediately after receiving the authentication response, the AMF sent a deregistration request to the UE, which was marked as "integrity protected" in the security header. According to the 3GPP 5G standard, NAS messages should only be integrity protected and/or encrypted after the successful completion of the 5G-AKA procedure, when the security context is established. Since the 5G-AKA was not completed, the UE had not yet derived the necessary keys to verify or process integrity-protected messages. The UE did not respond to the deregistration request, which is the correct and secure behavior, as it should not process or accept protected messages before the security context is in place. This prevents potential security vulnerabilities, such as accepting spoofed or manipulated messages before mutual authentication and key agreement are completed. Therefore, the UE's action in not responding to the protected deregistration request before 5G-AKA completion aligns with 3GPP security requirements and demonstrates secure behavior. 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 standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is required to establish security context and enable encryption and integrity protection for NAS messages—the AMF responded with a DownlinkNASTransport message containing a Deregistration Request (UE terminated) marked as "Illegal ME." Notably, this downlink message from the AMF was sent with a security header indicating it was both integrity protected and ciphered, even though the 5G-AKA had not yet been completed and thus no security context should have been established. The UE, upon receiving this protected message without an established security context, did not respond. According to the 3GPP 5G standard, a UE must ignore any NAS message that is integrity protected and/or ciphered if a security context has not yet been established (i.e., before 5G-AKA is completed), as the UE would not have the necessary keys to process such messages. By not responding to the protected deregistration request, the UE correctly followed the 3GPP security procedures, thereby preventing potential security vulnerabilities such as replay or spoofing attacks. Therefore, the UE's action in this scenario was secure. 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, after the initial NAS procedures, the UE sent an Identity Response to the AMF, which then replied with a Security Mode Command. Notably, the Security Mode Command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for encryption and integrity protection had not been established between the UE and the network. According to the 3GPP 5G standard, the UE should only accept a Security Mode Command if it is received after successful authentication and if it is properly protected (i.e., integrity protected and, if required, encrypted). Since the Security Mode Command was sent in plain text before authentication was completed, the UE correctly did not respond to this message, thereby preventing a potential security risk such as a downgrade or man-in-the-middle attack. This behavior aligns with the security requirements of the 5G standard, as the UE must not process security-related commands before a secure context is established. Therefore, the UE's action in this scenario was secure. 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, the UE and AMF were engaged in NAS communication as part of the 5G standalone authentication and security procedures. The UE sent an Identity Response message to the AMF, which is a normal step prior to authentication. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is required to establish NAS security keys for integrity and ciphering—the AMF sent a Configuration Update Command to the UE. This downlink message was marked as "integrity protected" (i.e., with a security header indicating integrity protection), but since 5G-AKA was not yet completed, the necessary NAS security context (keys) had not been established. According to 3GPP standards (TS 24.501), the UE must not accept or process NAS messages that are integrity protected or ciphered before the security context is established, as this would expose the UE to potential security risks (e.g., replay or spoofing attacks). In this test, the UE did not respond to the AMF's protected Configuration Update Command, which is the correct and secure behavior as per the standard, since it had not yet established the required security context. By refusing to process or respond to a protected message before security activation, the UE demonstrated compliance with 3GPP security requirements. 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 sent in plain NAS as the 5G-AKA authentication and key agreement had not yet been completed. The AMF, under test control, then sent a Configuration Update Command to the UE, also in plain NAS (unencrypted), which is not standard-compliant because, according to 3GPP specifications, configuration update commands should only be sent after security context establishment (i.e., after 5G-AKA is completed and NAS security is activated). Upon receiving this unexpected and potentially insecure plain configuration update command, the UE did not process the command but instead immediately initiated a Deregistration Request, effectively aborting the session. This behavior demonstrates that the UE did not accept or act upon a sensitive command sent without NAS security protection, as required by the 3GPP 5G security standards. By refusing to process the configuration update command in the absence of an established security context, the UE protected itself from a possible security breach or protocol misuse. Therefore, the UE's action was secure and in line with 3GPP security requirements. 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 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 security context and enable encryption and integrity protection for NAS messages—the AMF responded with a deregistration accept message. Notably, this downlink message from the AMF was sent as "protected," even though the security context had not yet been established. The UE, upon receiving this protected deregistration accept message before security activation, did not respond. According to the 3GPP 5G standard, the UE should only process protected NAS messages after the security context is established via 5G-AKA. If a protected message is received before this point, the UE is expected to ignore it or treat it as invalid, as it cannot verify its integrity or decrypt it. By not responding to the protected deregistration accept message before security activation, the UE correctly adhered to the 3GPP security requirements, thereby preventing potential security vulnerabilities such as spoofing or denial-of-service attacks that could arise from processing unauthenticated messages. Therefore, the UE's action in this scenario was secure. 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 security context and enable encryption and integrity protection for NAS messages—the AMF responded with a deregistration accept message that was protected (i.e., sent as if security had already been established). The UE, upon receiving this protected deregistration accept message before any security context was in place, did not respond. According to the 3GPP 5G standard, the UE should only process protected NAS messages after the 5G-AKA procedure has been successfully completed and a security context is established. If a protected message is received before this point, the UE is expected to ignore it or treat it as invalid, since it cannot verify its authenticity or integrity. The UE's lack of response in this scenario demonstrates correct and secure behavior, as it did not process or acknowledge a protected message sent prematurely, thereby preventing potential security vulnerabilities such as replay or spoofing attacks. 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 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 a security context for encryption and integrity protection had not been established between the UE and the network. Despite this, the AMF sent a configuration update command to the UE, and this message was protected with integrity and ciphering using a "new security context" (security header type 4). According to the 3GPP 5G standard, user and signaling messages should only be encrypted and integrity protected after the successful completion of the 5G-AKA procedure, which establishes the necessary security keys. Since the UE had not yet completed 5G-AKA and therefore did not have the required security context, it did not respond to the protected configuration update command. This behavior aligns with the 3GPP standard, as the UE should not process or respond to protected NAS messages before security activation. By refusing to respond to a prematurely protected message, the UE avoided a potential security risk where an attacker could attempt to force the use of an unestablished or invalid security context. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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, under test control, responded with a Configuration Update Command 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 at this point in the exchange. According to the 3GPP 5G security standards, 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. Since the AMF sent a protected message before 5G-AKA was completed, the UE, adhering to the standard, did not respond to this message. This lack of response indicates that the UE correctly refused to process a protected NAS message before security context establishment, thereby preventing potential security vulnerabilities such as replay or downgrade attacks. Therefore, the UE's action was in line with 3GPP security requirements and demonstrated secure behavior in this scenario. 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 InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a DownlinkNASTransport message carrying a Service Accept, which was sent as a protected (encrypted and integrity-protected) NAS message. However, the 5G-AKA authentication procedure, which is required to establish NAS security context (encryption and integrity protection keys), had not yet been completed at this point in the exchange. According to the 3GPP 5G standard, the UE should not be able to process or respond to protected NAS messages before the 5G-AKA procedure is completed and security context is established. The UE, in this case, did not respond to the protected Service Accept message from the AMF, which is the correct and secure behavior as per the standard, since it had not yet established the necessary security context to decrypt or verify the message. Therefore, the UE's action of not responding to the protected message before 5G-AKA completion aligns with 3GPP security requirements and prevents potential security vulnerabilities. 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 sent as a protected (encrypted or integrity-protected) NAS message, even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G standard, 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 would not have the required keys to decrypt or verify the integrity of the protected Service Accept message. The UE, upon receiving this prematurely protected message, responded by sending a Deregistration Request (UE originating), effectively aborting the registration process. This behavior aligns with 3GPP security requirements, as the UE should not accept or process protected NAS messages before security context establishment, and should instead terminate the procedure to prevent potential security risks. Therefore, the UE's action was 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) (5) (PLMN established) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on 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 registration. However, the AMF then sent a Deregistration Request message to the UE, and this message was sent with a security header indicating it was both integrity protected and ciphered. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) can only be applied after the 5G-AKA authentication and key agreement procedure is successfully completed, as this is when the necessary security context is established between the UE and the network. In this test, the 5G-AKA procedure was not completed, meaning the UE and AMF had not yet established the keys required for secure NAS message protection. The UE, upon receiving a protected (integrity and ciphered) NAS message before security context establishment, did not respond to the message. This behavior aligns with the 3GPP standard, which specifies that the UE should discard or ignore protected NAS messages if security has not been activated. Therefore, the UE's action of not responding to the protected Deregistration Request before 5G-AKA completion was secure and compliant with the 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) (97) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on 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 (encryption and integrity protection) was not yet established. The AMF, under test control, responded with a protected (i.e., integrity protected and/or encrypted) GMM status message with a 5GMM cause value of 98 ("Message type not compatible with the protocol state"). According to 3GPP standards (TS 24.501), before 5G-AKA is completed, the UE should not accept or process protected NAS messages, as the security context is not yet established and the keys required for protection are not available. The UE, in this case, did not respond to the protected GMM status message from the AMF, which is the correct and secure behavior as per the standard. This prevents potential security vulnerabilities such as replay or downgrade attacks before mutual authentication and key agreement are completed. Therefore, the UE's action of not responding to the protected message before 5G-AKA was completed is compliant with 3GPP security requirements and demonstrates secure behavior. 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 a protected (integrity-protected and/or ciphered) NAS message. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that the security context for NAS message protection (encryption and integrity protection) was not yet established between the UE and the AMF. According to the 3GPP 5G standard (TS 24.501), the UE should only process protected NAS messages after a security context has been established via 5G-AKA. If a protected NAS message is received before 5G-AKA completion, the UE is required to discard the message and not respond, as it cannot verify the integrity or decrypt the message without the security context. In this test, the UE did not respond to the protected GMM status message sent before 5G-AKA was completed, which is the correct and secure behavior as per the 3GPP standard. This prevents potential security vulnerabilities such as replay or spoofing attacks before mutual authentication and key agreement are established. Secure
288	288	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0008118152618408203 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.20334196090698242 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 protected using integrity protection (128-5G-IA2) but did not use ciphering (5G-EA0, the null cipher algorithm), and indicated a new security context. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that the mutual authentication and key agreement necessary for establishing secure NAS encryption had not taken place. Upon receiving the Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, the UE should not accept a Security Mode Command that is protected with a new security context before the 5G-AKA procedure is completed, as the necessary keys for secure communication have not yet been established. The UE's action—responding with a status message indicating invalid mandatory information—demonstrates that it correctly detected the protocol violation and did not proceed with insecure communication. This behavior aligns with the security requirements of the 5G standard, as it prevents the establishment of a security context without proper authentication and key agreement. Therefore, the UE's action in this scenario was secure. 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, after the initial NAS procedures, the UE sent an Identity Response to the AMF, and subsequently, the AMF sent another Identity Request, specifically requesting the GUTI, in plain (unencrypted) NAS signaling. 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 be cautious about sending sensitive information, such as the GUTI or SUCI, in plain NAS messages before security activation. If the AMF requests an identity in plain NAS after the UE has already provided an identity response, the UE should not respond with sensitive information in the clear, as this could expose the UE to privacy and security risks (e.g., IMSI catching or tracking attacks). In this test, the UE did not respond to the AMF's second, plain Identity Request for the GUTI, which aligns with the security recommendations of the 3GPP standard to avoid exposing sensitive identifiers before NAS security is established. Therefore, the UE's action was secure and in compliance with the 5G security requirements. 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, 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) NAS. 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, the UE is required to protect sensitive information, such as the IMEISV, and should not transmit it in the clear before NAS security is activated. The UE, in this case, did not respond to the AMF's plain (unencrypted) identity request for the IMEISV, which aligns with the security requirements of the standard. This behavior prevents the exposure of sensitive device information over an unprotected channel, thereby mitigating the risk of interception or misuse by unauthorized parties. Therefore, the UE's action of withholding the IMEISV until NAS security is established is consistent with 3GPP security guidelines and demonstrates secure behavior. 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 to the AMF, and the AMF subsequently sent another identity request, specifically requesting the TMSI, in plain (unencrypted) NAS signaling. 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 its permanent and sensitive identities (such as SUPI/IMSI) and should not send them in plain text over the air; instead, it should only send such information after NAS security is activated. However, temporary identities like TMSI (or 5G-GUTI) are designed to be less sensitive and can be sent in plain text before security activation. In this test, the UE did not respond to the AMF's plain identity request for the TMSI. This behavior is more restrictive than required by the standard, as the standard allows the UE to send temporary identities in plain text before security is established. However, from a security perspective, the UE's refusal to respond in plain text does not violate the standard and, in fact, errs on the side of caution by not exposing any identity information before security is in place. Therefore, the UE's action can be considered secure, as it avoids the risk of identity exposure in an unprotected state, even if it is more conservative than strictly required by 3GPP. 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) (Re-authentication) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on 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), but the 5G-AKA (Authentication and Key Agreement) 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 encryption is only possible after successful completion of 5G-AKA. The UE did not respond to this deregistration request. According to the 3GPP 5G standards, the UE should only accept and process protected NAS messages (such as deregistration requests) after the security context is established, which occurs upon successful completion of 5G-AKA. Since the 5G-AKA was not completed, the UE had not yet established the necessary security context for NAS message protection and encryption. By not responding to the deregistration request sent before security activation, the UE correctly followed the 3GPP security guidelines, thereby preventing potential security vulnerabilities such as unauthorized deregistration or denial-of-service attacks. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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 the 5G-AKA authentication 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 integrity protected and ciphered according to 3GPP TS 24.501. However, the AMF (under test control) sent a "Configuration Update Command" as a plain (unencrypted and non-integrity protected) NAS message, which is not compliant with the 5G security requirements. The UE, upon receiving this plain NAS message after security activation, did not respond. According to 3GPP standards, the UE is required to ignore any plain NAS messages received after the security context is established, as accepting such messages could expose the UE to security risks such as replay or man-in-the-middle attacks. The UE's lack of response demonstrates correct and secure behavior, as it did not process or acknowledge the insecure message. Therefore, the UE's actions were in line with 3GPP security requirements and protected the integrity and confidentiality of the communication. 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 protected 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 been established at this point. According to the 3GPP 5G standard (TS 24.501), once the security mode is 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. This behavior aligns with the 3GPP security requirements, as the UE must reject or ignore any NAS messages that are not properly protected after security activation. By refusing to respond to an unprotected message post-security mode complete, the UE demonstrated secure behavior and adherence to 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 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to begin secure NAS communication. Immediately after, the AMF sent a "service reject" message with 5GMM Cause 111 (protocol error, unspecified), but crucially, this message was sent in plain (unencrypted) NAS, despite the security context having been established. According to 3GPP 5G standards (TS 24.501), once the security mode is complete, 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) NAS message after security activation, is required by the standard to discard the message and not respond, as accepting or processing such messages could 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 reject" message, which is the correct and secure behavior as per 3GPP specifications. This demonstrates that the UE adhered to the security requirements by refusing to process or acknowledge a message that violated the expected security procedures. 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 then sent an "authentication request" message to the UE in plain (unencrypted) form, despite the fact that, according to the 3GPP 5G standard, all subsequent NAS messages after the security mode procedure must be integrity protected and, if required, ciphered. The UE, upon receiving this plain (unencrypted) authentication request after security mode completion, did not respond. This behavior aligns with the 3GPP standard, which expects the UE to reject or ignore any NAS messages that are not properly protected after security mode is established, as accepting or responding to such messages could expose the UE to security risks such as replay or man-in-the-middle attacks. Therefore, the UE's action of not responding to the unprotected message was secure and compliant with the 5G security requirements. 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 NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent a "deregistration accept" message to the UE in plain (unencrypted) form, and the UE did not respond to this message. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after the security mode complete message), all subsequent NAS messages between the UE and the AMF must be protected by the agreed security algorithms. The UE is required to ignore any unprotected (plain) NAS messages received after security activation, as accepting such messages could expose the UE to security risks such as spoofing or replay attacks. In this test, the UE correctly ignored the unprotected "deregistration accept" message sent by the AMF after security activation, demonstrating compliance with the 3GPP security requirements. Therefore, the UE's action was secure. 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 begin secure NAS 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 standards, once the security context is established (i.e., after 5G-AKA and security mode complete), all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The "authentication reject" message, if sent after security mode complete, should be protected according to the established security context. The UE, upon receiving an unprotected (plain) "authentication reject" message after security mode complete, did not respond, which aligns with the 3GPP security requirements. This behavior prevents potential security vulnerabilities such as replay or injection attacks by ensuring the UE does not act on unauthenticated or unprotected messages after security has been established. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. 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 begin secure NAS communication. Immediately after, the AMF sent an "authentication reject" message to the UE, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard, once the security context is established (i.e., after 5G-AKA and 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) "authentication reject" message after security activation, did not respond. This behavior aligns with the 3GPP security requirements, as the UE is expected to ignore or silently discard any NAS messages that are not properly protected after security has been activated. By not responding to the unprotected message, the UE demonstrated secure behavior and adherence to the 5G standard, thereby preventing potential security vulnerabilities such as replay or injection attacks by unauthorized entities. 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 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 TMSI, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once NAS security is established (i.e., after the security mode complete), all subsequent NAS messages must be protected (encrypted and integrity protected). The UE, upon receiving an unprotected identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which states that the UE should ignore or discard any unprotected NAS messages received after security is activated, as responding to such messages could expose sensitive information to potential attackers. Therefore, the UE's action of not responding to the plain identity request after security mode complete demonstrates secure and standards-compliant behavior. Secure