UE Response Evaluation Report: Test time: 2025-07-18 11:04:10

SL	Test Name	Test content	Remark
1	1	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006918907165527344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE initiated a registration request to the AMF, the AMF responded with an identity request asking for the IMEI, sent in plain (unencrypted) NAS message format. The UE did not respond to this plain identity request. According to the 3GPP 5G security standard (TS 33.501), the IMEI is considered a sensitive identifier and should only be sent over a protected (encrypted and integrity-protected) NAS connection, which is established only after successful completion of 5G-AKA authentication and key agreement procedures. Since the 5G-AKA process was not yet completed, any response from the UE containing the IMEI in plain text would have exposed sensitive information and violated 3GPP security requirements. The UE's refusal to respond to the plain identity request demonstrates adherence to the standard and a secure behavior, as it avoided leaking the IMEI before security context establishment. Therefore, the action taken by the UE was secure. Secure
2	2	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0011980533599853516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2027890682220459 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage with 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 responded with an identity response containing the requested SUCI. Notably, this exchange occurred before the completion of the 5G-AKA (Authentication and Key Agreement) procedure, and the AMF's identity request was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, the initial NAS messages, including the registration request and identity request/response exchanges, are allowed to be sent in plain text prior to the establishment of a security context (i.e., before 5G-AKA is completed). The use of SUCI, which is a privacy-preserving, encrypted form of the subscriber's permanent identifier (SUPI), is specifically designed to protect subscriber identity even when sent in plain text over the air. Therefore, the UE's action—providing the SUCI in response to an unprotected identity request before security context establishment—is compliant with 3GPP standards and does not expose the permanent subscriber identity. This process is considered secure by design, as the SUCI cannot be used to directly identify the subscriber without the decryption key, which is not available to potential attackers on the air interface. 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, as expected during the NAS (Non-Access Stratum) communication procedure. The AMF, under test control, immediately responded with an Authentication Reject message, which was sent in plain (unencrypted) NAS format. According to the 3GPP 5G standard, NAS messages prior to the completion of 5G-AKA (Authentication and Key Agreement) are permitted to be sent in plain text, as mutual authentication and ciphering keys are not established until AKA is successfully completed. The critical security requirement is that the UE should not process or respond to any authentication reject messages unless they are received in the correct sequence and context, especially since a plain authentication reject could be an attack vector (e.g., a fake AMF attempting to prematurely terminate registration). In this case, the UE did not respond to the plain authentication reject message sent before authentication was complete. This behavior aligns with 3GPP security recommendations, which state that the UE should ignore unexpected or out-of-context plain NAS messages that could be forged. Therefore, the UE's action—providing no response to a plain authentication reject before 5G-AKA completion—was secure and compliant with the standard. Secure
4	4	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0012979507446289062 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20431208610534668 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an identity request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. At this stage, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to 3GPP standards (TS 33.501), it is expected and required that the UE responds to the AMF's identity request with a SUCI, which is a privacy-preserving, concealed version of the permanent identifier (SUPI). The SUCI is designed to be sent in the clear (plaintext) before authentication and key agreement are completed, specifically to protect the user's permanent identity from exposure over the air. Therefore, the UE's action of providing the SUCI in response to the identity request, even though the message was sent in plaintext, is compliant with 3GPP security requirements and does not expose sensitive information. The UE did not send the SUPI or any other unprotected permanent identity, and only responded with the SUCI as intended by the standard. Based on this, the UE's behavior in this interaction was secure according to the 5G standard. 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 NAS communication by sending an initial registration request to the AMF. The AMF, under test control, responded with a registration reject message using NAS plain (unencrypted) format and included a 5GMM cause code 111 (protocol error, unspecified). Since the 5G-AKA authentication and key agreement procedure had not yet been completed, no NAS security context was established, and all messages were exchanged in plain text as per 3GPP standards. Upon receiving the registration reject, the UE responded by sending a deregistration request (UE originating), also in plain text. According to the 3GPP 5G standards, until 5G-AKA is completed, all NAS messages are permitted to be sent unencrypted, and the UE is expected to handle registration reject messages even when security is not activated. The UE's response to deregister after receiving a registration reject is consistent with standard-compliant behavior, as it does not continue to attempt protected communication without a valid security context. Therefore, the UE's actions in this scenario were secure, as they adhered to the expected procedures defined by 3GPP for handling NAS signaling prior to security activation. 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, after the UE initiated a registration procedure by sending an initial registration request to the AMF, the AMF responded with a registration reject message indicating cause 22 (congestion). Notably, this registration reject message was sent in plain (unencrypted) text, which is expected since the 5G-AKA authentication and key agreement procedure had not yet been completed; thus, security context for encryption was not established. Upon receiving the registration reject, the UE responded with a deregistration request (UE originating), also in plain text, as no security context was available. According to the 3GPP 5G standard, until the 5G-AKA procedure is completed and security context is established, NAS messages (such as registration requests and rejects) are transmitted unprotected except for certain integrity protections in specific scenarios. The UE is expected to accept and process registration reject messages sent in plain text before authentication, and its subsequent action of sending a deregistration request is consistent with the standard. Therefore, the UE's behavior—processing the plain registration reject and responding with a deregistration request before any security context was available—is in line with 3GPP security requirements for this state of the protocol. The UE did not violate any security expectations, as it did not accept any network commands that would require an established security context, nor did it transmit sensitive information before authentication. Secure

7	7	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 00000000000000000000000000000000 AUTN: 32303030007f0000ee555cc720560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.203125 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE initiated registration with the AMF, the AMF responded with an authentication request message that was sent in plain (unencrypted) form, with suspicious values for critical authentication parameters such as RAND (all zeros) and ABBA (0000). According to the 3GPP 5G standard, the authentication procedure (5G-AKA) must be completed before any secure communication can be established, and the authentication vectors (such as RAND and AUTN) must be properly generated and unique for each authentication attempt. The UE, upon receiving a plainly transmitted authentication request with invalid authentication parameters, responded with an "Authentication failure (Non-5G authentication unacceptable)" message. This behavior aligns with the 3GPP security standards, which require the UE to reject authentication requests that do not meet security requirements, such as those with improperly formatted or insecure authentication vectors, or requests sent in plain text when security context is expected. By refusing to proceed with authentication under insecure conditions, the UE demonstrated correct and secure behavior, protecting itself from potential security attacks or protocol downgrades. Secure

8	8	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 313030300000000078742b94d4550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005857944488525391 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20240378379821777 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE initiated the registration process by sending an initial registration request, the AMF responded with an authentication request message that was sent in plain (unencrypted) text, as the 5G-AKA authentication procedure had not yet been completed. The authentication request from the AMF contained a zeroed AUTN, a non-random RAND, and ABBA set to 0000, indicating that the message was intentionally malformed or non-standard as part of the test. Upon receiving this, the UE did not proceed with authentication or respond with sensitive information; instead, it sent a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, the UE should not process or respond to authentication requests that are malformed or do not comply with the expected format, especially before security has been established. The UE's response, which was to reject the authentication attempt due to invalid information, aligns with secure behavior as it avoids processing potentially malicious or non-compliant messages and does not reveal any sensitive data. This demonstrates that the UE correctly implemented the security requirements by refusing to proceed with the authentication process under insecure or suspicious conditions. 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 5G User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After the initial NAS steps, the UE responded to an identity request from the AMF by sending an identity response. The AMF then sent another identity request, specifically requesting the Subscription Concealed Identifier (SUCI), and the UE responded accordingly. Importantly, these exchanges occurred before the completion of the 5G Authentication and Key Agreement (5G-AKA) procedure, meaning that the NAS security context had not yet been established and messages were transmitted in plain (unencrypted) form. According to the 3GPP 5G standards, it is expected and permissible for identity requests and responses (including SUCI) to be sent in plain NAS messages prior to the establishment of security, as the SUCI is designed to protect the subscriber's permanent identifier (SUPI) from exposure, even when sent without encryption. The UE did not send any sensitive identifiers (like the SUPI) in the clear, and only provided the SUCI as specified by the standard. Therefore, the UE's actions were in alignment with 3GPP security requirements for the pre-authentication phase, and did not expose sensitive information. 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, the UE completed the initial NAS procedures and responded with an Identity Response to the AMF. The AMF then sent an Authentication Request in plain (unencrypted) NAS, with the 5G-AKA authentication procedure not yet completed—meaning no NAS security context was established. The Authentication Request included parameters such as ABBA, RAND, AUTN, and a native security context identifier (ngKSI_KSI:2). Upon receiving this, the UE replied with an Authentication Failure message, specifying "ngKSI already in use." According to the 3GPP 5G security standard (TS 33.501), a UE should not accept a new authentication challenge for an ngKSI (NAS key set identifier) that is already in use, as this could indicate a replay attack or a security anomaly. By refusing to process the authentication and sending an Authentication Failure, the UE correctly protected itself from a potential security issue and prevented the establishment of a compromised or redundant security context. This behavior aligns with the 5G security requirements, as the UE did not proceed with authentication under suspicious circumstances and did not accept unprotected NAS messages for sensitive procedures after the initial steps. 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 5G User Equipment (UE) and the Access and Mobility Management Function (AMF) engaged in a NAS (Non-Access Stratum) communication sequence. The UE sent an Identity Response to the AMF, which is a standard message sent in cleartext before security activation, as the 5G-AKA (Authentication and Key Agreement) had not yet been completed. Following this, the AMF responded with a Service Reject message indicating "PLMN not allowed" (5GMM Cause: 11), also sent in plain (unencrypted) form. According to 3GPP 5G security standards, it is expected and allowed that initial NAS messages (including identity procedures and reject messages) are exchanged in plain text before authentication and security procedures are established. The UE, upon receiving the Service Reject, did not respond further, which is the correct behavior as the network has denied service and no further communication is warranted. Therefore, the UE's actions were consistent with 3GPP security requirements, as it did not attempt to send sensitive information before security activation and properly ceased communication after receiving the reject. Based on this analysis, the UE's behavior was secure. Secure

12	12	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03978896141052246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04010796546936035 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2456059455871582 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after completing initial NAS procedures, the UE sent an identity response to the AMF. The AMF, under tester control, then sent another identity request to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), and did so in plain (unencrypted) NAS messaging because the 5G-AKA authentication and key agreement procedure had not yet been completed. The UE responded to this plain identity request by providing another identity response. According to 3GPP 5G security standards, prior to the completion of 5G-AKA, NAS messages—including identity requests and responses—are not encrypted, as security context establishment has not yet occurred. The UE is expected to respond to identity requests from the AMF, even if they are in plain text, during this pre-authentication phase. Thus, the UE's actions conform to the expected behavior defined by the 3GPP standard, as it is not required or even able to encrypt NAS messages before authentication and key establishment. The UE did not behave insecurely, as it followed the protocol as designed for this stage of the connection setup. 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 the described security test, the UE first completed the necessary preliminary NAS steps and responded to an identity request from the AMF with an identity response. Immediately after, the AMF sent an authentication reject message to the UE, and this message was sent in plain (unencrypted) form. The UE, upon receiving this authentication reject, did not generate any further response. According to the 3GPP 5G standard, messages exchanged before the completion of the 5G-AKA (Authentication and Key Agreement) procedure, such as identity responses and authentication rejects, are expected to be sent in plain text since encryption and integrity protection are not yet established. Furthermore, the standard specifies that upon receiving an authentication reject, the UE should not proceed further with NAS procedures and should not respond, as this message indicates a failed authentication attempt. The UE’s behavior—sending the identity response in plain text before authentication is completed and not responding to the authentication reject—is fully compliant with the 3GPP 5G security procedures. Therefore, based on the standard and the actions taken, the UE’s response in this scenario was secure. 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) completed the initial NAS procedures up to sending an Identity Response to the Access and Mobility Management Function (AMF). Critically, the 5G Authentication and Key Agreement (5G-AKA) procedure, which establishes mutual authentication and sets up NAS security (encryption and integrity protection), was not completed at this point. Immediately after receiving the Identity Response, the AMF sent a Registration Reject message with cause value 22 (Congestion) in plain (unencrypted) NAS, and the UE did not respond further. According to the 3GPP 5G standard, NAS messages sent before the completion of 5G-AKA are allowed to be in plain text, as security context (keys for encryption and integrity) is not yet established. The UE's actions—sending the Identity Response in plain text and not responding further after receiving the Registration Reject—align with expected behavior as per the standard. The UE did not proceed to send any sensitive information or continue communication after the rejection, which would have been insecure. Therefore, given the stage of the NAS procedure and the absence of a security context, the UE's actions were appropriate and did not expose it to unnecessary risk. 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: 3030303030303030007844783aae550000 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, the UE first responded to an identity request from the AMF with an identity response, after which the AMF sent an authentication request to the UE. The authentication request from the AMF was sent as a plain (unencrypted) message and included suspicious or invalid parameters—specifically, the AUTN (Authentication Token) was all zeros, and the ABBA value was 0000, which is not standard. The UE, upon receiving this authentication request, replied with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G standard, the UE should only proceed with authentication if the authentication request is valid and meets the security requirements of 5G-AKA. The UE is expected to reject authentication attempts that do not conform to 5G security protocols, such as when receiving an invalid AUTN or a non-5G authentication request. By refusing to proceed with authentication under these circumstances, the UE is protecting itself from potential downgrade or replay attacks and ensuring that only secure, standard-compliant authentication is accepted. This behavior aligns with the security principles outlined in the 3GPP standard, demonstrating that the UE correctly identified and rejected a potentially insecure or malicious authentication attempt. 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 completing 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. Subsequently, the AMF sent a Security Mode Command to the UE, which is intended to establish NAS security by activating ciphering and integrity protection algorithms for future NAS messages. However, the Security Mode Command was sent as a plain (unencrypted and unauthenticated) NAS message, which is correct and compliant with 3GPP specifications (TS 24.501, section 9.2.2.2), as security context has not yet been established at this point. The UE did not respond to the Security Mode Command. According to the 3GPP standard, the UE should respond with a Security Mode Complete message, which is the first NAS message to be protected by the new security context (i.e., encrypted and integrity protected). By not responding, the UE avoided sending any NAS messages without security, which is a conservative and secure approach, as it prevented the possibility of sending sensitive information in the clear or before security was established. Therefore, based on the 3GPP security procedures, the UE's action was secure, as it did not proceed with unprotected communication and did not violate the protocol by sending a protected message before the security context was activated. 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) completed the initial NAS procedures and sent an Authentication Response to the Access and Mobility Management Function (AMF). However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is necessary for establishing ciphering and integrity protection of NAS messages—the AMF sent a Service Reject message with 5GMM Cause 111 ("Protocol error, unspecified") in plain (unencrypted) form. The UE, upon receiving this unprotected Service Reject message, did not respond further. According to the 3GPP 5G standards, specifically TS 24.501, the UE is required to ignore and not process any NAS messages that are not integrity protected after the security context is established. However, before the 5G-AKA is completed, there is no security context, so messages are sent in plain text and the UE must still process them. In this case, since the 5G-AKA was not completed, the UE's action of not responding to an unprotected Service Reject message is compliant with the standard, as the UE is not required to respond to such a message and should avoid taking unauthorized actions. Therefore, the UE's behavior in this scenario is considered secure and adheres to the 3GPP specifications. 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 the described test scenario, after completing initial NAS procedures, the UE sent an authentication response to the AMF. However, before the 5G-AKA authentication and key agreement procedure was completed, the AMF issued an identity request for the SUCI (Subscription Concealed Identifier), and the UE responded with its identity. Notably, this identity request from the AMF was sent in plain (unencrypted) NAS signaling, as the security context had not yet been established due to the incomplete 5G-AKA procedure. According to the 3GPP 5G standard, specifically TS 33.501, the UE must not send any sensitive identifying information (such as SUPI) in plain NAS messages; only the SUCI, which is a privacy-preserving, encrypted version of the SUPI, may be sent before security activation. In this case, the UE responded to the plain identity request with its SUCI, which is considered privacy-preserving and intended for use before NAS security is activated. Therefore, based on the 3GPP standard, the UE's action was secure, as it did not expose sensitive identifiers in the clear and followed the expected procedure for this stage of the security setup. 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 the described 5G standalone security test, after successfully completing the 5G-AKA authentication procedure, the UE responded to the AMF's authentication challenge with an authentication response. Subsequently, the AMF 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. Crucially, the Security Mode Command was sent as "protected" and indicated a new security context, but the ciphering algorithm selected was 5G-EA0, which provides no encryption and thus does not protect the confidentiality of user data. Upon receiving this command, the UE rejected the security mode with an "unspecified" reason, as observed in the Security Mode Reject message. According to the 3GPP 5G security standards (TS 33.501), while 5G-EA0 is defined for certain exceptional scenarios (e.g., emergency calls or lawful interception), its use in normal operation is discouraged because it does not provide confidentiality. The UE's rejection of the security mode when asked to operate with no encryption (EA0) after authentication is a prudent security behavior, as it avoids downgrading to an insecure configuration that could expose user data. Therefore, the UE's action aligns with the intent of the 5G security standards to prevent the establishment of insecure ciphering and demonstrates a secure and standards-compliant response to the AMF's request. 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 the described 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, as the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed. The UE then proceeded to immediately send another Authentication Response to the AMF. According to the 3GPP 5G security architecture, all NAS signaling messages exchanged between the UE and the AMF before the successful completion of 5G-AKA are permitted to be sent in plain text, as encryption and integrity protection are only established after successful mutual authentication and key agreement. However, the critical aspect here is the UE's behavior when receiving an unexpected or repeated Authentication Request after already responding to a previous one. The 5G standard (e.g., 3GPP TS 24.501, TS 33.501) expects the UE to verify the freshness and validity of authentication challenges (RAND, AUTN) and to avoid responding to replayed or malformed authentication requests, as this could be indicative of a replay or downgrade attack. In this test, the UE sent an Authentication Response to a repeated Authentication Request with the same parameters (RAND, AUTN, ABBA) as before, without detecting or rejecting the replay. This behavior is not compliant with the 5G security requirements, as it exposes the UE to potential replay attacks and undermines the integrity of the authentication process. Therefore, the UE's action of responding to a repeated authentication challenge without proper validation is considered insecure by 3GPP standards. 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 the test scenario, the UE and AMF engaged in the NAS authentication procedure typical of 5G-AKA. After the UE sent an authentication response, the AMF (under test control) sent another authentication request to the UE, but this request was sent as a plain (unencrypted) message, and the 5G-AKA procedure had not yet 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 (MAC failure)" message, indicating that it detected a mismatch or integrity issue with the received message. According to the 3GPP 5G security standards, the UE is required to verify the integrity (Message Authentication Code, or MAC) of authentication requests and reject them if the MAC is invalid or the message is otherwise suspicious, especially if the 5G-AKA procedure is not yet completed and messages are sent in cleartext. The UE's action to reject the authentication request due to MAC failure—rather than proceeding insecurely—demonstrates that it correctly enforced the expected security checks as per 3GPP standards, protecting itself from potential replay, manipulation, or downgrade attacks during the critical authentication phase. Therefore, the UE's behavior in this test was secure. 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: 31313131313131313310057a1d8550000 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, after completing the initial NAS steps, the UE sent an authentication response to the AMF, which then responded with another authentication request message sent in plain (unencrypted) form. At this point, the 5G-AKA procedure had not been completed, which is a prerequisite for establishing a secure context and encrypting subsequent NAS messages. The UE, upon receiving a plain (unencrypted) authentication request after already having sent an authentication response, replied with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G standards, the UE is expected to reject any authentication procedure that does not comply with 5G security requirements, especially when messages are sent in plain after a security context should be established or if non-5G authentication methods are attempted. The UE's refusal to proceed with an unencrypted or non-standard authentication process demonstrates adherence to security requirements, as it avoids exposing sensitive information or proceeding with potentially insecure exchanges. Therefore, the UE's behavior aligns with secure practices as outlined by 3GPP for 5G systems. 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 initiated the NAS security setup by sending a Security Mode Command to the UE, specifying the use of the null ciphering algorithm (5G-EA0) and an integrity protection algorithm (128-5G-IA2), with the message protected by integrity using a new security context. Upon receiving this command, the UE responded with a Security Mode Reject, indicating "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, the use of the null ciphering algorithm (5G-EA0) means that user data would not be encrypted over the air interface, which poses a significant security risk unless there is a justified reason (such as emergency services or device limitations). The standard expects the UE to reject security mode commands that do not meet its security policy, especially if a secure ciphering algorithm is not mandated or if the configuration is otherwise unacceptable. The UE’s action to reject the security mode command under these circumstances aligns with the security principles of the 5G standard, as it avoids establishing a connection with insufficient protection. Therefore, the UE’s response was a secure action in compliance with 3GPP requirements. 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 completing the initial NAS procedures, the UE sent an Authentication Response to the AMF, indicating it had received and processed an earlier Authentication Request. However, the AMF then sent another Authentication Request, which was transmitted in plain (unencrypted) form, as the 5G-AKA procedure had not yet been completed—meaning that security context establishment and NAS message encryption had not yet been activated. The UE responded to this second Authentication Request with another Authentication Response, also in plain text. According to the 3GPP 5G standard, NAS message encryption and integrity protection are only activated after successful completion of the 5G-AKA procedure, which establishes the security context. Until then, messages are sent in plain text by design. However, the UE's action of accepting and responding to a second, unexpected Authentication Request after already sending an Authentication Response is questionable. Normally, the UE should expect the next step to be Security Mode Command, not a repeated Authentication Request, unless the previous authentication failed or was rejected. Responding to repeated authentication challenges without verifying their context could expose the UE to replay or downgrade attacks, especially since the messages are unprotected at this stage. Therefore, while the UE's use of plain messages before 5G-AKA completion is compliant with the standard, its acceptance and response to a repeated Authentication Request without additional checks indicates a lack of robustness against certain attack scenarios, and thus is not fully secure as per best security practices outlined by 3GPP. 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 unprotected NAS steps, it responded to an authentication challenge with an authentication response. The AMF, under the tester's control, then sent an Authentication Reject message to the UE in plain (unencrypted) form, as the 5G-AKA procedure had not yet been completed and security context was not established. According to the 3GPP 5G standards (TS 24.501), the Authentication Reject message is specifically allowed to be sent in unprotected (plain) form when 5G-AKA has not been completed, since at this point there is no established NAS security context to provide encryption or integrity protection. Upon receiving this Authentication Reject, the UE did not proceed with any further NAS procedures, nor did it attempt to establish a security context; instead, it responded with a Deregistration Request, effectively aborting the registration process and ceasing further communication. This behavior aligns with 3GPP security requirements, which mandate that the UE should not proceed with any sensitive operations or accept further commands from the network if authentication fails or is explicitly rejected. By refusing to continue and deregistering, the UE protected itself from potential impersonation or downgrade attacks that could occur if it acted on unauthenticated or unprotected messages. Therefore, the UE's actions were in accordance with the 5G security standards and were secure. Secure

26	26	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15973997116088867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15994787216186523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.3668229579925537 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it had established the agreed-upon security context (keys for integrity and ciphering). Shortly after, the AMF sent a deregistration request to the UE, which was correctly protected with both integrity and ciphering, as indicated by the security header (2). The UE then responded with a deregistration accept message, signaling compliance with the deregistration procedure. According to the 3GPP 5G standards, after the security context is established via 5G-AKA and Security Mode Command/Complete, all subsequent NAS messages exchanged between the UE and AMF must be integrity protected and, where required, ciphered. The packet capture shows that the deregistration request from the AMF was indeed protected, and the UE responded as expected, only after security activation. Since the UE did not accept or process any unprotected NAS messages after security setup, and only responded to a valid, protected deregistration request, its actions are consistent with the security requirements outlined by 3GPP. Therefore, the UE's behavior in this scenario demonstrates adherence to the expected security procedures for NAS communication in 5G standalone mode. 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 Authentication and Key Agreement (5G-AKA), the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated NAS security algorithms and was ready for protected NAS communication. The AMF then sent a "deregistration request" as a downlink NAS message, which was integrity protected and ciphered, as indicated by the security header (2), ensuring that the message was both encrypted and authenticated according to 3GPP standards. The UE responded with a "deregistration accept" message, also sent as an uplink NAS message, which would similarly be protected under the established NAS security context. The packet capture confirms that after 5G-AKA completion, all subsequent NAS messages (including the deregistration exchange) were transmitted with the appropriate security protections in place. According to 3GPP TS 24.501 and TS 33.501, it is mandatory for the UE to only accept and respond to NAS messages that are properly protected after the security context is established, and in this test, the UE adhered to this requirement by only responding to a protected deregistration request with a protected accept message. Therefore, the actions taken by the UE were consistent with the security requirements of the 5G standard, and there was no indication of insecure behavior or protocol violation. 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 successfully completing the 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security parameters. Unexpectedly, the AMF then sent another "security mode command" message, which was protected and specified the use of ciphering algorithm 128-5G-EA2 and integrity algorithm 5G-IA0 (null integrity). The UE responded by rejecting this security mode command, sending a "security mode reject" message with an unspecified reason. According to 3GPP standards, once the security context is established and acknowledged by the UE (via "security mode complete"), the AMF should not initiate a new security mode command unless there is a valid context change or error. Additionally, the use of a null integrity algorithm (5G-IA0) is considered insecure, as it does not provide integrity protection for NAS messages, which is against recommended security practices. The UE's action to reject the security mode command—especially one proposing null integrity after a security context was already established—is a secure and standards-compliant response, as it prevents the downgrading of security and protects against potential attacks or misconfigurations. Therefore, the UE's behavior in this scenario demonstrates secure handling of the security procedures as outlined by 3GPP. 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 successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the proposed security algorithms and the establishment of a new security context. However, the AMF subsequently sent another "security mode command" message to the UE, this time protected using null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, and indicated that the message was "integrity protected with new security context." Upon receiving this command, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. According to 3GPP 5G security standards (TS 33.501), after the security context is established, it is mandatory for the UE and the network to use strong (non-null) ciphering and integrity algorithms to protect NAS signaling; the use of null algorithms is only allowed in specific, limited scenarios (such as emergency services or early registration) and should not be used once a security context is in place. The UE correctly rejected the insecure security mode command that attempted to downgrade the security algorithms to null after a security context had already been established, thereby preventing a potential security downgrade attack. This behavior is compliant with the 3GPP security requirements and demonstrates proper protection against downgrade attacks. 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 completing the 5G-AKA authentication and key agreement 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 then sent another "Security Mode Command" message, which is unusual because, according to 3GPP standards, the Security Mode Command should precede the Security Mode Complete, not follow it. The Security Mode Command is used by the AMF to instruct the UE to activate the negotiated security algorithms, and only after receiving this command should the UE respond with a Security Mode Complete. In this test, the UE, after already sending a Security Mode Complete, responded again with another Security Mode Complete message upon receiving the subsequent (and out-of-order) Security Mode Command from the AMF. This behavior is problematic because the UE should not accept or respond to a redundant or out-of-sequence Security Mode Command after security context establishment. According to 3GPP TS 24.501, the UE must ignore such messages to prevent replay or downgrade attacks. By responding to a Security Mode Command after already completing the procedure, the UE exposes itself to potential security vulnerabilities, such as replay attacks or manipulation of the security context. Therefore, the action taken by the UE in this scenario does not align with the security expectations of the 5G standard and is considered insecure. Insecure

31	31	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.1600170135498047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16026687622070312 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36418795585632324 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone UE successfully completed the 5G-AKA authentication and key agreement procedure, which is a prerequisite for establishing a secure NAS communication channel. After this, the UE sent a Security Mode Complete message to the AMF, indicating acceptance of the negotiated security algorithms (5G-EA4 for ciphering and 5G-IA0, which is the null algorithm, for integrity protection). The AMF then sent a Security Mode Command message, which was protected as indicated by the security header ("Integrity protected with new security context (3)"). Following this, the UE sent a Deregistration Request. According to the 3GPP 5G security standard, after 5G-AKA completion, all subsequent NAS messages should be both integrity protected and ciphered, except for certain cases such as when a null integrity algorithm is negotiated. Here, the negotiated integrity algorithm is 5G-IA0 (null), meaning that integrity protection is not applied to the NAS messages, even though the ciphering algorithm (5G-EA4) is non-null and should provide encryption. This configuration is not recommended in real-world deployments, as it exposes the system to potential integrity attacks, but it is allowed by the standard and may be used for testing or specific scenarios. The UE's actions—accepting a null integrity algorithm and proceeding with deregistration—align with the 3GPP standard, as the standard permits the use of 5G-IA0 if both the network and UE agree. However, from a security perspective, this leaves the communication vulnerable to modification attacks. Therefore, while the UE's actions are compliant with the 3GPP standard, they are not secure by best security practices. **Insecure**

32	32	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.1595141887664795 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15984320640563965 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	The interaction between the UE and the AMF began with the successful completion of the 5G-AKA authentication, which is a prerequisite for establishing a secure NAS communication channel. Following this, 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 communication. Unexpectedly, the AMF then sent another "security mode command" message, which was already integrity protected and ciphered, as indicated by the security header and the selected algorithms (5G-EA4 for ciphering and 128-5G-IA3 for integrity). According to the 3GPP 5G standard, once the security mode is completed and the UE has acknowledged with "security mode complete," the NAS security context is established, and the UE should not expect another security mode command unless the context is being re-established or updated. The UE, upon receiving a redundant security mode command after completion, did not respond, which aligns with the standard's expectation that such a message is out of sequence or potentially malicious. The UE's refusal to respond prevents potential downgrade or replay attacks and upholds the integrity of the security context. Therefore, based on the adherence to the 3GPP protocol and the secure handling of unexpected or out-of-sequence messages, the UE's action 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: 0.16021108627319336 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1606900691986084 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Illegal ME) 0.36391305923461914 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	During this security test of a 5G standalone User Equipment (UE), after completing the 5G-AKA authentication and key agreement process, the UE sent a Security Mode Complete message, indicating it had accepted the security parameters and was ready to begin protected NAS communication. Immediately after, the AMF (which was under tester control) sent a protected 5GMM Status message with a cause value of 6, which corresponds to "Illegal ME" (Mobile Equipment). In response to this, the UE sent a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G standard, once 5G-AKA is completed and security mode is accepted, all subsequent NAS messages must be integrity protected and, where required, encrypted. The packet capture confirms that the AMF’s status message was protected, and the UE’s deregistration request was also sent after security was activated. The UE’s action—sending a deregistration request in response to receiving a protected 5GMM Status message indicating "Illegal ME"—is in line with expected behavior: upon receiving a status message indicating an abnormal situation (such as illegal equipment), the UE should deregister itself to prevent further unauthorized network access. Therefore, the UE's actions were in accordance with 3GPP security requirements: it only reacted to a protected message after security activation, and its response helps prevent potential misuse or continued network access by a device flagged as illegal. Based on this analysis, the UE's actions were secure. 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, indicating that both integrity and ciphering protections were established for subsequent NAS messages. The AMF, under tester control, then issued a "deregistration request" to the UE, which was received as an integrity protected and ciphered (security header type 2) downlink message. The UE responded with a "deregistration accept" message, also transmitted as an uplink NAS message. According to 3GPP standards (TS 24.501), once 5G-AKA is complete and security mode is established, all subsequent NAS signaling—including deregistration procedures—must be protected by integrity and ciphering. The UE's actions adhered to this requirement: it accepted and responded only to a properly protected deregistration request and sent its response under the established security context. Thus, the UE followed the expected security procedures as per the 5G NAS protocol and did not accept or process any unprotected messages after security activation. Based on this analysis, the UE's communication in this scenario 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, 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 NAS security algorithms and was ready to proceed with protected (encrypted and integrity-protected) NAS signaling. Subsequently, the AMF sent a "service accept" message to the UE, which, according to the test summary, was protected (i.e., encrypted and integrity-protected as per 3GPP requirements). After receiving the protected "service accept" message, the UE did not respond further. According to the 3GPP 5G NAS protocol, after the security context is established and confirmed with "security mode complete," all subsequent NAS messages between the UE and the AMF must be protected. The UE's action of not responding to a properly protected "service accept" message does not violate the 3GPP standard, as the standard does not require the UE to respond to a "service accept" unless further signaling is needed. The key security criterion is that the UE only communicates over protected NAS after security activation, which was satisfied in this case. Therefore, based on the information provided and the 3GPP standard, the UE's actions were secure. 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 procedure, the UE sent a "registration complete" message to the AMF, indicating the end of its registration process. Immediately afterward, the AMF (under tester control) sent a "deregistration request (UE terminated)" message to the UE, which was integrity protected and ciphered as indicated by the NAS security header type (2). The UE responded with a "deregistration accept (UE terminated)" message, acknowledging the deregistration. According to the 3GPP 5G standard (TS 24.501), after the NAS security context is established via 5G-AKA, all subsequent NAS messages between the UE and the AMF must be protected by integrity and, where required, confidentiality protection. The packet capture confirms that after 5G-AKA, the downlink deregistration request was protected and the UE responded appropriately. The UE did not process or respond to any unprotected NAS messages after security was activated, and it followed the correct procedure for deregistration per the standard. Therefore, the UE's actions were in line with 3GPP security requirements and did not expose any security vulnerabilities in its communication during this exchange. 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 successfully completing the 5G-AKA authentication and key agreement procedure, the UE sent a "registration complete" uplink NAS message to the AMF, followed by a PDU session establishment request. The AMF then responded with a protected "service accept" downlink NAS message, indicating that NAS security (i.e., encryption and integrity protection) was in place for subsequent messages as per 3GPP 5G security standards. After receiving the service accept, the UE sent a deregistration request (UE originating) to the AMF. According to 3GPP TS 33.501, once 5G-AKA is completed and NAS security is activated, all subsequent NAS messages between the UE and the AMF must be integrity protected and, if required, encrypted. Since the deregistration request was sent after NAS security was established and there is no indication in the packet capture or summary that the UE sent this message unprotected or in violation of security procedures, the UE's actions align with the 5G security requirements. The UE correctly followed the protocol by only sending sensitive NAS messages after security activation, ensuring the confidentiality and integrity of its communication. 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 completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration and security association process had concluded. Subsequently, the AMF sent a "Security Mode Command" message to the UE, which was protected using integrity protection and indicated the use of the null ciphering algorithm (5G-EA0) and 128-5G-IA2 for integrity. The security header was set to "Integrity protected with new security context (3)," meaning the message was protected with the freshly established keys from the 5G-AKA. Importantly, the UE did not respond to the "Security Mode Command" from the AMF. According to the 3GPP 5G standard (TS 24.501), after successful authentication and key establishment, the UE is expected to process the "Security Mode Command" and respond with a "Security Mode Complete" message, thus confirming acceptance of the negotiated security algorithms and context. The absence of a response from the UE at this stage indicates that it either rejected the security context or failed to process the command, which could be a security measure if the UE detected an anomaly (such as the use of the null ciphering algorithm, which is generally discouraged unless explicitly allowed by policy or configuration). From a security perspective, refusing to proceed with a null cipher (EA0) is considered a secure action, as it prevents unencrypted user data transmission. Therefore, the UE's lack of response to the "Security Mode Command" in this context aligns with secure behavior as defined by the 3GPP standard, particularly if the null cipher was not permitted by the UE's security policy. Secure
39	39	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.2683730125427246 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2686209678649902 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.476357936859131 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G Authentication and Key Agreement (5G-AKA) 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 observed in the packet capture as being protected by both integrity protection and ciphering, as specified by the security header (value 2). The UE then responded with a "configuration update complete" message. According to the 3GPP 5G security standards, after the 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, ciphered to ensure confidentiality and authenticity. The packet capture confirms that the downlink message from the AMF was indeed protected, and the UE responded appropriately. The actions taken by the UE—responding only after the security context was established and using protected NAS messages—align with 3GPP security requirements, demonstrating that the UE maintained secure NAS communication throughout the process. 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, the UE and AMF completed the 5G-AKA authentication and key agreement, establishing the security context necessary for protected NAS communication. Following this, the UE sent a "Registration Complete" message, after which the AMF responded with a "Configuration Update Command" that was integrity protected and ciphered, as indicated by the security header (value 2). The UE then replied with a "Configuration Update Complete" message. According to the 3GPP 5G standard, after successful 5G-AKA, all subsequent NAS messages between the UE and 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 sent as protected, and there is no indication that the UE responded in an insecure manner. Since the UE only sent its messages after security was established, and responded appropriately to a protected configuration update command, the UE's actions adhered to the 5G security requirements. Therefore, based on the sequence and protection of messages observed, the UE acted securely according to the 3GPP 5G standard. 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 successful completion of the 5G-AKA authentication, the UE sent a "registration complete" message to the AMF, indicating that the initial NAS procedures were completed and the UE was ready for further communication. The AMF then sent a "security mode command" message, which was marked as 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, as per 3GPP security requirements. However, the UE did not respond to this security mode command. Subsequently, the UE attempted to initiate a service request, but the AMF rejected it because the UE's identity could not be derived, which is consistent with the UE not having accepted or completed the security context activation. According to the 3GPP 5G standard, after 5G-AKA, the UE must respond to the security mode command to establish a secure NAS security context before further NAS messages (other than the registration complete) are exchanged. By failing to respond to the security mode command, the UE did not activate the negotiated security context and proceeded to send a service request without an established secure channel, which is a deviation from the standard and could expose the communication to security vulnerabilities. Therefore, the UE's behavior was not secure as per 3GPP requirements. 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, after the successful completion of the 5G-AKA authentication procedure, the UE sent an UplinkNASTransport message to the AMF, which indicates that a secure NAS security context should have been established. The AMF then responded with a protected Deregistration Accept message, indicating that the message was integrity protected and/or encrypted as per 3GPP standards. Following this, the UE did not respond further, which is expected behavior since the Deregistration Accept message is the final step in the UE-initiated deregistration procedure according to 3GPP TS 24.501. The UE is not required to acknowledge a Deregistration Accept; it should simply consider itself deregistered and release any related resources. Since the UE did not send any further messages after receiving a properly protected Deregistration Accept, and all prior security procedures were completed as required, the UE's actions align with 3GPP security requirements and best practices. Therefore, the UE's behavior in this scenario is 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 the 5G-AKA authentication and security procedures, the UE proceeded to send an Uplink NAS Transport message to the AMF. The AMF, under test control, responded with a Configuration Update Command that was protected with both integrity and ciphering, as indicated by the security header (2), ensuring the confidentiality and integrity of the message according to 3GPP standards. Following this, the UE sent a Deregistration Request (UE originating) to the AMF. Since the 5G-AKA procedure was completed prior to these exchanges, all subsequent NAS messages, including the Deregistration Request from the UE, should be protected as per 3GPP TS 33.501, which mandates that after security context establishment, NAS signaling must be integrity protected and ciphered. The packet capture does not indicate any deviation from these requirements, and there is no evidence that the UE sent unprotected messages after security activation. Therefore, the UE's actions align with the 5G security standards, maintaining protected communication throughout the exchange. 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 completion of 5G-AKA (authentication and key agreement), the UE sent an UplinkNASTransport message, which is a normal step in NAS communication. The AMF, under tester control, then sent a Deregistration Request (UE terminated) message that was integrity protected and ciphered, as indicated by the security header (2), meaning the message was both encrypted and protected for integrity. The UE responded with a Deregistration Accept (UE terminated) message, confirming the deregistration procedure. Since 5G-AKA was completed before these messages, the security context was established, ensuring that all subsequent NAS messages—including the critical deregistration request—were protected as per 3GPP standards. The UE’s action to only respond to a properly protected deregistration request and to accept deregistration in this context aligns with the 3GPP security requirements, which mandate that sensitive NAS signaling after authentication must be integrity protected and ciphered to prevent spoofing or tampering. Therefore, the UE's behavior demonstrates adherence to 5G security procedures, as it did not process or respond to unprotected or insecure messages, and only accepted a deregistration request that was securely delivered. 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, indicating that the security context was already established. Subsequently, 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 responded with a Configuration Update Complete message, also sent as a NAS message under the established security context. According to the 3GPP 5G standard (TS 24.501), once the 5G-AKA procedure 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 Configuration Update Command from the AMF was protected, and the UE responded appropriately with a Configuration Update Complete message, indicating adherence to the security requirements. Therefore, the actions taken by the UE align with the 3GPP security standards for NAS message protection after authentication and key establishment. Secure
46	46	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.425251007080078 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4254679679870605 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4255969524383545 AMF to UE DownlinkNASTransport, Configuration update command 2.629240036010742 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test of a 5G standalone User Equipment (UE), the interaction began with the successful completion of 5G-AKA, which is the authentication and key agreement procedure required to establish security context between the UE and the Access and Mobility Management Function (AMF). Following this, the UE sent an UplinkNASTransport message, after which the AMF, under the tester’s control, sent a Configuration Update Command to the UE. The packet capture shows that this downlink message was sent as “Protected” with a security header indicating both integrity protection and ciphering (value 2), signifying that the message was encrypted and authenticated according to 3GPP 5G security standards. The UE responded with a Configuration Update Complete message, also sent as UplinkNASTransport, which is the expected behavior after receiving a configuration update. Since all NAS signaling after the completion of 5G-AKA was protected (integrity and ciphering applied), and the UE only responded to properly secured messages, the UE’s actions align with the security requirements defined by 3GPP for NAS message protection in 5G systems. Therefore, based on the observed behavior and adherence to the standard, the UE’s actions were secure. 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 completing the 5G-AKA authentication and key agreement process, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent a Configuration Update Command to the UE, which, according to the packet capture and summary, was protected using both integrity protection and ciphering as indicated by the security header (value 2). The UE then responded with a Configuration Update Complete message. Since 5G-AKA was completed prior to these exchanges, the NAS security context would have been established, ensuring that subsequent NAS messages—including the Configuration Update Command and the UE’s Configuration Update Complete—were encrypted and integrity-protected as required by 3GPP TS 33.501. The UE's actions, specifically its response to a properly protected configuration update command, align with 3GPP security requirements: it only processed and replied to a message that was both integrity protected and ciphered, indicating that it adhered to the standard procedure for secure NAS communication after authentication and key setup. Therefore, based on the sequence and security status of the messages, the UE’s behavior was secure and compliant with 3GPP standards. 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 proceeded to send a UL NAS Transport message, indicating that it was ready for secure communication. The AMF, under test control, then sent a Security Mode Command message to the UE, which was correctly protected (integrity protected with a new security context) and specified the use of 5G-EA4 for ciphering and 128-5G-IA2 for integrity protection. However, upon receiving this message, the UE responded with a Security Mode Reject, citing an unspecified reason. According to the 3GPP 5G standards, after 5G-AKA, the UE is expected to accept a valid, correctly protected Security Mode Command unless there is a legitimate issue such as an unsupported algorithm, incorrect security context, or protocol error. Since the Security Mode Command was properly protected and followed standard protocol, the UE's rejection of the command without specifying a concrete reason (using "unspecified") is not compliant with the standard and suggests a potential flaw or misconfiguration in the UE's security handling. This could open the UE to denial-of-service attacks or prevent the establishment of a secure session, which is not considered secure behavior as per 3GPP requirements. Insecure

49	49	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 17.321523904800415 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.322353839874268 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Security mode command 17.532354831695557 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF. The AMF responded with a Security Mode Command, which was integrity protected and indicated the use of the 5G-EA0 (null) ciphering algorithm (meaning no encryption) and the 128-5G-IA2 integrity algorithm, with a security header specifying that a new security context was being used. Upon receiving this Security Mode Command, the UE responded with a Security Mode Reject, citing an unspecified reason. According to 3GPP standards, after 5G-AKA, the UE expects the network to require both integrity protection and encryption for NAS messages, unless there is a valid reason for using null encryption (5G-EA0). The use of the null ciphering algorithm (5G-EA0) in a situation where encryption should be enabled is considered insecure, as it exposes NAS messages to potential eavesdropping. The UE correctly detected this insecure configuration and refused to accept the security mode, thereby protecting itself from operating in an unencrypted state. This action aligns with 3GPP security recommendations, where the UE is expected to reject insecure security configurations after authentication. Therefore, the UE's actions were secure and in compliance with the standard. 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 5G-AKA authentication, the User Equipment (UE) initiated a Service Request by sending an uplink NAS message to the Access and Mobility Management Function (AMF). In response, the AMF sent a downlink NAS message containing a "Deregistration accept" message, which was protected (i.e., integrity protected and possibly ciphered) as per the 5G security requirements. Following this protected deregistration accept message from the AMF, the UE did not respond further. According to the 3GPP 5G standards, after 5G-AKA is completed, all subsequent NAS signaling messages between the UE and AMF must be integrity protected and, where required, ciphered. The "Deregistration accept" message is a valid and expected response from the network after a deregistration request, and the UE is not required to respond further upon receiving it, especially if it was received as a protected message. The UE's lack of response in this context is compliant with the standard, as it indicates proper handling of the protected message and no further unnecessary communication. Therefore, based on the observed behavior and adherence to 3GPP security requirements, the UE's actions 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, indicating that a secure NAS context had been established and that subsequent messages should be both integrity protected and ciphered, as per 3GPP 5G security requirements. The AMF, under test control, responded with a deregistration request (UE terminated), sent as a protected message with both integrity protection and encryption enabled (security header type 2). Despite the deregistration request being unexpected in the protocol state (as indicated by "Message type not compatible with the protocol state"), the UE processed the request and replied with a deregistration accept message, also sent in a secure, protected manner. According to 3GPP TS 24.501, the UE is required to respond to protected deregistration requests, even if they are unexpected, provided the security context is valid and the message is properly protected. The UE's actions—responding only to a protected, integrity-protected, and ciphered deregistration request after 5G-AKA—demonstrate adherence to the standard's security requirements, as the UE did not process any unprotected or suspicious messages. Therefore, based on the evidence from the packet capture and the 3GPP standard, the UE's behavior in this scenario was secure. 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 security test of a 5G standalone User Equipment (UE), the authentication procedure (5G-AKA) was completed first, establishing a secure context for subsequent communications. The UE initiated a service request, which was received by the AMF. In response, the AMF sent a Configuration Update Command as a downlink NAS message, which was integrity protected and ciphered, as indicated by the security header value (2). This means the message was both encrypted and its integrity was protected, as per 3GPP standards for NAS security after authentication. Upon receiving this protected message, the UE sent a Deregistration Request (UE originating) back to the AMF. Since the UE only proceeded with deregistration after receiving an appropriately protected command, and all communication after authentication was secured, the UE's actions align with 3GPP security requirements. The UE did not process any unprotected or suspicious messages, and all sensitive exchanges occurred under an established security context. Therefore, the UE's behavior in this interaction was secure and compliant with 3GPP 5G standards. Secure

53	53	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 17.000593185424805 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.001089096069336 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal UE) 17.204612970352173 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication and security procedure, the UE initiated a service request to the AMF, which is a normal step for accessing network services. In response, the AMF sent a deregistration request message to the UE, indicating that the UE should terminate its registration with the network. Notably, this deregistration request was sent with both integrity protection and encryption (ciphering), as indicated by the security header type (2), which means the message was secured according to 3GPP 5G NAS security requirements. The UE, upon receiving this protected deregistration request, responded with a deregistration accept message, thus following the expected protocol behavior for a legitimate, protected deregistration command. Since all NAS messages after 5G-AKA were appropriately protected and the UE only accepted a deregistration request that was integrity protected and ciphered, the UE’s actions were in line with 3GPP security standards. There is no indication that the UE accepted or processed any unprotected or illegitimate messages. Therefore, based on the observed behavior and adherence to security requirements, the UE's actions can be considered secure. Secure
54	54	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 100 UE provided: No response The packet capture during the test using wireshark is: 1.321023941040039 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.3216829299926758 AMF to UE DownlinkNASTransport, 5GMM status (Conditional IE error) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test scenario, the 5G standalone User Equipment (UE) first completed the 5G-AKA authentication procedure, establishing a secure context for further NAS communication. Afterward, the UE sent an uplink Service Request message to the Access and Mobility Management Function (AMF), which was expected behavior following NAS procedures. The AMF, under test control, responded with a protected (encrypted and integrity-protected) GMM Status message indicating a "Conditional IE error" (5GMM Cause: 100). According to the 3GPP 5G standards, specifically TS 24.501 section 8.4.2, when the UE receives a protected GMM Status message, it is not required to respond; the purpose of the Status message is to inform the peer of an error, not to solicit a reply. The UE, in this scenario, did not respond to the protected Status message, which aligns with the standard's security expectations—responding to such messages could create unnecessary signaling or potential vulnerabilities. Therefore, the UE's behavior was secure and compliant with 3GPP 5G security procedures. 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 5G standalone User Equipment (UE) initiated NAS communication by sending an initial registration request to the Access and Mobility Management Function (AMF). The AMF, controlled for testing purposes, responded with an Authentication Reject message before the 5G-AKA (Authentication and Key Agreement) procedure was completed, and this reject message was sent in plain (unencrypted) form. The UE, upon receiving this unauthenticated and unprotected Authentication Reject message, did not respond further. According to the 3GPP 5G standard, before the completion of 5G-AKA, NAS messages are not protected, and the UE is required to accept certain messages, such as Authentication Reject, even if they are received in plain text. Furthermore, the UE is expected to cease further communication upon receiving an Authentication Reject, as this indicates that authentication has failed. The UE’s lack of response aligns with the 3GPP specification, which aims to minimize the risk of further interaction based on potentially spoofed or unauthenticated messages. Therefore, the UE’s behavior in this scenario is considered secure as per the 5G standard, since it did not proceed with any further actions after receiving the Authentication Reject message in plain text before security context establishment. 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, after the UE initiated registration by sending an InitialUEMessage with a Registration Request to the AMF, the AMF responded with an Authentication Reject message sent in plain (unencrypted) form. Notably, the 5G-AKA authentication procedure had not yet been completed, and thus NAS security (encryption and integrity protection) was not yet established between the UE and the AMF. According to the 3GPP 5G standards, certain NAS messages, including Authentication Reject, are allowed to be sent in plain text prior to the completion of authentication and key agreement, as security contexts are not yet available. The UE, upon receiving an Authentication Reject message before NAS security was established, did not respond further. This behavior aligns with 3GPP specifications, which indicate that the UE should not take further action upon receiving an Authentication Reject prior to security establishment, as this message signals that registration cannot proceed. Therefore, the UE's action—specifically, its lack of response to an unauthenticated Authentication Reject before security establishment—was in line with the standard and did not introduce any security risk in this context. 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, which is expected behavior at the start of a NAS session. In response, the AMF sent an "authentication reject" message to the UE, and this message was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards, specifically TS 33.501, NAS messages exchanged prior to the successful completion of authentication and security mode command (i.e., before keys are established) are allowed to be sent unprotected (plain), and UEs are required to accept and process certain messages, such as authentication reject, even if they are received in plain. Importantly, the UE did not respond further to the authentication reject, which is in accordance with the standard: upon receiving an authentication reject, the UE should stop the registration procedure and not attempt further NAS communication unless a new registration attempt is initiated. Thus, the UE's behavior—accepting the plain authentication reject and not responding further—complies with 3GPP security requirements and does not introduce vulnerabilities. The UE avoided taking any insecure action or leaking information in response to a potentially spoofed or manipulated message. Based on this analysis, the UE's action in this scenario was secure. Secure
58	58	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003209114074707031 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) initiated a NAS registration procedure by sending an initial registration request 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 because the 5G Authentication and Key Agreement (5G-AKA) process had not yet been completed. According to the 3GPP 5G security architecture, encryption and integrity protection of NAS messages are only established after successful authentication and key agreement; thus, initial messages, including Registration Request and Authentication Reject, are permitted to be sent in plain text before 5G-AKA is completed. Upon receiving the Authentication Reject message, the UE did not respond further, which aligns with the 3GPP specification that dictates the UE should not proceed with registration or further NAS communication after receiving an Authentication Reject. This behavior prevents further interaction without proper authentication and protects the UE from potential replay or downgrade attacks. Therefore, the UE's action—ceasing communication after receiving a plain Authentication Reject message before security context establishment—follows 3GPP specifications and is considered secure. Secure

59	59	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002620220184326172 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an Initial Registration Request to the AMF, which is expected behavior during the NAS (Non-Access Stratum) communication phase. The AMF, under test control, responded with an Authentication Reject message before the 5G-AKA (Authentication and Key Agreement) procedure was completed; notably, this message was sent in plain (unencrypted) form, as encryption is only established after successful authentication. According to the 3GPP 5G security specifications, the UE should not respond to an Authentication Reject message received before authentication and security context establishment, especially if the message is received in plain text, since such messages could be spoofed by an attacker. The packet capture confirms that the UE did not respond to the Authentication Reject, which aligns with the 3GPP standard security recommendations to prevent downgrade or spoofing attacks before mutual authentication is achieved. Therefore, the UE's action in this scenario was secure and compliant with 5G security standards. 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 registration procedure by sending an initial registration request to the AMF, which is the expected first step in establishing a 5G connection. Since 5G-AKA (Authentication and Key Agreement) had not yet been completed, all NAS messages, including the registration request and any subsequent messages, would be transmitted in the clear (unencrypted). The AMF, under tester control, responded with an "Authentication Reject" message sent as a plain (unencrypted) downlink NAS message. Critically, the UE did not provide any response to this authentication reject message. According to 3GPP 5G standards (TS 24.501), upon receiving an unprotected (plain) "Authentication Reject" message before security activation, the UE should treat this as potentially insecure and not take further action or respond, as this could indicate a security attack (e.g., a fake or rogue AMF). The UE's lack of response demonstrates correct adherence to the 3GPP security guidelines, as it avoids further communication that could compromise security before authentication and key establishment. Therefore, the action taken by the UE in this scenario was 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 containing a 5GMM cause code 111 (Protocol error, unspecified), and this message was sent in plain (unencrypted) form. Notably, the 5G-AKA authentication procedure had not yet been completed at the time of this exchange. According to the 3GPP 5G security standards, NAS messages exchanged before the completion of 5G-AKA—specifically before security context establishment—are expected to be sent unencrypted (in plain), as mutual authentication and key agreement have not yet taken place. Upon receiving the Registration Reject, the UE did not respond further, which is the expected and secure behavior, as the registration procedure is terminated upon receipt of a reject. Therefore, the UE's actions in this scenario—sending the initial request, accepting the plain Registration Reject, and not responding further—are fully compliant with the 3GPP standard and do not expose the UE to any security risk at this stage of the protocol. The UE did not proceed to any further steps that would require encryption, nor did it react improperly to the reject. 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 5G-AKA authentication, the UE initiated a service request to the AMF, which is the expected behavior for accessing services in a 5G standalone network. In response, the AMF sent a deregistration accept message to the UE, and this downlink message was sent as a protected (i.e., integrity protected and/or ciphered) NAS message, indicating that the security context established during 5G-AKA was being utilized. The UE, upon receiving this deregistration accept, did not send any further response, effectively terminating its NAS communication as per the AMF's instruction. According to the 3GPP 5G standards, after receiving a protected deregistration accept message, the UE is expected to cease further NAS signaling unless re-registration or other procedures are initiated. The UE did not attempt to send any unprotected or unexpected messages after the protected deregistration accept, nor did it attempt to continue service in violation of the NAS state machine. This indicates that the UE properly adhered to the security procedures and state transitions defined by 3GPP, maintaining the integrity and confidentiality of its communication and session management. Therefore, based on this interaction, the UE's actions were secure and compliant with the 5G standards. 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 successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, as expected. The AMF then issued a Security Mode Command, which, according to the packet capture and message details, was sent as a protected message—specifically, it was integrity protected with a new security context and specified the use of ciphering and integrity algorithms (128-5G-EA1 and 128-5G-IA2). The UE, upon receiving this command, responded with a Deregistration Request (UE originating). According to the 3GPP 5G security standards, after 5G-AKA is completed and a new security context is established via the Security Mode Command, all subsequent NAS messages from the UE must be protected (i.e., integrity protected and, if required, ciphered) using the negotiated algorithms. The critical point here is whether the Deregistration Request sent by the UE after receiving the Security Mode Command was sent with the appropriate security protections enabled by the new context. Since the test summary and packet capture do not indicate any deviation from the standard (such as sending the Deregistration Request unprotected or before security activation), and since the Security Mode Command was properly protected and acknowledged by the UE's subsequent message, the UE's actions align with 3GPP security requirements. Therefore, the UE's behavior in this sequence is considered secure. Secure
64	64	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.12326717376709 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.123653173446655 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes the security context for encrypting NAS messages), the UE initiated a Service Request to the AMF. The AMF then responded with a Service Accept message, which was sent as a protected (encrypted and integrity-protected) downlink NAS message. However, the UE did not provide any response to this protected Service Accept message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages (such as Service Accept) must be both integrity protected and ciphered. The AMF correctly sent the Service Accept in a protected manner, and the UE, upon receiving this message, should have processed it and continued the procedure (typically by sending an uplink NAS message, such as an uplink NAS transport or a confirmation). The UE's lack of response to a valid, protected Service Accept message indicates that it did not correctly process the message as per 3GPP requirements. This behavior could suggest a flaw in the UE's handling of protected NAS messages, potentially leaving the communication incomplete or vulnerable to disruption. Therefore, based on the 3GPP security requirements and the UE's lack of response to a protected message after 5G-AKA, 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 5G standalone security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a “security mode complete” message to the AMF, indicating acceptance of the negotiated security parameters. However, the AMF, under test control, subsequently sent another “security mode command” to the UE, this time as a protected message with specified ciphering (128-5G-EA2) and integrity (128-5G-IA1) algorithms, and a security header indicating “integrity protected with new security context.” Upon receiving this unexpected and potentially suspicious message, the UE responded with a “security mode reject,” specifying the reason as “security mode rejected, unspecified.” According to the 3GPP 5G standard, once the security context is established and the security mode is completed, receiving a second security mode command without a valid reason is considered abnormal and could indicate a security attack or protocol misuse. The UE’s decision to reject the second security mode command, rather than accepting it or proceeding with further communication, demonstrates adherence to the standard’s security requirements by preventing potential downgrade or replay attacks, or unauthorized changes to the security context. This cautious behavior aligns with the 3GPP guidance for UEs to reject invalid or unexpected security procedures, thereby maintaining the integrity of the established 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.	During the test, after the successful completion of 5G-AKA authentication, the UE sent an uplink NAS transport message to the AMF, indicating that it was ready for further NAS procedures under a mutually established security context. The AMF then sent a Security Mode Command (SMC) to the UE, which was protected using the negotiated ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and the security header indicated that a new security context was in use. Upon receiving the SMC, the UE responded with a Security Mode Reject message, specifying that the security mode was rejected for an unspecified reason. According to the 3GPP 5G standard (TS 24.501), a UE is required to reject a Security Mode Command if it detects any inconsistency, integrity failure, or unsupported security algorithms, or if it cannot accept the proposed security context for any other reason. The fact that the UE sent a Security Mode Reject implies that it detected an issue with the SMC or the proposed security context and, rather than proceeding insecurely or accepting a potentially compromised context, it correctly refused to continue. This is a secure behavior as per 3GPP requirements, as it prevents the UE from operating under potentially unsafe security parameters or contexts. Therefore, the UE's actions demonstrate adherence to secure protocol behavior as specified by the standard. Secure

67	67	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.8137481212615967 UE to AMF UplinkNASTransport, Service request 0.814223051071167 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 1.0217480659484863 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 access to network services. The AMF, under tester control, responded with a protected (encrypted and integrity-protected) 5GMM Status message carrying the cause value 98, which indicates "Message type not compatible with the protocol state" as per 3GPP TS 24.501. Upon receiving this message, the UE replied with its own 5GMM Status message, echoing the same cause value. According to the 3GPP 5G NAS protocol specifications, when a UE receives a STATUS message with an unexpected or invalid message type in a given protocol state, it is expected to respond with a STATUS message indicating the incompatibility. The fact that the UE sent a STATUS message in response to a protected STATUS message from the AMF, and did so using NAS security (since 5G-AKA was completed), demonstrates that the UE followed the protocol as intended and did not leak information or behave abnormally. The communication remained protected, and the UE's response was in line with the 3GPP standard's requirements for error handling and security. Therefore, the UE's actions in this scenario were secure. 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.	During the security test, after 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 DownlinkNASTransport message containing a Configuration Update Command, which was integrity protected as indicated by the security header. The UE then responded appropriately with a Configuration Update Complete message, and subsequently sent a Registration Request. According to the 3GPP 5G standard, after 5G-AKA is completed, NAS messages between the UE and AMF must be integrity protected (and optionally encrypted depending on the configuration and message type). The packet capture confirms that the Configuration Update Command from the AMF was protected, and the UE responded as expected. There is no indication that the UE sent any unprotected or insecure messages after authentication was established. Therefore, the UE behaved in accordance with 3GPP security requirements for NAS communication post-authentication. Based on this interaction, the UE's actions were 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 successfully completing 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, indicating the selection of security algorithms: 5G-EA0 (null ciphering, meaning no encryption) and 128-5G-IA2 (integrity protection). The Security Mode Command message was protected and indicated the establishment of a new security context. Upon receiving this, the UE responded with a Security Mode Reject, citing an unspecified reason. According to 3GPP standards (TS 24.501 and TS 33.501), ciphering algorithm 5G-EA0 provides no confidentiality protection for user or signaling data, which is generally only allowed in specific, limited scenarios (such as emergency calls or regulatory requirements). In standard, non-emergency communication, the UE is expected to reject the use of null ciphering for security reasons to prevent unencrypted transmission of sensitive information. The UE's decision to reject the Security Mode Command when offered only null ciphering is therefore aligned with security best practices and the intent of the 3GPP standards, as it prevents insecure communication. The UE's response was thus secure and appropriate in this context. Secure

70	70	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.547684907913208 UE to AMF UplinkNASTransport, Registration complete 0.5478739738464355 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the authentication and key agreement procedure (5G-AKA) was successfully completed, after which the UE sent a "registration complete" message to the Access and Mobility Management Function (AMF). Subsequently, the AMF sent a "security mode command" message to the UE, which was protected using integrity protection and ciphering with a new security context, as indicated by the security header type (4). The ciphering algorithm used was 5G-EA0 (null), meaning no encryption, while the integrity algorithm was 128-5G-IA2, providing integrity protection. The UE did not respond to this security mode command. According to the 3GPP 5G standard, after successful authentication, the AMF should initiate security mode control to establish NAS security; the UE is expected to respond to the security mode command to confirm the negotiated security algorithms and activate the security context. The use of 5G-EA0 (null ciphering) is allowed but only under specific, controlled circumstances (e.g., for emergency services or in trusted environments), and the UE should still respond to the security mode command regardless of the ciphering algorithm used. The UE's lack of response to the security mode command is not compliant with the 3GPP standard, as it should acknowledge and accept or reject the security mode command. By failing to respond, the UE does not establish a secure NAS layer, potentially leaving the session vulnerable or incomplete. Thus, the UE's behavior in this scenario is considered insecure according to the standard. Insecure

71	71	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0332 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 4.62968111038208 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 4.630121946334839 AMF to UE SACK (Ack=10, Arwnd=106361) , DownlinkNASTransport, Configuration update command 4.6305460929870605 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF completed the 5G-AKA authentication, enabling the subsequent exchange of NAS messages with security context established. After the authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Security Mode Command. The Security Mode Command was protected, as indicated by the security header (integrity protected and ciphered), and specified ciphering with 128-5G-EA3 and null integrity (5G-IA0). According to 3GPP standards, after 5G-AKA, the UE should respond to a Security Mode Command by confirming the security algorithms and activating them, provided the message is properly protected and the negotiated algorithms are acceptable. However, in this test, the UE did not respond to the Security Mode Command. This lack of response from the UE is significant: by not accepting a Security Mode Command that uses null integrity protection (5G-IA0), the UE is refusing to proceed with weak or potentially insecure security settings. This behavior aligns with best security practices, as 3GPP TS 33.501 recommends that UEs should not accept null integrity protection unless explicitly allowed by the operator and configuration, since it leaves NAS messages vulnerable to modification or replay attacks. Therefore, by refusing to respond under these circumstances, the UE demonstrated secure behavior in line with 3GPP security requirements. 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, indicating it was ready for further NAS procedures. The AMF, under test control, responded with a Security Mode Command, which was integrity protected and indicated the use of ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA2, and included an ABBA value of 3300. Upon receipt of this Security Mode Command, the UE responded with a Security Mode Reject, specifying "Security mode rejected, unspecified" as the cause. According to 3GPP standards (TS 24.501), the UE should only reject a Security Mode Command if it detects an issue such as an unsupported algorithm, a mismatch in the security context, or an integrity failure. Since the Security Mode Command was protected and followed the completion of 5G-AKA, the UE's rejection may indicate a detected inconsistency or a security concern with the parameters provided by the AMF, or possibly an implementation issue. The fact that the UE did not proceed with accepting potentially insecure or unexpected security parameters, and instead explicitly rejected the Security Mode Command, aligns with secure behavior as defined by 3GPP—provided the rejection was for a valid security reason and not due to a protocol error. This demonstrates the UE's adherence to strict security policy, refusing to establish a security context when there is any ambiguity or potential risk, which is the expected secure behavior. Secure

73	73	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1599750518798828 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602010726928711 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3605461120605469 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described test scenario, after successfully completing the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, indicating that it accepted the previously negotiated security parameters. Unexpectedly, the AMF then sent another Security Mode Command, this time using the null cipher algorithm (5G-EA0) but with integrity protection enabled (128-5G-IA2), and the message was protected with the new security context. Upon receiving this, the UE responded with a Security Mode Reject message, indicating that it rejected the security mode for an unspecified reason. According to the 3GPP 5G security standards, once a secure context is established through 5G-AKA, the use of a null cipher algorithm (5G-EA0) is typically not permitted unless explicitly allowed by the UE's security policy, as it would leave user data unencrypted and vulnerable to interception. The UE's decision to reject the security mode command that attempted to set the ciphering algorithm to null (even though integrity was still protected) aligns with the security requirements to avoid downgrading to an insecure state after authentication. This behavior demonstrates that the UE is enforcing the standard's security policies by refusing to accept a configuration that would compromise the confidentiality of user data. Therefore, the action taken by the UE was secure according to the 3GPP 5G security standard. Secure

74	74	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03b3 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11993098258972168 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12021493911743164 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3277699947357178 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing 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 new security context, specifying ciphering and integrity algorithms (128-5G-EA3 and 128-5G-IA2) and an ABBA value. Upon receiving this protected Security Mode Command, the UE responded with a Security Mode Reject message, citing an unspecified reason. According to the 3GPP 5G standards, after authentication, the UE must verify the integrity and correctness of the Security Mode Command, including supported algorithms, ABBA value, and the security context. If any of these parameters are unacceptable or if the message is malformed, the UE is permitted to reject the security mode setup to prevent the establishment of insecure or unsupported security contexts. Since the Security Mode Reject was sent with an "unspecified" cause, the UE did not disclose detailed error information, which is a cautious approach to avoid leaking internal state information to a potential attacker. Given that the UE did not proceed with establishing security parameters it may have deemed invalid or suspicious, and instead rejected the setup without providing sensitive details, this behavior aligns with secure practices as per 3GPP requirements for protecting the UE and the network. Secure

75	75	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0392 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.4745960235595703 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4750940799713135 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.47630810737609863 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) completed the 5G-AKA authentication procedure, establishing the necessary security context for protected NAS communication. The UE then sent an Uplink NAS Transport message to the AMF, after which the AMF responded with a Security Mode Command that was correctly protected using integrity and ciphering algorithms (5G-EA5 and 128-5G-IA1), as indicated by the security header "Integrity protected with new security context (3)." However, after receiving this Security Mode Command, the UE did not provide any response, which is not in line with the 3GPP 5G NAS standard. According to 3GPP TS 24.501, upon receiving a valid Security Mode Command, the UE is required to respond with a Security Mode Complete message if it accepts the proposed algorithms and security context, or a Security Mode Reject if it cannot accept them. The absence of any response from the UE is a deviation from the standard and could indicate a failure in the UE's security handling or protocol implementation. This lack of response could potentially result in a denial of service or leave the UE in an insecure or undefined state, as further NAS messages would not be processed under the new security context. Therefore, based on the 3GPP standard, the action taken by the UE is considered insecure because it did not properly complete the security mode procedure. 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 security test simulation, the 5G standalone User Equipment (UE) completed the early NAS procedures and sent an authentication response to the AMF. At this stage, the 5G-AKA authentication procedure had not yet been completed, meaning that the NAS security context (encryption and integrity protection) was not yet established. The AMF then sent an identity request for the SUCI (Subscription Concealed Identifier) to the UE in plain (unencrypted) NAS, as expected before 5G-AKA completion. The UE, upon receiving this plain identity request for the SUCI, did not respond. According to the 3GPP 5G standard, the SUCI is a privacy-preserving identifier that can be transmitted in plain NAS messages prior to authentication and security context establishment, specifically to allow the network to identify the subscriber without exposing the SUPI (Subscription Permanent Identifier). However, since the SUCI is designed to be safe for transmission in cleartext, the 3GPP standard expects the UE to respond to such a request. By refusing to provide the SUCI in this scenario, the UE is being overly cautious and not strictly compliant with the standard, but from a security perspective, this action avoids even the minimal risk of exposing subscriber information, however protected, before security is established. Therefore, while the UE's behavior is not standard-compliant, it is secure from a privacy and security standpoint, as it avoids sharing any identifying information before NAS security is in place. 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 registration by sending an initial registration request to the AMF. The AMF, under your control, responded with an identity request message, specifically requesting the SUCI (Subscription Concealed Identifier), and sent this message in plain (unencrypted) form. The UE then replied with an identity response, providing the requested SUCI. According to the 3GPP 5G standard, before the completion of 5G-AKA (Authentication and Key Agreement), the NAS (Non-Access Stratum) messages between the UE and AMF are not yet encrypted, as key material for encryption is not established until after authentication. The standard requires that the UE never sends the cleartext SUPI (permanent identifier) before security is activated, but it is specifically designed for the SUCI (which is a privacy-preserving, encrypted form of the SUPI) to be sent in the clear if requested prior to security activation. Since the UE responded with the SUCI, and not the SUPI, before the completion of 5G-AKA and NAS security activation, its behavior aligns with the privacy and security requirements set by 3GPP. Therefore, based on the 5G standard, the action taken by the UE is considered secure in this context. 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 successfully completing 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 security mode command. However, the AMF subsequently sent another "security mode command" message, this time with the ciphering algorithm set to 5G-EA0 (null encryption) and the integrity algorithm set to 128-5G-IA2, and the message was integrity protected but not ciphered. Upon receiving this, the UE responded with a "security mode reject," citing an unspecified reason. According to the 3GPP 5G standard (TS 24.501), once the security context is established and the security mode complete is sent, the UE expects all subsequent NAS messages to be protected according to the agreed-upon algorithms. If the network attempts to downgrade security (e.g., by using 5G-EA0/null ciphering after a successful authentication and security mode procedure), the UE is expected to reject such attempts to prevent potential security breaches such as "null ciphering attacks." The UE's decision to reject the security mode command that proposed null encryption, even though integrity protection was present, aligns with the standard's security requirements and demonstrates correct, secure behavior, as it prevents possible exploitation by refusing to accept a lower level of security than previously agreed. Thus, based on the interaction, the UE's actions were secure and in compliance with 3GPP standards. Secure

79	79	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1600358486175537 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16031789779663086 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36404991149902344 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the User Equipment (UE) sent an authentication response to the Access and Mobility Management Function (AMF). The AMF then issued a Security Mode Command to the UE, specifying the use of the 5G-EA0 (null) ciphering algorithm 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, 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 and AMF negotiate security algorithms for ciphering and integrity protection. The selection of 5G-EA0 (null ciphering) means that no encryption would be applied to subsequent NAS messages, even though integrity protection is enabled. The 3GPP standard (TS 33.501) allows the use of 5G-EA0 only in exceptional circumstances (e.g., for emergency calls or under regulatory requirements) and generally expects UEs to reject security mode commands that propose null encryption when not appropriate. The UE's decision to reject the security mode command when only the null ciphering algorithm was proposed aligns with best security practice, as it prevents unencrypted NAS message exchange, thereby safeguarding user privacy and network security. Therefore, the action taken by the UE was in accordance with 3GPP security requirements and demonstrates secure behavior in this context. 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 the 5G-AKA authentication and security procedures, the UE sent a service request to the AMF. In response, the AMF sent a configuration update command, which was integrity protected with a new security context, indicating that the message was secured according to 5G security procedures. However, instead of processing the configuration update command as expected, the UE responded with a 5GMM status message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G standards, once the security context is established, the UE is expected to process protected NAS messages that are valid for its current protocol state. If the UE receives a message that is not compatible with its protocol state, it is standard-compliant and secure for the UE to reject the message and inform the network using a 5GMM status message. This behavior prevents the UE from acting on potentially malicious or misrouted commands and ensures protocol integrity. Therefore, the UE's action of rejecting an unexpected or out-of-sequence message after security activation aligns with 3GPP security requirements and best practices for robust protocol implementation. 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 the described test scenario, the UE and AMF completed the 5G-AKA authentication procedure, after which the UE sent an Authentication Response to the AMF. The AMF then issued a Security Mode Command to the UE, specifying the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, with the security header indicating "integrity protected." According to the 3GPP 5G standard (TS 33.501), the use of null algorithms (EA0/IA0) means that neither encryption nor integrity protection is actually applied to NAS messages, which exposes the communication to potential interception and manipulation. The UE, upon receiving a Security Mode Command with null algorithms, is expected to reject the configuration and not proceed with establishing security using inadequate algorithms, as this would compromise the confidentiality and integrity of subsequent communications. In this test, the UE did not respond to the Security Mode Command, which aligns with the security requirements of the 5G standard, as accepting null algorithms would be insecure. By refusing to proceed under these insecure conditions, the UE demonstrated secure behavior in accordance with 3GPP guidelines. 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, the 5G standalone User Equipment (UE) successfully completed the 5G-AKA authentication process, after which it sent an authentication response to the Access and Mobility Management Function (AMF). Subsequently, the AMF sent a Security Mode Command to the UE, specifying the use of ciphering algorithm 128-5G-EA3 and the integrity algorithm 5G-IA0 (null), with the message being integrity protected using 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 (TS 33.501), integrity protection is mandatory for all NAS signaling, and the use of the null integrity algorithm (5G-IA0) is generally not permitted unless specifically allowed by the UE's security capabilities and policies. The UE's decision to reject the Security Mode Command—because the AMF attempted to establish a security context with no integrity protection—demonstrates proper adherence to 5G security requirements, as accepting such a configuration would expose the UE to potential security risks. Therefore, the UE's action aligns with the 3GPP security standards and reflects secure behavior in this context. 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 completion of the 5G-AKA authentication procedure, the UE initiated a service request by sending an InitialUEMessage to the AMF, indicating a request for mobile-originated data. The AMF responded with a Service Accept message, which, according to the packet capture, was sent as a protected (encrypted and integrity-protected) downlink message. However, the UE did not provide any response to this protected Service Accept message. According to the 3GPP 5G standard, after successful 5G-AKA, NAS messages exchanged between the UE and the AMF should be protected to ensure confidentiality and integrity. The AMF's action of sending a protected Service Accept message is compliant with the standard. The UE, however, is expected to be able to process and respond to protected NAS messages after authentication and key establishment. The lack of response from the UE to a properly protected (encrypted) message from the AMF suggests that the UE either failed to decrypt or process the message, or did not recognize it as valid. This behavior is not compliant with 3GPP security requirements, as it indicates the UE may not be properly handling protected NAS messages post-authentication, potentially exposing itself to security risks or failing to maintain secure communication. Based on this analysis, the UE's action in this scenario 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, after the successful completion of the 5G-AKA authentication procedure, the UE responded to the AMF's authentication challenge with an authentication response. The AMF then sent a Security Mode Command message, which, as indicated by the packet capture, was protected (integrity protected with a new security context) and specified the use of the 128-5G-EA2 cipher and 128-5G-IA2 integrity algorithms, along with the ABBA parameter. Upon receiving this command, the UE replied with a Security Mode Reject message, citing an unspecified reason for the rejection. According to 3GPP 5G security standards (TS 24.501 and TS 33.501), a UE is required to verify the integrity and correctness of the Security Mode Command before accepting new security parameters. If the UE detects any anomaly—such as unsupported algorithms, mismatched parameters, or issues with the security context—it is required to reject the command to prevent possible security breaches or misconfigurations. Since the UE did not proceed with potentially insecure or misconfigured security settings and instead rejected the Security Mode Command, it acted in compliance with the security requirements to protect itself and the network. Although the reason for rejection was unspecified, the UE's cautious approach in not accepting new security parameters without full validation aligns with the intent of the 3GPP security architecture. Therefore, the UE's action in this scenario should be considered secure. Secure

85	85	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16005301475524902 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16028904914855957 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36393094062805176 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described test scenario, after completing 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. Unexpectedly, the AMF then sent another "security mode command" message, this time indicating the use of null algorithms for both ciphering (5G-EA0) and integrity protection (5G-IA0), even though the message itself was integrity protected with a new security context. Upon receiving this, the UE responded with a "security mode reject" message, specifying that the security mode was rejected for an unspecified reason. According to the 3GPP 5G standards (TS 24.501 and TS 33.501), after successful authentication, the network should not downgrade security by selecting null algorithms unless explicitly required by the UE's capabilities or local regulations. The UE is expected to reject any security mode command that attempts to use null algorithms when stronger algorithms are available and required, as accepting such a command would leave the communication unprotected and vulnerable to interception or manipulation. The UE's rejection of the security mode command that specified null algorithms demonstrates adherence to the 5G security standards and shows that it is not susceptible to a downgrade attack. Therefore, the UE's action in this scenario is secure. Secure

86	86	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered (2) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15096688270568848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15124177932739258 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.35789990425109863 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating acceptance of the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection). However, instead of proceeding with normal NAS communication, the AMF sent another "security mode command" message, which is atypical since the security mode procedure is expected to be a single exchange: the AMF sends a "security mode command," and the UE responds with "security mode complete." According to 3GPP standards (TS 24.501), once the UE has sent "security mode complete," it should consider the security context established and only accept further NAS messages that are properly protected according to the negotiated algorithms. The UE, however, responded again with another "security mode complete" upon receiving a second "security mode command" from the AMF, which is not compliant with the standard. The standard expects the UE to ignore or reject unexpected "security mode command" messages received after security mode completion, as accepting such messages could open the door to replay or downgrade attacks. Therefore, while the messages themselves were protected, the UE's willingness to process a repeated "security mode command" after security context establishment is a deviation from secure behavior as per 3GPP requirements. 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 successful completion of the 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 that was integrity protected and ciphered, indicating that the security context was active and messages were encrypted as per 3GPP standards. Upon receiving the Deregistration Request, the UE replied with a 5GMM Status message indicating "Invalid mandatory information," suggesting the UE detected an issue with the content or structure of the Deregistration Request. The UE then retransmitted additional messages, including another Service Request and an InitialUEMessage, but the AMF ultimately rejected the service, stating that the UE identity could not be derived. The key point here is the UE's response to the protected Deregistration Request: instead of blindly accepting or acting on a potentially malformed or abnormal message, the UE reported an error condition ("Invalid mandatory information") using a protected channel, which aligns with 3GPP security guidelines for robust error handling and message integrity checks. The UE did not proceed with deregistration or leak sensitive data, and all its messages after 5G-AKA were sent using security-protected NAS signaling, as required by the standard. This behavior demonstrates that the UE adhered to the 3GPP security requirements by maintaining message protection and validating the integrity and correctness of received messages before acting on them. Therefore, the UE's actions in this interaction were secure. 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, the UE completed the initial NAS steps and sent an authentication response to the AMF, after which the AMF issued an identity request for the SUCI (Subscription Concealed Identifier) in plain (unencrypted) NAS message format, as the 5G-AKA procedure had not yet been completed. The UE responded with an identity response, providing the requested SUCI. According to the 3GPP 5G security standards, before the completion of 5G-AKA, NAS messages are exchanged in plain text because the security context (ciphering and integrity protection keys) is not yet established. The SUCI is specifically designed to protect the subscriber's permanent identifier (SUPI) during transmission over an unprotected channel by concealing it with public key cryptography. Therefore, the UE's action of providing the SUCI in response to a plain identity request before security activation is in full compliance with the 3GPP standard and does not expose sensitive information. The UE did not transmit the SUPI directly and responded as specified, thus maintaining the intended security posture. Secure

89	89	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.12005400657653809 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12025594711303711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request 0.3216700553894043 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 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 an Identity Request message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). This Identity Request was sent as a plain (unencrypted) NAS message, as encryption of NAS signaling messages can only be established after successful completion of the 5G-AKA procedure. The UE responded to this request by sending an Identity Response message containing the requested SUCI, also in plain text. According to the 3GPP 5G standards, the SUCI is specifically designed to be a privacy-preserving identifier that can be safely transmitted over unprotected channels before authentication and key agreement are completed; it is a concealed version of the SUPI (Subscription Permanent Identifier) and does not reveal the subscriber's identity. Therefore, the UE's action of sending the SUCI in response to a plain Identity Request from the AMF, prior to the completion of 5G-AKA, is in line with 3GPP security guidelines and does not compromise the subscriber's privacy or security. The process followed by the UE is as intended by the standard for this stage of the NAS security context establishment. 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, the 5G standalone User Equipment (UE) first completed the initial NAS procedures and sent an Authentication Response to the AMF, but the 5G-AKA (Authentication and Key Agreement) procedure was not yet completed. Following this, the AMF sent an Identity Request message in plain (unencrypted) form, asking the UE for its SUCI (Subscription Concealed Identifier). The UE then responded with an Identity Response message containing the requested identity. According to the 3GPP 5G standards, before the completion of the 5G-AKA, the NAS signaling messages—including identity procedures—are permitted to be sent in plaintext, as encryption and integrity protection are only established after successful authentication and key agreement. The SUCI itself is a privacy-preserving identifier, designed to protect the subscriber's permanent identity (SUPI) even when sent over an unprotected channel. Therefore, the UE's action of responding with the SUCI in plaintext before NAS security was activated aligns with 3GPP security requirements and does not expose sensitive information. Based on this, the UE's behavior in this context was secure and compliant with 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 and key agreement), the UE sent a Service Request to the AMF, which was properly encrypted and integrity protected, as required by the 5G security specifications. The AMF, under test control, responded with a Deregistration Request message, also protected with both integrity and ciphering, indicating that the UE should be deregistered. In response, the UE sent a 5GMM Status message indicating "Invalid mandatory information." According to the 3GPP 5G standards (such as TS 24.501), when the UE receives a NAS message that is protected (integrity protected and ciphered) but contains invalid or unexpected mandatory information elements, the correct and secure behavior for the UE is to respond with a 5GMM Status message indicating the specific error. This allows for proper error handling and prevents the UE from acting on potentially malformed or malicious messages, while also maintaining the confidentiality and integrity of the communication. Therefore, the actions taken by the UE were in line with the 3GPP security requirements and best practices for error handling in protected NAS messaging. 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, the UE initiated a service request to the AMF, which was then followed by the AMF sending a deregistration request to the UE. Notably, this deregistration request from the AMF was integrity protected and ciphered, indicating that security context was established and the message was both encrypted and authenticated, as required by 3GPP standards for NAS security after 5G-AKA. The UE responded with a deregistration accept message, signifying compliance with the deregistration procedure. According to the 3GPP standard (TS 24.501), after security mode is established, all subsequent NAS messages, including deregistration, must be integrity protected and ciphered unless otherwise specified. Since the UE only responded to a properly protected and encrypted deregistration request, and did not act on any unprotected or suspicious messages, its behavior aligns with the expected secure operation defined by the 5G standard. Therefore, the UE's actions in this scenario were secure. 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, the UE and AMF completed the 5G-AKA authentication, after which the UE sent a Security Mode Complete message, indicating it had accepted the previous security parameters. However, the AMF then sent another Security Mode Command, this time with the ciphering algorithm 5G-EA4 and the integrity algorithm 5G-IA0 (null), and the message was protected using the new security context. 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 use of an integrity algorithm set to null (5G-IA0) is only permitted in very limited scenarios, and generally, integrity protection is mandatory for signaling messages to prevent tampering and replay attacks. The UE, by rejecting the security mode command that attempted to establish a security context with no integrity protection, was acting in accordance with the standard's security requirements and protecting itself from potential downgrade or null-encryption attacks. This behavior demonstrates that the UE correctly enforced 5G security policies by refusing to accept insecure parameters, thus maintaining the integrity and confidentiality of its communications. 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 requested the UE's identity (specifically the SUCI) via an identity request message sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. The UE responded to this request by transmitting an identity response, also in plain text, containing the SUCI. According to the 3GPP 5G security standard (TS 33.501), the SUCI (Subscription Concealed Identifier) is specifically designed to protect the user's permanent identifier (SUPI) during initial registration and before the establishment of a secure NAS connection. The SUCI is a privacy-preserving, encrypted version of the SUPI, intended to be sent over the air in plain text before security activation, and only the home network can decrypt it. Since the UE sent the SUCI (not the cleartext SUPI or IMSI) in response to the AMF's plain identity request before the security context was established, this behavior aligns with the 5G security requirements and does not expose the user's permanent identity. Therefore, the UE's actions in this scenario were secure and compliant with the 3GPP 5G 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 not compatible with the protocol state) 0.9204661846160889 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA procedure was completed, establishing a security context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). After this, the UE sent a Service Request uplink message, which was expected behavior as part of normal NAS procedures. The AMF then sent a Deregistration Request (UE terminated) as a downlink message, which was integrity protected and ciphered, indicating that it was both encrypted and authenticated as per 3GPP 5G security requirements. Upon receiving this protected deregistration request, the UE responded with a Deregistration Accept message, thereby following the protocol for handling such requests. According to the 3GPP 5G NAS protocol (TS 24.501), the UE is required to process properly protected deregistration requests from the AMF, even if the message type is unexpected in the current protocol state, as long as the message passes integrity and ciphering checks. Since the UE only responded to a protected, authenticated message after security establishment and did not process any unprotected or unauthenticated messages, its actions align with the security requirements of 5G NAS procedures. Therefore, the UE’s behavior was secure, as it did not accept or act on any insecure or improperly protected messages and strictly followed the 5G standard for handling NAS messages post-security activation. 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 User Equipment (UE) was interacting with the Access and Mobility Management Function (AMF) in a 5G standalone environment. After completing the initial NAS procedures, the UE sent an Identity Response, which was followed by an Identity Request from the AMF, specifically requesting the Subscription Concealed Identifier (SUCI). The UE then responded with another Identity Response. Notably, these messages were exchanged before the completion of the 5G Authentication and Key Agreement (5G-AKA) procedure, meaning that NAS security (encryption and integrity protection) had not yet been established. According to the 3GPP 5G standard, the initial identity exchange (including SUCI) is permitted to occur in plain text before the authentication and security context are established, as the SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) from exposure, even when sent without NAS security. Therefore, the UE's actions—responding to an AMF Identity Request for SUCI before 5G-AKA completion and without NAS encryption—are compliant with the 3GPP standard and do not expose sensitive information. Thus, the UE's behavior in this interaction was secure. 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 User Equipment (UE) and Access and Mobility Management Function (AMF) were engaged in NAS communication prior to the completion of 5G-AKA authentication. The UE responded to an identity request from the AMF by sending an identity response, specifically providing its SUCI (Subscription Concealed Identifier). After this, the AMF, under test control, sent another identity request to the UE, again requesting the SUCI, and the UE responded once more with an identity response. Importantly, all these exchanges occurred before the establishment of NAS security (i.e., before 5G-AKA completion), meaning the messages were transmitted in plaintext. According to the 3GPP 5G security standard, the UE is required to transmit the SUCI, which is a privacy-preserving, encrypted form of the permanent identifier (SUPI), in response to identity requests sent in plaintext before authentication and key agreement are completed. This mechanism is specifically designed to protect the subscriber's identity even when the transport is not yet encrypted. Since the UE correctly sent the SUCI (not the cleartext SUPI or IMSI) in response to identity requests before NAS security was established, it adhered to the security requirements of the 5G standard. Therefore, the UE's actions did not expose sensitive information and followed the proper security procedure as intended by 3GPP. 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, the UE initiated a service request to the AMF, which is a standard procedure to request access to network services. The AMF responded with a configuration update command, sent as a protected (integrity-protected) downlink NAS message, indicating that security procedures were correctly in place and a new security context was being used. Upon receiving this configuration update command, the UE responded with a 5GMM Status message, indicating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS protocol specifications, the UE should only accept certain NAS messages depending on its current protocol state. If the AMF sends a message that is not allowed in the UE's current state, the UE is expected to respond with a status message indicating the incompatibility, as a security and protocol compliance measure. This prevents the UE from processing unexpected or potentially malicious messages that could disrupt its state machine or compromise security. Therefore, the UE's action—responding with a 5GMM status message to signal the protocol violation—demonstrates correct and secure behavior as defined by the standard, ensuring that it does not accept or process messages that are not allowed in its current state. 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 the described 5G standalone security test, the UE first completed the 5G-AKA authentication procedure with the AMF, establishing the necessary security context for protected NAS communication. After this, the UE sent an Uplink NAS Transport message (PDU session establishment request), which, following 3GPP standards, should be integrity protected and ciphered post-authentication. The AMF then responded with a Downlink NAS Transport message containing a Service Accept, which was sent as a protected message. Notably, after receiving this protected message, the UE provided no response. According to the 3GPP 5G security specifications (TS 33.501), once the security context is established via 5G-AKA, the UE must only accept and process downlink NAS messages that are integrity protected and ciphered. Since the AMF sent a protected message and the UE did not respond, it indicates that the UE did not process or act upon the message in any insecure manner. This behavior aligns with security best practices, as the UE did not accept or respond to potentially untrusted or malformed messages and maintained the integrity of the secure communication channel. Therefore, based on the interaction and adherence to the 3GPP standard, the UE's actions were secure. Secure
100	100	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 92 UE provided: No response The packet capture during the test using wireshark is: 0.4685640335083008 UE to AMF UplinkNASTransport, Registration complete 0.4687800407409668 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Insufficient user-plane resources for the PDU session) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G-AKA authentication and security procedures, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior in the registration process. Subsequently, the AMF sent a protected (i.e., encrypted and integrity-protected) GMM Status message with cause 92 ("Insufficient user-plane resources for the PDU session") to the UE. The UE, upon receiving this protected status message, did not respond. According to the 3GPP 5G standard, specifically TS 24.501, section 8.2.22, the GMM Status message is used for error reporting and is not mandatory for the UE to respond to, especially if the message is protected and the cause code does not require a specific UE action. The lack of response from the UE is therefore compliant with the standard and does not indicate any security weakness. Furthermore, since all NAS messages after 5G-AKA were protected, the confidentiality and integrity of the communication were maintained. The UE's actions align with the 5G security requirements and best practices as outlined by 3GPP. 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 5G-AKA (authentication and key agreement), the UE sent an Uplink NAS Transport message, specifically a PDU session establishment request, to the AMF. Following this, the AMF responded with a Security Mode Command message, which was integrity protected with a new security context and specified the use of 128-5G-EA3 for ciphering and 128-5G-IA2 for integrity protection, as indicated by the security header. However, after receiving the Security Mode Command, the UE did not respond at all. According to the 3GPP 5G standard, after receiving a Security Mode Command, the UE is required to process the command, set up the new security context, and reply with a Security Mode Complete message, confirming acceptance and activation of the negotiated security algorithms. The absence of any response from the UE indicates a failure to follow the standard security procedure, which can leave the NAS signaling unprotected and the session in an undefined or insecure state. This lack of response could be interpreted as a vulnerability, as it prevents the proper establishment of secure communication as intended by the standard. Therefore, based on the 3GPP requirements for secure NAS signaling, the UE's action in this scenario was **insecure**. Insecure

102	102	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7492289543151855 UE to AMF UplinkNASTransport, Service request 0.749459981918335 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9532349109649658 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to initiate NAS signaling. The AMF then responded with a Security Mode Command message, which is used to establish NAS security (encryption and integrity protection) for subsequent messages. Notably, the Security Mode Command from the AMF specified the use of null algorithms for both ciphering (5G-EA0) and integrity protection (5G-IA0), meaning no actual encryption or integrity protection would be applied to NAS messages, even though the security header indicated "Integrity protected with new security context." Upon receiving this, the UE responded with a 5GMM Status message indicating "Invalid mandatory information," which suggests that the UE recognized the use of null security algorithms as invalid or insecure in this context and did not proceed further with NAS signaling. According to the 3GPP 5G security standards, null algorithms (EA0/IA0) are only to be used in specific, limited scenarios (such as emergency services or when explicitly permitted), and UEs are expected to reject or at least not accept null algorithms for normal protected communication after authentication. The UE's action to reject the Security Mode Command by reporting invalid mandatory information demonstrates adherence to the 5G security requirements and prevents insecure communication. Therefore, the UE acted securely in this scenario. 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 the described test scenario, after successful completion of the 5G-AKA authentication procedure, the User Equipment (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, under tester control, responded with a Deregistration Request message that was integrity protected and ciphered, as indicated by the security header. According to 3GPP standards, once the security context is established (as is the case after 5G-AKA), the UE is expected to process protected NAS messages from the AMF. However, in this test, the UE did not respond at all to the protected Deregistration Request. If the message was properly protected and formatted according to the standard, the UE should have at least acknowledged or processed it, even if it chose to reject or ignore the deregistration request content. The lack of any response suggests that the UE either failed to process a legitimate, protected NAS message or did not handle the deregistration procedure as required by 3GPP TS 24.501, which could indicate a security or interoperability issue. Given this, the UE's behavior appears to be non-compliant with the 5G standard, as secure UEs are required to handle such protected messages appropriately. 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, the UE and AMF successfully completed the 5G-AKA authentication procedure, establishing mutual authentication and deriving keys for NAS security. Following this, the UE sent an Uplink NAS Transport message (for PDU session establishment) to the AMF, and the AMF responded with a Deregistration Request (UE terminated) message, which was integrity protected and ciphered, indicating that NAS security was active. The UE, however, did not respond to the Deregistration Request. According to 3GPP TS 24.501, upon receiving a protected Deregistration Request from the AMF, the UE is expected to process the request and respond with a Deregistration Accept message, also protected, unless there is a specific reason not to (such as internal error or protocol violation). The lack of response from the UE to a properly protected, standard-compliant Deregistration Request is a deviation from expected secure behavior and could indicate a security or protocol handling issue on the UE side. In summary, while the UE did not transmit any unprotected or insecure messages, its failure to respond to a valid, protected NAS message from the AMF is not compliant with 3GPP security procedures and could be exploited in certain scenarios, thus representing insecure behavior. 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 to the AMF, which is a standard procedure for establishing a PDU session. The AMF then responded with a Configuration Update Command, which, as indicated by the security header, was both integrity protected and ciphered—meaning that it was encrypted and authenticated according to 3GPP standards. The UE then replied with a Configuration Update Complete message, acknowledging receipt and processing of the configuration update. Since the 5G-AKA procedure was completed before these NAS messages were exchanged, and the Configuration Update Command from the AMF was sent as a protected (integrity protected and ciphered) message, the UE's actions—responding only after receiving a properly protected message—align with the security procedures defined by 3GPP for 5G standalone networks. This ensures that sensitive information is not exposed and that the messages are not vulnerable to tampering or eavesdropping. Therefore, based on the sequence of events and the use of NAS security, the UE's actions were secure and compliant with the 5G standard. 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 security test, after successfully completing the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command, which was integrity protected and indicated the use of 5G-EA4 for ciphering and 128-5G-IA3 for integrity, with the security header showing that a new security context was in use. Upon receiving this command, the UE rejected it, explicitly citing a "UE security capabilities mismatch" in its Security Mode Reject message. According to 3GPP standards (TS 24.501), the UE is required to reject a Security Mode Command if the security algorithms proposed by the network do not match the UE's own capabilities, as this could indicate a misconfiguration or a potential security threat such as a downgrade or misalignment attack. The UE's rejection of the command upon detecting this mismatch demonstrates proper adherence to 5G security procedures, as it prevents the establishment of a security context with unsupported or insecure algorithms. Therefore, the UE's action was secure and in compliance with the 5G standard. 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, the User Equipment (UE) first completed the 5G Authentication and Key Agreement (5G-AKA) procedure, establishing a security context with the Access and Mobility Management Function (AMF). After this, the UE sent a "Registration complete" message, which was then acknowledged by the AMF. Subsequently, the AMF sent a "Deregistration request" to the UE; this message was protected, as indicated by the security header specifying integrity protection and ciphering. Upon receiving the protected deregistration request, the UE responded with a "Deregistration accept" message, signaling its compliance with the request. According to the 3GPP 5G standard, after 5G-AKA is completed, NAS messages between the UE and AMF must be both integrity protected and ciphered to ensure confidentiality and authenticity. The UE’s actions, including responding to a properly protected deregistration request only after a secure context was established, align with the security requirements of the standard. There is no indication that the UE accepted or responded to any unprotected or improperly protected messages, nor did it terminate its session without proper security procedures. Based on this sequence and the protections in place, the UE’s behavior was secure and in accordance with 3GPP requirements. Secure

108	108	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5200989246368408 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204448699951172 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7219538688659668 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of 5G-AKA (authentication and key agreement), the UE sent an Uplink NAS Transport message, which was followed by the AMF sending a Configuration Update Command. Notably, the AMF's downlink message was sent with integrity protection and a new security context, indicating that security procedures were correctly followed up to this point. Upon receiving the Configuration Update Command, the UE responded with a 5GMM Status message, indicating "Message type not compatible with the protocol state." According to the 3GPP 5G standard, after the security context is established, all subsequent NAS messages must be integrity protected and, where applicable, encrypted. The UE's action—responding with a status message when it receives an unexpected or out-of-sequence message—is in line with the protocol, as it ensures that the UE does not process messages that are not valid in its current state, thereby preventing potential attacks or protocol violations. This behavior demonstrates that the UE is correctly enforcing protocol state validation and is not accepting or acting on messages that could compromise its security or the integrity of the NAS procedure. Therefore, based on the observed behavior and adherence to the 3GPP standards, the UE's actions in this scenario were secure. 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 the 5G-AKA authentication procedure (which establishes security and encryption for NAS messages), the UE sent an Uplink NAS Transport message to the AMF, as expected in the protocol. The AMF, under test control, then sent a "GMM Status" message with a 5GMM Cause value of 98 ("Message type not compatible with the protocol state") as a protected (encrypted and integrity-protected) NAS message. In response, the UE sent a "5GMM Status" message with the same cause value back to the AMF, indicating its detection that the received message was not compatible with its current protocol state. According to 3GPP specifications (TS 24.501), when a UE receives a NAS message that is not compatible with its current protocol state, it is required to respond with a 5GMM Status message indicating this cause. Since the 5G-AKA procedure was completed prior to this exchange, all subsequent NAS messages, including the "GMM Status" messages, were protected as required by the standard. The UE's action—recognizing and reporting the protocol state mismatch—demonstrates correct and secure behavior as per 3GPP requirements, ensuring that it did not process an unexpected or potentially malicious message but instead followed the specified error handling. Therefore, the UE's behavior in this scenario aligns with the security expectations of the 5G standard. 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 successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a protected uplink NAS message indicating "registration complete" to the AMF, followed by a deregistration request. In response, the AMF sent a protected downlink NAS message with a 5GMM status indicating cause 101 ("Message not compatible with the protocol state"). Notably, the UE did not respond to this status message from the AMF. According to the 3GPP 5G NAS specifications (TS 24.501), after the security context is established (as ensured by the completion of 5G-AKA), all subsequent NAS messages should be integrity protected and, where required, encrypted. The UE correctly sent its registration complete message in a protected manner. Upon receiving a protected GMM status message with cause 101, the standard allows the UE to ignore such a message if it is not compatible with its current protocol state, especially since responding to an unexpected status could potentially lead to security vulnerabilities or protocol confusion. The UE's lack of response is therefore compliant with the standard, as it avoids unnecessary or potentially unsafe state transitions. Thus, the UE's behavior in this scenario demonstrates adherence to 3GPP security guidelines and proper protocol handling. 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 successfully completing 5G-AKA authentication (which establishes the security context), the UE sent a service request to the AMF. The AMF responded with a Security Mode Command, which was protected and indicated the use of the 5G-EA5 ciphering algorithm and the 5G-IA0 (null) integrity algorithm. The security header showed integrity protection with a new security context. Upon receiving this, the UE replied with a Security Mode Reject message, citing "UE security capabilities mismatch." According to the 3GPP 5G standard, the use of the null integrity algorithm (5G-IA0) is generally not allowed unless explicitly permitted by the UE's declared capabilities, as it would leave the NAS signaling vulnerable to tampering. The UE, recognizing that the requested security algorithms did not match its capabilities or security policy (likely because the AMF proposed no integrity protection), correctly rejected the security mode command. This behavior is in line with 3GPP security requirements, as the UE must not accept a security configuration that does not meet its minimum security standards. Therefore, the UE acted securely by refusing to proceed with insecure parameters. 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, the UE and AMF completed the 5G-AKA authentication, establishing a security context necessary for protected NAS communication. The UE then sent a Service Request to the AMF, which responded with a Security Mode Command, protected using the negotiated security algorithms (5G-EA5 for ciphering and 128-5G-IA2 for integrity protection) and indicating the use of a new security context. Upon receiving this command, the UE replied with a Security Mode Reject message, citing a mismatch in UE security capabilities. According to the 3GPP 5G security standard, a UE must reject a Security Mode Command if the algorithms or security parameters proposed by the network are not supported or are incompatible with its own capabilities. This prevents the establishment of a potentially insecure or non-functional security context. The UE's action to reject the security mode setup due to a capabilities mismatch is a correct and secure behavior as per the standard, ensuring that only mutually supported security algorithms are used for subsequent protected communication. This safeguards the UE from being forced into a security configuration it cannot properly support, thereby maintaining the integrity and confidentiality of its communication. 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 5G-AKA authentication, the UE sent a Service Request to the AMF, which responded with a Security Mode Command, protected using the negotiated ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms and marked as "Integrity protected with new security context." The UE then replied with a Security Mode Reject message, specifying the cause as "Security mode rejected, unspecified." According to the 3GPP 5G standard (TS 24.501), the UE is expected to reject a Security Mode Command only if it detects an issue such as an unsupported algorithm, an invalid security context, or if it cannot process the command for another valid reason. Since the Security Mode Command was properly protected and the security context was newly established after 5G-AKA, a rejection with an "unspecified" cause suggests that the UE did not provide a clear, standards-based reason for the rejection. This behavior could be considered insecure, as a standards-compliant UE should only reject security mode commands with a specific, justified cause, and an "unspecified" rejection may indicate improper handling of security procedures or a potential vulnerability. Therefore, while the UE did not accept an insecure context, its failure to provide a specific rejection reason is not fully aligned with 3GPP security requirements. Insecure
114	114	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5208940505981445 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215411186218262 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7234148979187012 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described test scenario, the 5G-AKA authentication and key agreement procedure was completed before the relevant NAS message exchanges, ensuring that both the User Equipment (UE) and the Access and Mobility Management Function (AMF) had established a shared security context. Following this, the UE sent an Uplink NAS Transport message, after which the AMF responded with a Configuration Update Command. Notably, this downlink message was protected using both integrity protection and ciphering, as indicated by the security header (2), signifying compliance with 3GPP requirements for message confidentiality and integrity after security activation. The UE then responded with a Configuration Update Complete message, acknowledging the command. Since the 5G-AKA was completed prior to these exchanges and the messages were protected accordingly, the UE's actions demonstrate adherence to the 3GPP 5G security standards for NAS signaling, maintaining the confidentiality and integrity of its communications. Therefore, the UE's actions in this sequence were secure and compliant with the 5G standard. 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 the described test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Service Request to the AMF, which then responded with a Security Mode Command. This Security Mode Command was properly protected, utilizing the ciphering algorithm 5G-EA4 and integrity algorithm 128-5G-IA3, and was marked as "integrity protected with new security context," indicating that the security context established during 5G-AKA was being used as per the 3GPP standard. However, upon receiving this command, the UE responded with a 5GMM Status message indicating "Invalid mandatory information," suggesting that the UE detected a problem or inconsistency in the Security Mode Command message. According to the 3GPP specification, if a UE receives a NAS message with invalid mandatory information, it should respond with a Status message to inform the network, which is exactly what the UE did. This behavior is compliant with the standard, as the UE did not proceed with insecure communication or attempt to establish security with incomplete or invalid parameters; instead, it notified the network of the issue. Thus, the UE acted securely and as expected by the 3GPP standard by refusing to proceed with an invalid security setup and reporting the error to the AMF. 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 5G standalone security test, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a PDU session establishment by sending an uplink NAS transport message to the AMF. The AMF then responded with a Security Mode Command, which was protected using the negotiated ciphering (128-5G-EA2) and integrity (128-5G-IA2) algorithms, and indicated the use of a new security context. Upon receiving this protected Security Mode Command, the UE responded with a Security Mode Reject message, specifying an unspecified reason for the rejection. According to the 3GPP 5G standards, after 5G-AKA, the UE should accept the Security Mode Command if the parameters (algorithms, ABBA, etc.) are valid and match the negotiated security context. A Security Mode Reject is only expected if the UE detects an issue—such as an unsupported algorithm, mismatched parameters, or a security threat (e.g., replay, downgrade, or integrity failure). Since the Security Mode Command was properly protected and followed the expected sequence, the UE's rejection without a specific reason ("unspecified") is not in line with the standard secure behavior, which expects the UE to provide a clear cause for rejection, especially after a successful authentication and protected command. This ambiguous rejection could indicate a flaw in the UE's security implementation or an inability to properly process the protected message, potentially exposing the UE to denial-of-service or downgrade attacks. Therefore, the UE's action in this scenario is considered insecure. Insecure

117	117	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.5606789588928223 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5618300437927246 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a UL NAS Transport message to the AMF, which is expected behavior as it indicates that the UE is attempting to establish a PDU session. Subsequently, the AMF responded with a Security Mode Command, which was properly protected (integrity protected and ciphered with the new security context established during 5G-AKA), using the specified cipher and integrity algorithms (5G-EA5 and 128-5G-IA1). According to the 3GPP 5G standard, upon receiving a Security Mode Command that is correctly protected, the UE is required to process the command, apply the new security context, and send a Security Mode Complete message back to the AMF, confirming that it has accepted and activated the new security parameters. In this test, the UE did not respond at all after receiving the Security Mode Command. This lack of response indicates that the UE failed to comply with the required 3GPP procedures, as it neither acknowledged nor established the agreed security context. From a security perspective, this is actually a secure behavior, because the UE did not proceed with communication under a potentially untrusted or unvalidated security context, nor did it continue to send any unprotected or improperly protected messages. However, from a protocol compliance perspective, the UE is non-compliant, as it should have sent a Security Mode Complete message. Since the focus here is on the security of the UE's action, and the UE refrained from insecure communication, its behavior can be seen as secure in this context, despite being non-compliant. Secure
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, the 5G-AKA authentication procedure was completed first, establishing a secure context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent an Uplink NAS Transport message, and the AMF responded with a Configuration Update Command. The packet capture indicates that this downlink message from the AMF was protected using both integrity protection and ciphering, as reflected by the security header value of (2). The UE then replied with a Configuration Update Complete message. According to the 3GPP 5G standards, after the successful completion of 5G-AKA, all subsequent NAS signaling messages between the UE and the AMF should be both integrity protected and ciphered to ensure confidentiality and authenticity. The actions taken by the UE—sending the Configuration Update Complete message in response to a protected command—are in line with these requirements, as the security context was already established and all further communication was protected. Therefore, the UE's behavior in this interaction adheres to the expected security protocols as per 3GPP standards. 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 the 5G-AKA authentication procedure, the UE initiated a NAS UplinkNASTransport message, and the AMF responded with a Security Mode Command. This Security Mode Command was protected (integrity protected with a new security context) and specified the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA1 integrity algorithm. Upon receiving this, the UE responded with a Security Mode Reject message, indicating "Security mode rejected, unspecified." According to the 3GPP 5G standard (TS 33.501), after authentication, the network must negotiate and activate both ciphering and integrity protection algorithms for NAS signaling. The use of 5G-EA0 (null ciphering) is allowed only under specific, controlled conditions (such as emergency services or regulatory requirements), but generally, the UE should reject Security Mode Commands that request null ciphering when not justified, to prevent unprotected transmission of sensitive information. The UE's rejection of the Security Mode Command that requested null ciphering, especially after a successful 5G-AKA (which establishes keys for secure communication), demonstrates adherence to security best practices as outlined by 3GPP. Therefore, the UE's action was secure, as it refused to proceed with a configuration that would leave its NAS messages unencrypted. Secure
120	120	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.46767306327819824 UE to AMF UplinkNASTransport, Registration complete 0.46790289878845215 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the 5G-AKA authentication procedure was completed successfully, indicating that both the UE and the AMF established mutual authentication and derived security keys for NAS signaling protection. Afterward, the UE sent a "Registration Complete" message to the AMF, and the AMF responded with a "Deregistration Accept" message, which was indicated as being "Protected"—meaning it was integrity protected and/or encrypted as per the 5G NAS security context. The UE, according to the test summary, did not respond to the protected "Deregistration Accept" message. According to the 3GPP 5G standard, specifically TS 24.501, upon receiving a valid, protected "Deregistration Accept" message from the network, the UE is expected to consider the deregistration procedure complete and does not need to send any further response. The absence of a response from the UE is therefore compliant with the standard and does not indicate any security weakness. The UE only processes protected NAS messages after security activation, and the message exchange observed here followed this requirement. Based on this analysis, the UE's actions adhered to the expected secure behavior as per 3GPP specifications. 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 steps and sent an authentication response to the AMF as part of the 5G-AKA authentication procedure. However, before the authentication and key agreement (5G-AKA) process was completed—which is required to establish NAS security and enable encryption and integrity protection of subsequent messages—the AMF sent a Service Reject message to the UE, using a plain (unencrypted) NAS message with 5GMM Cause 111 ("Protocol error, unspecified"). The UE, upon receiving this plain Service Reject message prior to the completion of 5G-AKA, did not respond further. According to the 3GPP 5G standard (TS 24.501), the UE is only required to accept plain NAS messages before NAS security is activated (i.e., before 5G-AKA is completed), and it is also permitted for the AMF to send a Service Reject in plain text in this situation. The UE's lack of response to the Service Reject, rather than proceeding with further communication or accepting the service reject in a way that could be exploited, aligns with the standard's security expectations, as responding to a plain Service Reject after security activation could open up denial-of-service or spoofing vulnerabilities. Therefore, the UE's behavior in this test scenario is consistent with 3GPP security requirements and does not introduce any security weaknesses in the context of the test. 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 the NAS registration procedure by sending an initial registration request to the AMF. The AMF, under tester control, responded with a plain (unencrypted) Service Reject message indicating "UE identity cannot be derived by the network" (5GMM Cause 9). Since the 5G-AKA authentication and key agreement procedure had not yet been completed, no NAS security context was established, and thus all NAS messages—including the Service Reject—were transmitted in plain text as per 3GPP standards. The UE, upon receiving the Service Reject, did not respond further. According to the 3GPP 5G specifications, before NAS security is established (i.e., before successful completion of 5G-AKA), the UE is expected to accept and process certain plain NAS messages, including Service Reject, and should not attempt to establish security contexts or respond further to a service reject with cause 9. The UE's behavior—sending the registration request, accepting the plain Service Reject, and not responding further—is compliant with the 3GPP standards and does not expose any security weakness, since it did not process sensitive information or accept insecure procedures outside the standard. Therefore, based on the observed interaction and the 3GPP security requirements, the UE acted securely in this scenario. 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 the test scenario, after the UE completed the initial NAS procedures and responded to an identity request, the AMF sent a Security Mode Command message to the UE. This message was protected (integrity protected with a new security context) and specified the cipher and integrity algorithms to be used. However, the 5G-AKA authentication procedure, which is essential for establishing the security context required for encryption and integrity protection of NAS messages, had not yet been completed. Upon receiving the Security Mode Command, the UE responded with a Security Mode Reject, citing an unspecified reason. According to the 3GPP 5G standard, the UE should only accept a Security Mode Command after successful completion of the authentication procedure, as accepting protected messages before authentication could expose the UE to security risks such as unauthorized access or man-in-the-middle attacks. The UE's decision to reject the Security Mode Command before the completion of 5G-AKA demonstrates adherence to the security requirements outlined in the standard, as it prevents the establishment of a potentially insecure security context. Therefore, the UE's action in this scenario was secure. 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 security test, the 5G standalone User Equipment (UE) engaged in NAS communication with the AMF, where the 5G-AKA authentication procedure had not yet been completed. The UE first sent an identity response, after which the AMF issued another identity request for the SUCI (Subscription Concealed Identifier), both of which were exchanged in plain (unencrypted) NAS messages, as is standard before the 5G-AKA procedure establishes security. According to 3GPP standards, identity request and response messages (particularly those involving the SUCI, which is a privacy-preserving, encrypted form of the SUPI) are permitted to be sent in cleartext before security activation, because the SUCI itself is designed to protect the subscriber's real identity even over an unprotected channel. The UE correctly responded to the AMF's plain identity request with a SUCI in the identity response, adhering to 3GPP security guidelines. Thus, the UE's actions were in alignment with the 5G standard and did not expose sensitive information in an insecure manner. 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, which was sent in plain (unencrypted) form, as the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards, specifically TS 33.501, the initial NAS messages exchanged before the completion of 5G-AKA (i.e., before NAS security context establishment) are allowed to be sent without encryption or integrity protection, as there is no shared key yet between the UE and the network. The critical security consideration in this scenario is how the UE responds to a plain Authentication Reject message received before security activation. The UE correctly provided no response to the Authentication Reject, which is the expected and secure behavior as per the standard: upon receiving an Authentication Reject before security activation, the UE should abort the registration procedure and not attempt further communication, as this could be an indication of an attack (e.g., a fake AMF attempting to force the UE off the network). Therefore, the UE's action in not responding is consistent with 3GPP security requirements and demonstrates secure behavior in this context. Secure
126	126	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5059909820556641 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5062329769134521 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7099969387054443 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement, the UE sent a "Registration Complete" message to the AMF, indicating the end of the initial NAS registration process. Following this, the AMF sent a "Deregistration Request (UE terminated)" message, which was integrity protected and ciphered, as indicated by the security header (2), meaning the message was both encrypted and authenticated using keys derived from the completed 5G-AKA procedure. The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, acknowledging the request. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages must be protected to ensure confidentiality and integrity. The UE’s actions—processing the protected deregistration request and responding with a deregistration accept—demonstrate compliance with the standard, as it only accepted a properly protected command and responded securely. There is no indication that the UE accepted or processed any unprotected or improperly protected NAS messages. Therefore, the UE’s behavior in this scenario was secure and in line with 3GPP requirements. 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 5G standalone User Equipment (UE) initiated NAS communication and, after completing the initial steps, sent an Identity Response message to the AMF. At this stage, the 5G-AKA authentication procedure had not yet been completed, meaning that the security context (including NAS encryption and integrity protection) had not been established. The AMF, under the tester's control, responded with a Deregistration Accept message sent in plain (unencrypted) format. According to the 3GPP 5G standard, until the 5G-AKA procedure is completed and security context is established, NAS messages between the UE and AMF are permitted to be sent in plain text. The UE, upon receiving the plain Deregistration Accept message before security activation, did not respond further, which is consistent with expected behavior since the message was correctly formatted and sent at an allowed phase of the protocol. Therefore, the UE's actions adhered to the 3GPP standard and did not expose itself to any additional security risks by accepting a plain Deregistration Accept message before security context activation. **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, the UE first sent an Identity Response to the AMF, after which the AMF replied with an Authentication Request. Notably, the Authentication Request was sent in plain (unencrypted) form, with both the RAND and AUTN fields set to all zeros, and the ABBA field set to 3031. Since the 5G-AKA procedure had not yet been completed, there was no security context established between the UE and the AMF, meaning that the NAS messages were not protected by encryption or integrity algorithms at this stage. Upon receiving the malformed Authentication Request, the UE responded with a 5GMM Status message indicating "Invalid mandatory information." According to 3GPP 5G security standards, a UE is expected to validate the integrity and correctness of critical fields in the Authentication Request, such as RAND and AUTN. If these fields are missing, invalid, or set to all zeros, the UE should not proceed with authentication and is expected to respond with an error or status message, as was observed here. This behavior prevents the UE from processing potentially malicious or malformed authentication challenges, which could compromise security. Therefore, the UE's action in this test—rejecting the invalid authentication request and not proceeding with authentication—aligns with the 3GPP security requirements and demonstrates a secure response to an insecure or non-standard network challenge. 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.	During this 5G standalone security test, the UE and AMF completed the 5G-AKA authentication procedure, after which the UE sent an authentication response. The AMF then issued a Security Mode Command to the UE, specifying the use of the null cipher algorithm (5G-EA0) and the integrity algorithm 128-5G-IA2, with the security header indicating "integrity protected with new security context." The Security Mode Command was sent as a protected message. Upon receiving this command, the UE responded with a Security Mode Reject message, citing "security mode rejected, unspecified" as the cause. According to 3GPP standards, after successful authentication, the establishment of a secure NAS connection requires both integrity and confidentiality protection. The use of 5G-EA0 (null ciphering) means that user plane and NAS messages would not be encrypted, exposing user data to potential eavesdropping. 3GPP TS 33.501 specifies that UEs should reject security mode commands that only offer null encryption unless explicitly allowed by the network policy and user agreement, as this could compromise confidentiality. The UE's rejection of the security mode command under these conditions demonstrates adherence to 3GPP security requirements and best practices, as it avoids operating with insufficient encryption. Therefore, the UE's behavior in this scenario was secure. 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, prior to completion of the 5G-AKA procedure. The UE then responded with an authentication failure message, specifically indicating "Non-5G authentication unacceptable." According to 3GPP 5G security standards, NAS messages containing authentication requests must be protected by integrity and confidentiality mechanisms, which can only be established after successful completion of the 5G-AKA procedure. Sending authentication requests in plain text before security context establishment is not compliant with 3GPP security requirements. The UE correctly identified that the authentication request was not properly protected and refused to proceed with authentication, as indicated by its "Non-5G authentication unacceptable" response. This behavior aligns with 5G security best practices and the requirements outlined by 3GPP TS 33.501, which mandate that sensitive NAS messages must not be processed by the UE unless they are properly protected. Therefore, the UE's action was secure and compliant with the 5G standard. Secure
131	131	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00038909912109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a registration request to the AMF. The AMF, under test control, responded with a plain (unencrypted) Registration Reject message, carrying 5GMM Cause 26 ("Non-5G authentication unacceptable"), before any 5G-AKA authentication procedure was completed. According to the 3GPP 5G security standard, NAS messages between the UE and the AMF are transmitted in plain text until mutual authentication and key establishment (5G-AKA) are completed; only then can NAS message integrity protection and ciphering be activated. The UE, upon receiving the Registration Reject message prior to authentication, did not respond further, which is correct behavior as per the standard: the UE should only accept such messages in plain text before authentication and should not proceed with further registration attempts unless specifically allowed by the cause code or timer expiry. Since the UE did not attempt to send any sensitive or protected information before authentication and did not react inappropriately to the plain Registration Reject, its actions were in line with 3GPP security requirements for this phase of registration. Therefore, the UE's behavior in this scenario was secure. 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, after completing the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected to be unprotected since 5G-AKA authentication and key agreement had not yet been completed. Subsequently, the AMF (under tester control) responded with a Service Reject message, also sent in plain (unencrypted) form, with a 5GMM cause value of 99, indicating "Information element non-existent or not implemented." The UE, upon receiving this message, did not respond further. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are allowed to be sent in plain text, as there is no established key to provide NAS message protection. The UE's behavior—sending an unprotected Identity Response and not responding further after a Service Reject—is consistent with the standard. The UE did not proceed with any further communication or attempt to establish a secure session after the Service Reject, which is the correct and secure behavior as per 3GPP guidelines. Therefore, the UE's actions in this scenario do not expose it to any additional security risk beyond what is permitted by the standard at this stage of the protocol. 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 the AMF's identity request with an identity response message. Subsequently, the AMF sent an authentication request to the UE, but crucially, this authentication request was transmitted in plain (unencrypted) form before the completion of the 5G-AKA (Authentication and Key Agreement) procedure, which is required to establish a secure context for further communication. Upon receiving this plain authentication request, the UE replied with an "Authentication failure" message, specifically indicating "Non-5G authentication unacceptable." According to the 3GPP 5G security standards, the 5G-AKA procedure must be successfully completed to establish mutual authentication and derive the security keys necessary for encryption and integrity protection of subsequent NAS messages. If the authentication request is sent in plain text before security is established, a compliant and secure UE should not accept or process such requests and should instead reject them, as was observed in this test. This behavior prevents potential interception or tampering with sensitive authentication information. Therefore, the UE's action in rejecting the plain authentication request before 5G-AKA completion aligns with the 5G security standards and demonstrates correct and secure handling of the authentication procedure. 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 sent an Identity Response message in plain text, which is expected because the 5G-AKA authentication and key agreement procedure—responsible for establishing NAS security and enabling encryption—had not yet been completed. The AMF, under tester control, responded with a Service Reject message (cause: Illegal UE, 5GMM Cause 3), also sent in plain text. Following this, the UE did not respond further. According to the 3GPP 5G standards, initial NAS messages exchanged before the completion of 5G-AKA are permitted to be sent unencrypted, as security context has not yet been established. The UE's behavior—sending identity information in plain text prior to authentication, and not responding to a service reject—aligns with standard procedures and does not introduce a security vulnerability in this context, since encryption is only mandated after successful authentication. Therefore, based on the described interaction and adherence to 3GPP security procedures, the UE's actions were appropriate and secure for this stage of the protocol. 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, after the UE initiated the registration procedure by sending an InitialUEMessage containing a Registration Request, the AMF responded with a Security Mode Command. However, the AMF chose to use null algorithms for both ciphering (5G-EA0) and integrity protection (5G-IA0), and set the security header to indicate "Integrity protected with new security context." Critically, the 5G-AKA authentication procedure had not yet been completed, which means no valid security context or keys had been established between the UE and the network. According to the 3GPP 5G security specifications (TS 33.501), the use of null algorithms is only permitted under very specific circumstances, for example, when the UE explicitly supports it and the network allows it, and never before authentication and key agreement are complete. Furthermore, the security context must be established through 5G-AKA before any security mode command is accepted and before any messages are protected with integrity or ciphering. The UE, upon receiving a security mode command with null algorithms and without a valid security context (since 5G-AKA was not completed), correctly rejected the security mode command by sending a Security Mode Reject message with an unspecified reason. This behavior aligns with 3GPP security requirements, as accepting such a command would expose the UE to significant security risks, such as man-in-the-middle attacks or unauthorized access. Therefore, the UE's action was secure and compliant with the 5G standard. 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 initial NAS procedures, the UE responded to an identity request with an identity response. Subsequently, the AMF sent a Security Mode Command to the UE, indicating the use of the null cipher algorithm (5G-EA0), an integrity algorithm (128-5G-IA3), and specifying "Integrity protected with new security context" in the security header. However, the 5G-AKA authentication procedure had not yet been completed, meaning that a valid NAS security context (with keys derived from authentication) was not yet established. The UE, upon receiving a Security Mode Command that attempted to establish NAS security before authentication, correctly rejected the command with a "Security mode reject (Security mode rejected, unspecified)" message. According to 3GPP 5G standards (TS 33.501 and TS 24.501), the UE must not accept security mode commands that attempt to establish NAS security before successful authentication and key agreement, as this would expose the UE to potential security vulnerabilities, including man-in-the-middle attacks or replay attacks. By refusing to proceed with NAS security setup before 5G-AKA, the UE acted in accordance with the security requirements of the standard. This demonstrates that the UE's action was secure and compliant with 3GPP security guidelines. 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 first completed initial NAS steps and then sent an Authentication Response to the AMF. The AMF, under your control, subsequently sent another Authentication Request to the UE, and this message was transmitted in plain (unencrypted) form, as 5G-AKA had not yet been completed. The UE responded with another Authentication Response. According to the 3GPP 5G standard, NAS messages prior to the completion of 5G-AKA are indeed sent without encryption, as mutual authentication and key establishment have not yet taken place. However, a key security expectation is that the UE should only respond to a single Authentication Request in a given authentication sequence and should not respond to unexpected or repeated Authentication Requests after already having sent an Authentication Response, unless a new authentication procedure has been properly initiated. The fact that the UE responded again to a second, unsolicited Authentication Request—while the authentication procedure was not properly restarted—indicates it did not properly track the state of the authentication process, potentially allowing replay or reflection attacks. This behavior is not compliant with the security requirements outlined by 3GPP, which expects the UE to ignore or reject such out-of-sequence or repeated authentication challenges. Therefore, the action taken by the UE in this scenario is considered insecure. Insecure

138	138	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5089499950408936 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5091559886932373 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7129359245300293 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the registration process had concluded. The AMF, under test control, then sent a "Deregistration Request (UE terminated)" message to the UE. This message was integrity protected and ciphered, as indicated by the security header (2), demonstrating that NAS security had been activated following the 5G-AKA procedure. The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to the 3GPP 5G standard, after the 5G-AKA is completed, all subsequent NAS messages must be integrity protected and ciphered to ensure confidentiality and integrity of signaling. The UE only responded to a properly protected and encrypted deregistration request, and its actions aligned with the expected secure behavior defined by the standard. Therefore, the UE's handling of the NAS deregistration procedure was secure, as it only accepted and responded to protected messages after security activation. 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 simulated 5G standalone security test, the UE initiated a registration by sending an InitialUEMessage containing a registration request to the AMF. In response, the AMF sent an Authentication Request message to the UE, but this message was sent as plain (unencrypted) and contained an invalid AUTN (all zeros), a specific RAND, and ABBA set to 0000. Notably, the 5G-AKA authentication procedure had not yet been completed, which means that a security context had not been established and subsequent NAS messages should not yet be encrypted. Upon receiving the plain and malformed Authentication Request, the UE did not proceed with authentication; instead, it responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G NAS protocol specifications, when the UE receives an authentication request with missing or invalid mandatory information prior to security activation, it is expected to respond with a status message indicating the error, and this status message may be sent in plain since security is not yet established. Therefore, the UE's action—rejecting the malformed authentication request and not proceeding with authentication—adhered to the expected secure behavior as per the standard, ensuring that it did not process invalid authentication material or expose sensitive information before authentication and security activation. 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 registration with the AMF by sending an InitialUEMessage containing a Registration Request. In response, the AMF sent an Authentication Request message in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning no NAS security context (encryption and integrity protection) was established. Upon receiving the plain (unencrypted) Authentication Request, the UE immediately responded with a Deregistration Request (UE originating), effectively aborting the registration and authentication process. According to the 3GPP 5G standard, it is expected and required that NAS messages prior to the completion of authentication and key agreement are sent in plain text, as encryption can only be applied after security keys are established through 5G-AKA. However, it is also expected that the UE should only abort the procedure if it detects an anomaly (such as an invalid AUTN, failed authentication, or other protocol errors). In this case, since the AMF sent a standard Authentication Request with plausible parameters, the UE's immediate deregistration suggests it did not proceed with authentication, which could indicate either a failure to handle the authentication step or an overly cautious security posture. If the UE aborted the procedure due to a legitimate detection of an invalid or suspicious authentication challenge (for example, a replayed or malformed AUTN), this would be considered secure behavior. However, if the UE aborted the process without attempting to verify the authentication parameters or without a valid security reason, it would be considered insecure as it fails to comply with the standard authentication flow, potentially causing unnecessary service denial. Without further evidence of an invalid authentication challenge, the UE's action appears premature and not fully compliant with the 3GPP standard authentication procedure. Insecure
141	141	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.17494893074035645 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.17513012886047363 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and the AMF engaged in NAS communication where, after the initial steps, the UE sent an Authentication Response message to the AMF. In response, the AMF sent back an Authentication Reject message, which was transmitted in plain (unencrypted) form. The 5G-AKA procedure, which establishes mutual authentication and derives keys for NAS encryption and integrity protection, had not yet been completed at this point in the exchange. According to 3GPP standards (TS 24.501), all NAS messages exchanged before the completion of 5G-AKA—including authentication and security mode commands—are sent in plain text, as encryption and integrity protection are only enabled after successful authentication and security mode procedures. The UE, upon receiving the Authentication Reject message, provided no further response, which is the expected behavior according to the specification, as the UE should consider itself unauthenticated and not proceed with further NAS communication. Therefore, the UE's actions were in line with 3GPP security guidelines, as it did not send any sensitive information in plain text after receiving the reject, and did not attempt to continue communication without proper authentication and security context established. 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 the described test scenario, after the usual NAS procedures, the UE sent an authentication response to the AMF, which then replied with another authentication request sent in plain (unencrypted) format. The UE responded to this with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security specifications, specifically TS 33.501, the 5G-AKA procedure must be successfully completed before any security context is established, and only after that should NAS messages be encrypted and integrity protected. If the AMF sends authentication requests in plain text after an authentication response, it is not following the expected 5G-AKA flow. The UE, recognizing this deviation and the lack of proper security context, correctly rejected the request as "Non-5G authentication unacceptable." This behavior aligns with 3GPP standards, as the UE must not accept authentication procedures that do not conform to the 5G-AKA protocol or that present a risk of downgrade or replay attacks. By refusing further authentication in the absence of a valid 5G security context, the UE demonstrated secure and standards-compliant behavior. Secure
143	143	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5046439170837402 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 0.5048840045928955 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test scenario, the UE and AMF completed the 5G-AKA authentication procedure, establishing a secure channel for NAS communication. The UE then sent a "Registration Complete" message, indicating the end of the registration process. Subsequently, the AMF sent a "Deregistration Request" to the UE. Importantly, this downlink message from the AMF was both integrity protected and ciphered, as indicated by the security header, meaning it was encrypted and authenticated according to 3GPP 5G security standards. However, the UE did not respond to the deregistration request. According to the 3GPP standard, after a protected deregistration request is received, the UE is expected to process the request and respond appropriately (for example, with a deregistration accept message). The absence of any response from the UE indicates a failure to properly handle a legitimate, protected message as required by the standard. This could leave the UE in an inconsistent state and potentially open to denial-of-service or other protocol-related issues. Therefore, while the initial communication was secure, the UE's lack of response to a properly protected message is not compliant with 3GPP expectations for secure and robust behavior. Insecure

144	144	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5077369213104248 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080108642578125 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.7157459259033203 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the User Equipment (UE) sent a "Registration Complete" message to the Access and Mobility Management Function (AMF), indicating that it had finished the registration process. Following this, the AMF sent a "Configuration Update Command" to the UE, which was observed in the packet capture as being both integrity protected and ciphered, meaning it was encrypted and authenticated according to the security requirements of the 3GPP 5G standard. The UE then responded with a "Configuration Update Complete" message, confirming receipt and processing of the command. Since 5G-AKA was completed prior to these exchanges, the security context for both integrity protection and encryption was already established. The UE's actions—accepting and responding only to protected (integrity protected and ciphered) NAS messages after authentication—are fully in line with 3GPP specifications, which require that sensitive signaling messages be protected after security activation. Therefore, based on the outlined interaction and the fact that the UE only processed and responded to protected messages after authentication, the UE's behavior is considered secure according to the 5G standard. Secure
145	145_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15980100631713867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16017889976501465 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3686530590057373 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the security algorithms and parameters negotiated during the security mode command process. However, immediately after receiving this "security mode complete," the AMF sent another "security mode command" message to the UE, which is not the expected flow according to 3GPP standards. The UE then responded with another "security mode complete" message, essentially accepting a second security mode command within the same session. According to 3GPP TS 24.501, once the security context is established and the UE has responded with a "security mode complete," the AMF should not send a second "security mode command" unless a new security context is being established (e.g., after a mobility event or context loss). The UE, in this case, accepted and responded to the redundant security mode command without rejecting it or raising an error, which could expose it to replay or downgrade attacks if exploited by a malicious network element. Therefore, the UE's action of accepting multiple consecutive security mode commands within the same security context does not align with the secure behavior expected by the 3GPP standard and may represent a security vulnerability. 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, after completing the 5G-AKA authentication and key agreement process, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security parameters (ciphering and integrity protection algorithms) and was ready to begin protected NAS communication. Immediately following this, the AMF sent a "deregistration accept" message, which was properly protected (encrypted and integrity protected) as indicated in the test summary. The UE, upon receiving the protected "deregistration accept," did not respond further, which is expected behavior since a "deregistration accept" is a terminal message in the deregistration procedure and does not require an acknowledgement from the UE according to 3GPP standards (TS 24.501). The packet capture also confirms that all NAS messages after security mode complete were exchanged as protected messages, which aligns with the 5G security procedures. Since the UE only sent protected NAS messages after security activation and did not respond to a protected "deregistration accept" (which is correct per the standard), the UE's actions were secure and compliant with 3GPP requirements. Secure
147	147	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.15987586975097656 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16038084030151367 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.3645758628845215 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement (which establishes the security context for NAS communication), the UE sent a "security mode complete" message to the AMF, indicating that it had activated the negotiated NAS security algorithms. Subsequently, the AMF sent a "configuration update command" as a protected (integrity-protected and ciphered) downlink NAS message, as indicated by the security header "Integrity protected with new security context (3)." Upon receiving this, the UE responded with a "5GMM status" message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS protocol (TS 24.501), once the security context is established, all subsequent NAS messages must be integrity-protected and, if required, ciphered. The receipt of a protected configuration update command from the AMF was expected, and the UE's response—sending a 5GMM status message—suggests that it detected the configuration update command as unexpected or not allowed in its current protocol state. This behavior is correct and aligns with 3GPP specifications, as the UE must reject or indicate protocol errors for messages that are not compatible with its state, rather than processing potentially invalid or malicious commands. By providing a status message (rather than, for example, failing silently or acting on an invalid command), the UE demonstrates robust and secure protocol handling as per 3GPP standards. Therefore, the UE's actions in this scenario were secure. 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 and key agreement procedure, the UE sent a Security Mode Complete message, indicating that it had accepted the negotiated NAS security algorithms and was ready to begin protected communication. Following this, the AMF sent a Deregistration Request (UE terminated) message, which was integrity protected and ciphered, as indicated by the security header (2). The UE responded with a Deregistration Accept message, completing the deregistration procedure. According to the 3GPP 5G standard (TS 24.501), after the security mode is established, all subsequent NAS messages between the UE and AMF must be integrity protected and ciphered to ensure confidentiality and authenticity. In this test, the UE only sent messages (including the deregistration accept) after security was activated, and all its transmissions were in accordance with the security context established via 5G-AKA and the security mode procedure. There is no indication that the UE accepted or responded to any unprotected NAS messages after security activation, nor did it violate any security procedures. Therefore, based on the observed behavior and compliance with 3GPP security requirements, the UE's actions were secure. 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 security 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 security algorithms and parameters negotiated (Cipher: 5G-EA7, Integrity: 128-5G-IA2). However, following this, the AMF sent another "security mode command" message to the UE, which is unusual because, according to the 3GPP 5G standard, the security mode command should only be sent once per security context establishment, and the UE should only respond once with a "security mode complete" message. The packet capture confirms that the UE sent a second "security mode complete" message in response to the unexpected, repeated security mode command from the AMF. From a security perspective, this behavior is problematic. The UE should not accept and process a second security mode command in the same context, as this could be exploited by an attacker to downgrade or alter security parameters, violating the 3GPP security requirements that protect against replay and downgrade attacks. The correct and secure behavior would be for the UE to ignore or reject unexpected or repeated security mode commands once the security context has been established. Therefore, the UE's acceptance and response to a repeated security mode command indicates a security weakness in its implementation. 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, the 5G standalone User Equipment (UE) first completed the 5G-AKA authentication and key agreement procedure, ensuring that both the UE and the Access and Mobility Management Function (AMF) had established a shared security context. Following this, the UE sent a Security Mode Complete message, indicating that it had successfully configured the security algorithms and was ready to communicate securely. The AMF then sent a Deregistration Request to the UE, which was integrity protected and ciphered, as indicated by the security header (2), meaning both confidentiality and integrity protections were active. The UE responded with a Deregistration Accept message, completing the deregistration process. According to 3GPP standards, after the successful completion of 5G-AKA and security mode procedures, all subsequent NAS messages—such as the Deregistration Request and Accept—must be protected using the agreed-upon security algorithms. The packet capture confirms that the UE only responded to a properly protected (integrity protected and ciphered) Deregistration Request, and its subsequent message was sent in the expected secured manner. This behavior adheres to the 3GPP requirements for NAS message protection, demonstrating that the UE did not accept or respond to any unprotected or improperly protected messages and maintained the integrity and confidentiality of its communication throughout the interaction. Therefore, the action taken by the UE was secure and compliant with the 5G standard. Secure
151	151	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00026297569274902344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration procedure by sending an initial registration request to the AMF. In response, the AMF sent an identity request message, specifically requesting the UE's GUTI (Globally Unique Temporary Identifier). Importantly, this identity request was sent in plain (unencrypted) form, which is allowed by the 3GPP 5G standard prior to the completion of the 5G-AKA authentication and key agreement procedure. According to the 3GPP TS 33.501 specification, the UE should not disclose sensitive permanent identifiers (such as SUPI/IMSI) in the clear before a secure NAS connection is established; however, responding with a GUTI in plain text is considered acceptable, as GUTI is a temporary, non-sensitive identifier designed for such scenarios. In this test, the UE took no action and did not respond to the AMF's plain identity request for GUTI. While the UE's lack of response does not expose any sensitive information, it also means the registration procedure cannot proceed. From a security perspective, the UE's action is cautious, erring on the side of not disclosing even a temporary identifier in plain text, which is stricter than the standard requires. Therefore, the UE's behavior is secure, as it avoids any risk of identifier exposure, even if this means failing to progress in the registration process. 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, after the UE sent an initial registration request to the AMF, the AMF responded with a configuration update command that was marked as "protected" but with an unknown security header and before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, user and signaling messages between the UE and AMF should only be integrity-protected and/or ciphered after successful completion of the 5G-AKA procedure, which establishes the necessary security context and keys. Since the UE had not yet completed 5G-AKA, it would not have the security keys required to validate or decrypt protected NAS messages. The UE's action of not responding to the configuration update command is, therefore, appropriate and secure, as it prevents the processing of potentially unauthenticated or spoofed management commands before a secure context is established. This behavior aligns with 3GPP specifications, which require the UE to ignore or reject protected NAS messages if a security context is not established. 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 registration by sending an initial registration request to the AMF. The AMF responded with a Security Mode Command message that was marked as "protected" and specified the use of ciphering algorithm 128-5G-EA3 and integrity algorithm 5G-IA0 (null), with a security header indicating "integrity protected with new security context." However, the 5G-AKA authentication procedure had not been completed, meaning that the necessary keys for encryption and integrity protection were not yet established between the UE and the network. When the UE received this Security Mode Command, it responded with a 5GMM status message indicating "Invalid mandatory information," signaling that it did not accept or process the message as valid. According to the 3GPP 5G security standards, the UE must not accept or process security mode commands that are protected using keys derived from an incomplete authentication process, as this would expose the UE to potential security risks (such as accepting commands based on unauthenticated or untrusted keying material). By refusing to process the Security Mode Command in the absence of completed 5G-AKA, the UE correctly adhered to the 3GPP security protocols, thereby preventing a potential security vulnerability. Therefore, the action taken by the UE in this interaction was secure. Secure

154	154	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0009160041809082031 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the User Equipment (UE) initiated the registration process by sending an initial registration request to the Access and Mobility Management Function (AMF). After receiving this request, the AMF responded with a Configuration Update Command, which was sent as a downlink NAS message marked as "integrity protected and ciphered," indicating that it was protected by NAS security. However, the 5G-AKA (Authentication and Key Agreement) procedure, which is essential for establishing the necessary security context (i.e., deriving encryption and integrity keys), had not yet been completed at this stage. According to the 3GPP 5G standard, NAS security (encryption and integrity protection) must only be applied after successful authentication and key agreement. Since the UE had not yet completed 5G-AKA, it correctly refused to process or respond to the protected Configuration Update Command, as it did not yet possess the required security keys. This behavior demonstrates that the UE adhered to the 3GPP security requirements by not accepting protected messages before authentication was complete, thereby preventing potential security risks such as replay or spoofing attacks before a secure context is established. 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 Initial Registration Request to the AMF, as observed in the packet capture. However, before the 5G-AKA authentication and key agreement procedure was completed—which is essential for establishing NAS security and enabling encryption and integrity protection—the AMF sent a Deregistration Accept message to the UE. Notably, this message was sent as "protected," meaning it was cryptographically secured, even though the 5G-AKA had not yet completed and thus no security context should have been established. The UE, in response, provided no further messages or acknowledgments to this protected downlink message from the AMF. According to the 3GPP 5G security standards, the UE must not accept or process protected NAS messages from the network before a security context is established via 5G-AKA, as the cryptographic keys required for protection are only derived during and after this procedure. The UE's lack of response indicates that it correctly rejected or ignored the protected message, which is the expected and secure behavior per the standard. Thus, the UE's actions were in line with 3GPP security requirements for NAS communication prior to the completion of 5G-AKA. 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 security test, after the initial registration request was sent by the UE, the AMF responded with a Security Mode Command that was protected using null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, and indicated integrity protection with a new security context before the completion of the 5G-AKA authentication procedure. The UE, upon receiving this command, responded with a Security Mode Reject message, specifying that the security mode was rejected for an unspecified reason. According to the 3GPP 5G standards, secure NAS communication requires that the 5G-AKA procedure is completed to establish cryptographic keys before any security mode command using actual protection algorithms is accepted; using null algorithms (EA0/IA0) is only permitted in specific, limited scenarios (e.g., for emergency services) and not for normal registration. The UE's refusal to accept the security mode command under these conditions demonstrates adherence to the security requirements of the standard, as accepting null security or prematurely applying a new security context without proper authentication would expose the UE to significant security risks, such as man-in-the-middle or downgrade attacks. Therefore, the UE's action to reject the security mode command in this context was the correct and secure response according to 3GPP guidelines. 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 security test, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under tester control, responded with a Deregistration Request message that was protected with integrity and ciphering, as indicated by the security header. However, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the necessary security context for encryption and integrity protection had not been established between the UE and the network. According to 3GPP 5G standards, the UE should only accept and process NAS messages with integrity protection and ciphering after a successful 5G-AKA, which establishes the required keys and security context. Since the AMF sent a protected message before the security context was established, and the UE did not respond to this message, the UE's behavior is correct and secure—it refused to process a protected message before mutual authentication and key agreement. This action prevents potential security vulnerabilities, such as replay or spoofing attacks, that could arise if the UE accepted protected messages without prior authentication. Therefore, the UE's lack of response in this scenario aligns with 3GPP security requirements. 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 steps, the UE sent an identity response to the AMF, after which the AMF, still before completing the 5G-AKA authentication procedure, sent another identity request for the IMEISV in plain (unencrypted) NAS. The UE did not respond to this request. According to the 3GPP 5G security standard, sensitive information such as the IMEI/IMEISV should not be transmitted over the air in plain text after the initial registration steps, unless the NAS security context has been established (i.e., after 5G-AKA is completed and encryption is active). The UE's refusal to respond to the plain IMEISV request before the completion of 5G-AKA and establishment of NAS security aligns with the security requirements set by 3GPP to protect device identity from exposure to potential attackers. By not sending the IMEISV in the clear, the UE prevents possible device tracking or identification by malicious entities. Thus, the UE's action demonstrates adherence to the standard and good security practice. 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, after completing the initial NAS procedures, the UE sent an Identity Response to the AMF, which was expected and compliant with the standard. The AMF then replied with a GMM Status message carrying the cause "Roaming not allowed in this tracking area" (5GMM Cause: 13), and crucially, this message was sent in plain (unencrypted) form. The 5G-AKA security procedure had not yet been completed, meaning that NAS-level encryption and integrity protection were not yet established. According to 3GPP standards, before the completion of 5G-AKA, NAS messages (including Identity Response and Status) are allowed to be sent in plain text, as security context has not yet been derived. The UE did not respond to the GMM Status message, which is also compliant with the standard, as the UE is not required to respond to a status message with cause 13, especially before security activation. Therefore, the UE's actions—sending messages in plain before security is established, and not responding to the status message—align with 3GPP security requirements and do not expose the UE to additional risk in this context. The UE did not act insecurely in this exchange. 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 security test, the UE and AMF exchanged NAS messages during the initial phase of 5G registration, with 5G-AKA (authentication and key agreement) not yet completed. The UE sent an Identity Response message, and the AMF replied with a Configuration Update Command as a plain (unencrypted and unauthenticated) NAS message, indicated by the security header type "Plain NAS message (0)." According to 3GPP 5G standards, before 5G-AKA is completed, NAS messages are allowed to be sent in plain text, as security contexts and encryption keys have not yet been established. However, after receiving a plain Configuration Update Command before authentication, the UE did not respond. This is the correct and secure behavior as per 3GPP TS 24.501, which specifies that certain NAS procedures, such as configuration updates, should only be accepted after security activation to prevent potential security risks like spoofing or manipulation by an unauthorized entity. By not responding to a plain configuration update command before security was activated, the UE demonstrated secure behavior in compliance with the 5G standard. Secure
161	161	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0400080680847168 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04023408889770508 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). The UE sent an identity response message to the AMF before the 5G-AKA (Authentication and Key Agreement) procedure was completed, meaning that security context establishment—specifically NAS integrity and encryption—had not yet occurred. Subsequently, the AMF sent a deregistration accept message, which was protected (integrity protected and/or encrypted), but the UE did not respond to this message. According to the 3GPP 5G security standard, NAS message protection (integrity and encryption) is only possible after the successful completion of the 5G-AKA procedure. Any NAS messages exchanged before security context activation, such as the identity response, are sent unprotected, which is compliant with the standard. When the AMF sent a protected deregistration accept message before security context establishment, the UE appropriately did not respond, as it would not be able to verify or decrypt the message without the necessary keys from 5G-AKA. This behavior demonstrates that the UE adhered to the security requirements set by 3GPP, as it did not process a protected message before security activation and did not allow a potential downgrade or confusion attack. Therefore, the actions taken by the UE in this interaction were secure and in compliance with 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, after initial NAS procedures, the UE sent an Identity Response message to the AMF, which is an expected step when the network requests the UE's identity. Importantly, this interaction occurred before the completion of the 5G-AKA authentication and key agreement procedure. According to the 3GPP 5G standard, NAS message protection (encryption and integrity) is only applied after successful authentication and the establishment of security context via 5G-AKA. In this test, the AMF, under tester control, sent a Service Accept message to the UE as a protected (encrypted/integrity-protected) NAS message, even though 5G-AKA had not yet been completed. The UE did not respond to this message. This behavior aligns with the 3GPP security requirements, which state that a UE must not process or respond to protected NAS messages before security context is established, as it would not have the necessary keys to decrypt or verify them. The UE's lack of response demonstrates compliance with the standard and ensures that it does not inadvertently expose itself to potential security risks by accepting protected messages prematurely. Therefore, the UE acted securely according to 3GPP specifications. 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, after the initial NAS procedures, the UE sent an Identity Response to the AMF, which is expected as part of the authentication and identification process. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed, the AMF sent a Deregistration Request to the UE. Notably, this deregistration message from the AMF was both integrity protected and ciphered, as indicated by the security header, even though the 5G-AKA procedure (which establishes the necessary security context and keys for encryption and integrity protection) had not yet been completed. According to the 3GPP 5G standards, NAS security (ciphering and integrity protection) must only be applied after a successful 5G-AKA, as the required keys are derived during this process. Since the UE did not respond to the deregistration request that was sent with security protection prior to the establishment of a security context, the UE correctly refused to process or reply to a message that violated the security procedures outlined by the standard. This behavior demonstrates that the UE adhered to the 3GPP security requirements and did not accept protected NAS messages before the appropriate security context was established. 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, the UE and AMF completed the initial NAS steps, with the UE sending an identity response to the AMF. The AMF then sent a Security Mode Command to the UE, which was marked as "Protected" and indicated the use of ciphering (5G-EA4) and integrity (128-5G-IA1) algorithms, with the security header set to "Integrity protected with new security context (3)." However, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the necessary security keys for encryption and integrity protection had not been established between the UE and the network. According to 3GPP standards (TS 24.501), the Security Mode Command must not be integrity protected with a new security context or attempt to establish NAS security before the 5G-AKA is completed, as this would violate the security procedures and potentially expose the UE to security risks. The UE, recognizing that a Security Mode Command was received before the completion of 5G-AKA, correctly rejected the command with a "Security mode reject (unspecified)" message. This behavior aligns with the security requirements outlined by 3GPP, as the UE did not proceed with establishing NAS security using uninitialized or invalid security contexts, thereby preventing a potential security vulnerability. Secure

165	165	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3100 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 5G- IA0 (null) Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.03973889350891113 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040254831314086914 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24545598030090332 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, the 5G standalone User Equipment (UE) completed the initial NAS steps and responded to an identity request from the Access and Mobility Management Function (AMF) with an identity response. Subsequently, the AMF sent a Security Mode Command to the UE, but this message was sent as a plain (unencrypted) NAS message, with the 5G-AKA (Authentication and Key Agreement) procedure not yet completed. The selected ciphering algorithm was 128-5G-EA2, but the integrity algorithm was set to 5G-IA0 (null), indicating no integrity protection. After receiving the Security Mode Command, the UE immediately sent a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G security specifications, user and signaling messages must not be sent in plain text after the security context is established, and sensitive signaling should only occur after mutual authentication (5G-AKA) is complete and NAS security is activated. In this scenario, the UE refused to proceed with security activation under insecure conditions by sending a Deregistration Request instead of processing the Security Mode Command. This is the expected secure behavior, as the UE did not accept to operate without proper authentication and security activation, thus protecting itself from potential security risks such as Man-in-the-Middle attacks. Therefore, the UE's action was in line with 3GPP security standards and demonstrated secure behavior. 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, after the initial NAS procedures, the UE sent an "Authentication Response" message to the AMF, which is the expected uplink message during the 5G-AKA authentication process. However, before the completion of 5G-AKA (as indicated by "5G-AKA: Not completed yet"), the AMF sent a "Configuration Update Command" to the UE, and this message was integrity protected but not encrypted, since encryption keys are not established until after 5G-AKA is completed. According to the 3GPP 5G security standards (TS 33.501), the UE should not accept or process any NAS messages that are integrity protected (or encrypted) with keys derived from 5G-AKA before the authentication procedure is completed, as this could expose the UE to spoofing or replay attacks. In this case, the UE did not respond to the configuration update command sent by the AMF before the completion of authentication, which is the correct and secure behavior as per the 5G standard. The UE's refusal to process NAS messages before security context establishment ensures that it is not vulnerable to attacks exploiting the lack of established security. Therefore, the UE's actions in this scenario were secure. 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, the UE completed the initial NAS procedures and sent an authentication response to the AMF. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed, the AMF sent an identity request for the IMEISV to the UE in plain (unencrypted) NAS messaging. 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; instead, it should be protected by encryption, which is only established after the successful completion of the 5G-AKA procedure. By refusing to respond to the plain identity request before security was activated, the UE followed the security guidelines designed to protect user privacy and device identity. This behavior prevents the exposure of the IMEISV over an unprotected channel, which could otherwise be exploited by malicious actors or in rogue network scenarios. Therefore, the UE's lack of response to the unprotected identity request demonstrates correct and secure behavior as per the 3GPP 5G security 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 responded with a "service accept" message that was protected (i.e., integrity protected and/or encrypted). However, the 5G-AKA procedure, which establishes the security context necessary for NAS message protection, was not yet completed according to the test summary. Despite this, the AMF sent a protected "service accept" message, and the UE subsequently sent a deregistration request. According to the 3GPP 5G standard (TS 24.501), NAS message protection (encryption/integrity) is only to be applied after successful completion of the 5G-AKA procedure, which establishes the necessary keys and security context. If the UE processes or accepts protected messages from the AMF before the security context is established, this is a deviation from the standard and introduces a security risk, as the cryptographic keys for protection are not yet agreed upon or valid. The UE's action of proceeding with NAS communication (sending a deregistration request) after receiving a protected message before 5G-AKA completion indicates that it did not properly enforce the required security procedures, which could be exploited by an attacker. Therefore, the UE's behavior in this scenario is not compliant with 3GPP security standards and is considered insecure. Insecure

169	169	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.1594829559326172 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15969610214233398 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Authentication Response to the AMF as part of the 5G-AKA process, which had not been completed yet. The AMF, under tester control, replied with a GMM Status message indicating "Non-5G authentication unacceptable" (5GMM Cause: 26), and this message was sent in plain (unencrypted) form, as is expected before the 5G-AKA is completed. The UE did not respond to this plain GMM Status message from the AMF. According to the 3GPP 5G standards, the UE should not process or respond to NAS messages that are sent in plain text after the authentication process has started but before security context establishment, unless explicitly allowed by the specification. The UE's lack of response to the plain GMM Status message is thus in line with security best practices and the 3GPP standard, as responding could expose the UE to security risks such as replay or spoofing attacks. Therefore, the UE's behavior in this scenario demonstrates a secure implementation of the standard. 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 and AMF began NAS communication, with the UE sending an authentication response to the AMF. However, before the 5G-AKA procedure (Authentication and Key Agreement) was completed, the AMF sent a deregistration request to the UE. Notably, this deregistration request was sent as a protected message, with both integrity protection and ciphering applied (security header type 2). According to the 3GPP 5G standards, security protection for NAS messages (integrity and ciphering) must only be activated after successful completion of the 5G-AKA procedure, which establishes the necessary security context and keys. Since the 5G-AKA was not completed at this point, the UE would not have the security keys required to decrypt or verify the integrity of the protected message. The UE, recognizing that the security context was not yet established, did not respond to the deregistration request. This behavior aligns with the 3GPP standard, as the UE must not accept or process protected NAS messages before the security context is in place. Therefore, the UE's lack of response demonstrates correct and secure behavior according to 5G security requirements. Secure

171	171	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15981698036193848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16000986099243164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (Authentication and Key Agreement), the UE sent a Security Mode Complete message to the AMF, indicating that NAS security procedures had been established and that subsequent NAS messages should be encrypted and integrity protected. However, the AMF then sent an Identity Request message to the UE requesting the IMEISV, but this message was sent in plain (unencrypted) form. The UE, upon receiving this unprotected Identity Request after security activation, did not respond. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after Security Mode Complete), the UE should only accept and respond to NAS messages that are both integrity protected and, where applicable, ciphered. If the UE receives a security-unprotected message after this point, especially one requesting sensitive information like IMEISV, it should ignore it to prevent potential security breaches (such as identity theft or tracking). Therefore, the UE's lack of response to the unprotected Identity Request was the correct and secure behavior as per the 3GPP standard, ensuring that sensitive information is not disclosed over an unprotected channel. 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, after the completion of 5G-AKA authentication and security mode establishment, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) was now active for subsequent NAS messages. Immediately after, the AMF sent an "identity request" message to the UE, asking for the UE's GUTI (Globally Unique Temporary Identifier). However, this identity request was sent in plain (unencrypted) NAS, even though security had already been activated. According to 3GPP standards (TS 24.501), once the security context is established and security mode complete is exchanged, 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 security requirements, as the UE is expected to reject or ignore any plain NAS messages after NAS security is enabled to prevent potential security breaches such as replay or interception attacks. Therefore, the UE’s action of not responding to the unprotected identity request after security activation demonstrates secure behavior in accordance with 3GPP 5G standards. 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 security test, the 5G standalone User Equipment (UE) completed the 5G-AKA authentication procedure, establishing the necessary security context for subsequent NAS message encryption and integrity protection. The UE then transmitted a Security Mode Complete message, which should indicate that secure NAS communication (i.e., encryption and integrity protection) is now in effect. However, the AMF, under test control, responded with a Service Reject message (5GMM Cause 111: Protocol error, unspecified) sent in plain (unencrypted) text. Upon receiving this, the UE responded with a Deregistration Request (UE originating). According to the 3GPP 5G standard, once the security context is established and Security Mode Complete is sent, all subsequent NAS messages between the UE and AMF must be protected (encrypted and integrity checked). The UE, upon receiving a plain Service Reject message after security was activated, should have treated this as a protocol error, ignored the message, and not acted upon it, since it was not properly protected. By responding to an unprotected message with a Deregistration Request, the UE failed to enforce the security requirements outlined by 3GPP, exposing itself to potential security risks such as downgrade or denial-of-service attacks. This indicates a non-compliance with the standard and demonstrates insecure behavior by the UE. Insecure
174	174	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: c2ada16de5afa04c9abbf0b2aba327aa AUTN: 3030303030303000ee55922b5d550000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.15995287895202637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016292572021484 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Security Mode Complete" message to the AMF, indicating its acceptance of the negotiated security algorithms and the establishment of a security context. However, the AMF then sent an "Authentication Request" message to the UE in plain (unencrypted) form, which is not the expected behavior according to 3GPP standards. According to the 3GPP TS 33.501 specification, after the security context is established (i.e., after the Security Mode Complete message), all subsequent NAS messages between the UE and the AMF must be integrity protected and, if required, ciphered. The UE, upon receiving a plain (unencrypted and unprotected) authentication request after security activation, did not respond. This behavior aligns with the security requirements of the standard, as the UE must reject or ignore any unprotected NAS messages once a security context is active, in order to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to the plain authentication request after security mode completion was correct and secure according to the 3GPP 5G security standards. 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 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated NAS security algorithms and the start of protected NAS communication. Following this, the AMF sent a "service accept" message to the UE; however, this message was sent in plain (unencrypted) text. According to the 3GPP 5G standard (TS 24.501), after the security mode complete message, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered. When the UE received a plain (unencrypted) "service accept" message after security activation, it did not respond, which aligns with the 3GPP requirements: the UE is expected to discard or ignore any NAS messages that are not integrity protected after security mode is activated. This behavior prevents potential security breaches such as replay or man-in-the-middle attacks. Therefore, the UE's action—refusing to respond to an unprotected message after security activation—was secure and compliant with the 5G standard. 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 the described test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the initial security procedures were finished and that NAS security should now be active for subsequent messages. However, the AMF then sent an "Identity Request" message to the UE, specifically requesting the SUCI, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards (TS 33.501), once NAS security has been activated following successful authentication and key agreement (i.e., after 5G-AKA is completed), all subsequent NAS messages must be integrity protected and, if confidentiality is activated, encrypted. The SUCI (Subscription Concealed Identifier) is sensitive information designed to protect user identity privacy, and should never be transmitted in the clear after security activation. The UE, upon receiving an identity request for SUCI in a plain (unencrypted) NAS message after security activation, correctly did not respond, as replying would have violated 3GPP security requirements and exposed the user's identity. This behavior demonstrates that the UE adhered to the 5G security specifications by refusing to respond to an insecure request after security activation. Therefore, the UE's actions in this scenario were secure. Secure

177	177	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 1230c172c0fe20b56039f8264c2856d4 AUTN: 2d236d5db431900054adfe579b1ec661 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.4670701026916504 UE to AMF UplinkNASTransport, Registration complete 0.46730613708496094 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure between the User Equipment (UE) and the Access and Mobility Management Function (AMF), the UE sent a "registration complete" message, which is expected behavior. However, the AMF subsequently sent an "authentication request" message to the UE in plain (unencrypted) form, despite the fact that the security context should have been established after the 5G-AKA process. According to 3GPP standards (TS 33.501), after successful authentication and key agreement, NAS signaling messages between the UE and the AMF must be integrity protected and, where necessary, encrypted to prevent interception or tampering. The UE, upon receiving a plain (unencrypted) authentication request after security context establishment, did not respond to this message. This behavior aligns with the security requirements of the 5G standard, as the UE is expected to reject or ignore messages that do not comply with the established security context to prevent possible replay or man-in-the-middle attacks. Therefore, the UE's action of providing no response to an insecure, plain authentication request after security context establishment was appropriate and secure as per 3GPP requirements. 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 successfully completing the 5G-AKA authentication procedure, the UE sent a "registration complete" message to the AMF, indicating that mutual authentication and key establishment had been achieved. Immediately after, the AMF sent an identity request for the SUCI (Subscription Concealed Identifier) to the UE, but this request was sent in plain (unencrypted) NAS signaling, despite the security context being established. Instead of responding with the requested SUCI, the UE initiated a deregistration request (UE originating), effectively refusing to comply with the identity request. According to 3GPP 5G security standards, after the completion of 5G-AKA and establishment of a NAS security context, all subsequent NAS messages (including identity requests) must be protected (encrypted and integrity protected) to prevent exposure of sensitive information and to guard against security threats such as interception, replay, or modification. The UE's decision not to respond to an identity request sent in the clear, and instead deregister, demonstrates adherence to the security requirements specified by 3GPP, as responding in plain would have exposed sensitive identifiers. Thus, the UE's action was aligned with 5G security standards and protected its identity information. 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 security test of a 5G standalone User Equipment (UE), the 5G-AKA authentication procedure was completed successfully, after which the UE sent a "registration complete" message to the AMF. Subsequently, the AMF sent a "configuration update command" to the UE, but crucially, this message was sent as a plain (unencrypted and unauthenticated) NAS message, even though security procedures should have been activated following the completion of 5G-AKA. Upon receiving this unprotected message, the UE responded by sending a "deregistration request (UE originating)" to the AMF. According to the 3GPP 5G standard, after the successful completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. The UE is expected to reject or ignore any NAS messages that are not protected, as accepting unprotected messages could expose the device to security risks such as spoofing or manipulation. In this scenario, the UE did not process the unprotected configuration update command; instead, it initiated a deregistration procedure, which is a secure and standards-compliant response to receiving an unprotected NAS message after security activation. This action demonstrates that the UE correctly enforced NAS security requirements and did not accept insecure commands, thereby upholding the security standards defined by 3GPP. Secure
180	180	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.5163559913635254 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.5165369510650635 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.5166728496551514 AMF to UE DownlinkNASTransport, Configuration update command 2.7203638553619385 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent an Uplink NAS Transport message, and the AMF responded with a Configuration Update Command. Notably, the Configuration Update Command from the AMF was sent as a plain (unencrypted) NAS message, as indicated by the security header value of 0. According to 3GPP 5G standards (TS 24.501), once NAS security has been established (which occurs after 5G-AKA is completed), all subsequent NAS messages exchanged between the UE and AMF must be integrity protected and, when applicable, ciphered. Upon receiving a plain (unencrypted and unauthenticated) NAS message after security context is established, a standards-compliant UE is required to reject the message and initiate deregistration, as accepting plain NAS messages at this stage exposes the UE to security risks such as spoofing and man-in-the-middle attacks. In this test, the UE correctly responded to the receipt of a plain Configuration Update Command by sending a Deregistration Request (UE originating), which is the expected and secure behavior as per 3GPP standards. This action ensures that the UE does not process potentially malicious or unauthenticated messages after security establishment, thereby protecting itself and the network. 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 completing the 5G-AKA authentication procedure, the UE sent an uplink NAS transport message to the AMF. Subsequently, the AMF sent an Authentication Request to the UE, but this message was sent in plain (unencrypted) format. Notably, the UE did not respond to this plain Authentication Request. According to the 3GPP 5G security standards, once the 5G-AKA procedure is completed, a security context should be established, and all subsequent NAS messages between the UE and the AMF are required to be integrity protected and, where applicable, encrypted. The UE, by refusing to respond to a plain (unencrypted and unprotected) Authentication Request after security context establishment, is adhering to the 3GPP security requirements, as responding to such a message could expose sensitive information or allow for certain types of attacks (such as replay or man-in-the-middle attacks). Therefore, the UE's action of not responding is considered secure and compliant with the standard. Secure

182	182	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.5082509517669678 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, UL NAS transport, 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 the 5G-AKA procedure—which establishes mutual authentication and should enable NAS security (encryption and integrity protection)—the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF responded with a Service Reject message using a plain (unencrypted and unauthenticated) downlink NAS message, with a 5GMM cause code of 111 (Protocol error, unspecified). According to the 3GPP 5G standard (TS 24.501), after the security context is established via 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF should be protected using NAS security (i.e., encrypted and integrity protected). The UE, upon receiving a plain (unprotected) NAS message after security activation, is required by the standard to discard such messages and not process them, as accepting unprotected messages at this stage would expose the UE to various attacks, such as downgrade or replay attacks. Based on the packet capture and test summary, the UE did not respond to the unprotected Service Reject message sent by the AMF. This indicates that the UE correctly followed the 3GPP security requirements by ignoring an unprotected NAS message after 5G-AKA completion, thereby preventing a potential security vulnerability. 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 the observed security test, after completing the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, after which the AMF sent an Authentication Request message to the UE. Notably, this Authentication Request was sent in plain (unencrypted) form, despite the 5G-AKA already being marked as completed. The UE, upon receiving this message, responded by sending a Deregistration Request (UE originating), effectively terminating its connection to the network. According to the 3GPP 5G standards, once 5G-AKA is completed and a security context is established, all subsequent NAS messages exchanged between the UE and the AMF are required to be integrity protected and, in most cases, encrypted to ensure confidentiality and authenticity. The UE's action to deregister upon receiving a plain (unencrypted) Authentication Request after security context establishment demonstrates correct and secure behavior, as it refused to process a message that violated security expectations. This aligns with 3GPP security requirements, which state that the UE should not accept further unprotected NAS messages once a security context is in place. Therefore, the UE's action in this scenario was secure. 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 (which establishes NAS security), the UE sent an Uplink NAS Transport message, after which the AMF responded with a plain (unencrypted) Identity Request for the IMEI. Instead of responding with its IMEI, the UE initiated a Deregistration Request (UE originating), effectively refusing to provide its identity in response to an unprotected (plain) request. According to the 3GPP 5G standard (TS 24.501), once NAS security is established (i.e., after 5G-AKA), all subsequent NAS messages containing sensitive information, such as identity responses, must be integrity protected and, where applicable, ciphered. The UE is expected to reject or ignore requests for sensitive information sent in plain text after security has been activated. By refusing to provide its IMEI in response to a plain Identity Request and instead deregistering, the UE correctly adhered to the security requirements set by the standard, protecting the confidentiality of its identity. This behavior demonstrates that the UE is secure in its handling of NAS messages post-authentication, as it does not expose sensitive information over an unprotected channel. 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 the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message to the AMF, indicating that NAS security should have been activated and all subsequent NAS messages should be protected (integrity protected and, in most cases, ciphered) according to 3GPP TS 24.501. However, the AMF responded with a Registration Reject message (5GMM Cause 62: "No network slices available") sent in plain (unencrypted and non-integrity protected) NAS, which is only permitted prior to the establishment of NAS security. The UE, upon receiving this plain Registration Reject after security activation, took no further action and did not respond to the message. According to 3GPP standards, specifically TS 24.501, section 4.4.6 and 8.2.24, the UE must ignore any downlink NAS messages received in plain NAS after NAS security has been activated, as accepting such messages could expose the UE to security vulnerabilities such as spoofing or denial of service attacks. By not responding to the unprotected Registration Reject, the UE correctly adhered to 3GPP security requirements and protected itself against potential attacks or protocol violations. 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 (specifically, a PDU session establishment request) to the AMF. In response, the AMF issued a Security Mode Command as a plain (unencrypted and unauthenticated) NAS message, indicating the selection of 5G-EA6 ciphering and 128-5G-IA1 integrity algorithms, with the ABBA parameter set to 3200. According to 3GPP TS 24.501, after 5G-AKA is completed, the AMF must send the Security Mode Command as a plain NAS message, since security context is not yet activated; the UE is then expected to respond with a Security Mode Complete message, which will be the first NAS message protected with the negotiated security algorithms. However, in this test, the UE did not respond with Security Mode Complete. Instead, it sent a Deregistration Request (UE originating), which is not the expected behavior according to the 5G standard. The UE should only reject the Security Mode Command if there is a valid reason (e.g., unsupported algorithms or integrity check failure), and should otherwise proceed with secure communication. By deregistering immediately after receiving a valid Security Mode Command, the UE failed to enter secure NAS communication as required by 3GPP, potentially exposing itself to denial-of-service or downgrade scenarios. Therefore, the action taken by the UE is not compliant with the 5G standard and is considered insecure. Insecure
187	187	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 2.197134017944336 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 2.197467088699341 AMF to UE SACK (Ack=11, Arwnd=106334) , DownlinkNASTransport, Configuration update command 2.1975760459899902 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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 IMEISV, and this message was sent in plain (unencrypted) NAS. The UE did not respond to this request. According to the 3GPP 5G security specifications (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, ciphered. Sensitive information, such as the IMEISV, must not be sent in cleartext after security activation, to prevent privacy and security breaches. The UE's refusal to respond to the identity request sent in plain NAS after security was established is therefore in line with 3GPP security requirements, as responding would have exposed sensitive information in an insecure manner. By withholding its IMEISV in this context, the UE correctly protected its identity and adhered to the security standards. 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 completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, indicating that the security context had been established and subsequent NAS messages should be protected (integrity protected and ciphered) according to 3GPP TS 33.501 and TS 24.501. However, the AMF responded with a "deregistration accept" message sent in plain (unencrypted and unprotected) NAS, which is not compliant with the 5G security requirements, as messages after 5G-AKA completion and security mode command should be protected. The UE, upon receiving this plain, unprotected downlink message, did not respond. According to 3GPP standards, the UE is required to ignore or discard any NAS messages that are not integrity protected and ciphered once a security context is active, especially for messages that can affect registration or session state. The UE's lack of response in this scenario demonstrates correct and secure behavior, as it did not process or acknowledge an unprotected critical NAS message after security activation. This behavior prevents possible security breaches, such as session hijacking or unauthorized deregistration. Therefore, the UE acted according to the 3GPP security requirements. 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 successful completion of the 5G-AKA authentication procedure, the UE sent a service request uplink message to the AMF, which then responded with a Security Mode Command in plain NAS format (i.e., unprotected by ciphering or integrity protection). The Security Mode Command indicated that the AMF selected 5G-EA6 for ciphering and 128-5G-IA2 for integrity protection, but the message itself was sent without any security header (Plain NAS message, security header type 0). According to 3GPP TS 24.501, after 5G-AKA, NAS messages must be integrity protected (and, if applicable, ciphered) except for specific initial procedures, such as the initial Security Mode Command, which is allowed to be sent in plain text to establish the security context. However, after the Security Mode Command is received, the UE is expected to respond with a Security Mode Complete message, which should be integrity protected and, if ciphering is activated, also encrypted. In this test, the UE did not respond at all to the Security Mode Command sent in plain text. This lack of response may indicate that the UE refused to proceed with an unprotected message, which is a conservative and secure behavior, as it avoids engaging in potentially insecure communication before security contexts are properly established and confirmed. Therefore, based on the 3GPP standard and the observed behavior, the UE's action of not responding to a plain Security Mode Command after 5G-AKA can be considered secure, as it avoids a potential downgrade or exposure to security risks. Secure

190	190	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1010 RAND: 7479eaccb74fb3be01aa8b2b6ff1abcb AUTN: dd84e27507488000bb521f82528f6f6e ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 16.614274978637695 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 16.614504098892212 AMF to UE SACK (Ack=22, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE initiated a Service Request to the AMF. In response, the AMF sent an Authentication Request message to the UE, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, after the successful completion of 5G-AKA, the UE and network should establish a security context, and all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted. When the UE received a plain (unencrypted) Authentication Request after 5G-AKA completion, it did not respond. This behavior aligns with the 3GPP security specifications, which state that the UE must not accept or process security-sensitive NAS messages that are not protected after a security context is established. By refusing to respond to the unprotected message, the UE prevented a potential downgrade or replay attack, maintaining the integrity of the security context. Therefore, based on the described interaction, the UE acted securely according to the 5G standard. Secure

191	191_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1010 RAND: 765bcfb5ee4bd70eb854f2deac92aea9 AUTN: 7f72e2496ad28000fd0cf5cd8a2492b7 ngKSI_TSC: Native security context ngKSI_KSI: 4 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 8.671967029571533 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.672221899032593 AMF to UE SACK (Ack=14, Arwnd=106496) , DownlinkNASTransport, Authentication request 8.874675035476685 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF, under test control, issued a new authentication request message in plain (unencrypted) form, using the same ngKSI (key set identifier) as before, indicating the use of the native security context. Upon receiving this, the UE responded with an "Authentication failure (ngKSI already in use)" message. According to the 3GPP 5G security standards, once the 5G-AKA procedure has been completed and a security context has been established, any subsequent authentication requests reusing the same ngKSI should be considered suspicious, as this could be indicative of a replay attack or protocol misuse. The UE's decision to reject the authentication request and notify the AMF that the ngKSI is already in use is in line with the security requirements to prevent replay and downgrade attacks. Moreover, the UE did not proceed with further NAS procedures using an insecure or duplicated security context, thereby protecting itself from potential security breaches. Therefore, the UE's actions demonstrate adherence to 3GPP security standards and proper handling of the situation. Secure
192	192	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 35.06067895889282 UE to AMF SACK (Ack=27, Arwnd=106496) , UplinkNASTransport, Service request 35.06101393699646 AMF to UE SACK (Ack=36, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (authentication and key agreement), the UE initiated a service request to the AMF. In response, the AMF sent an identity request message to the UE, specifically requesting the TMSI (Temporary Mobile Subscriber Identity). Notably, the AMF sent this identity request as a plain (unencrypted) message, even though the 5G-AKA procedure—which establishes the security context for NAS message encryption and integrity protection—had already been completed. According to 3GPP standards (TS 33.501 and TS 24.501), once the security context is established after 5G-AKA, all subsequent NAS messages, including identity requests, must be protected (i.e., encrypted and integrity protected). The UE, upon receiving an unprotected (plain) identity request after security activation, correctly did not respond, as replying to such a request would risk exposing sensitive information in cleartext and violate the 5G security requirements. Therefore, the UE's action was in line with the 3GPP security specifications and demonstrated secure behavior by refusing to respond to an improperly protected message. 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 security test of a 5G standalone User Equipment (UE), the 5G-AKA authentication procedure was completed, establishing a security context between the UE and the AMF. Following this, the UE sent a service request uplink message to the AMF, and the AMF responded with a downlink Configuration Update Command, which was sent as a protected message. Notably, the security header of the AMF's message was marked as "Unknown," and the UE did not respond to the configuration update command. According to the 3GPP 5G standards, after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered, and the UE should only process protected messages. If the UE receives a NAS message with an unknown or unprotected security header after security has been activated, it should discard the message and not respond, as a security measure to prevent replay or downgrade attacks. In this scenario, the UE did not respond to the AMF's configuration update command, which was either not properly protected or had an invalid security header. This behavior aligns with 3GPP security requirements, as the UE refused to process a potentially insecure message after security activation. Therefore, the UE's action in this interaction 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 security 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 an Authentication Reject message, which was sent in plain (unencrypted) form. According to the 3GPP 5G standard, specifically TS 24.501 and TS 33.501, once the 5G-AKA is completed, both the UE and the network are expected to establish NAS security, which includes encryption and integrity protection for subsequent NAS messages. The Authentication Reject message is considered a security-critical message and, after the security context is established, should be protected (i.e., encrypted and integrity protected). In this test, the UE received an unprotected Authentication Reject message after security activation and, as per the standard, the UE is expected to ignore such messages that are not integrity protected or encrypted when a security context is present. The UE did not respond to the unprotected Authentication Reject, which aligns with 3GPP security requirements and demonstrates correct and secure behavior, as responding to or accepting unprotected critical messages could expose the UE to security risks such as denial-of-service or impersonation 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, after the completion of the 5G-AKA authentication procedure, the User Equipment (UE) sent a service request to the Access and Mobility Management Function (AMF). In response, the AMF sent an identity request message to the UE, specifically requesting the Subscription Concealed Identifier (SUCI). Notably, this identity request was sent as a plain (unencrypted) message, and the UE responded with an identity response containing the SUCI. According to the 3GPP 5G security standards, after the 5G-AKA procedure is completed, all subsequent NAS messages—including identity requests and responses—should be protected by NAS security (i.e., encrypted and integrity-protected). The fact that the UE responded to an unprotected (plain) identity request with its SUCI after authentication is a deviation from the standard, as it should have expected NAS security to be activated and should not have accepted or responded to plain NAS messages post-authentication. This behavior could expose the UE to potential security risks, such as identity interception. Therefore, based on the 3GPP 5G security requirements, the action taken by the UE was insecure. Insecure
196	196	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 9.49011492729187 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.490720987319946 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the User Equipment (UE) sent a Service Request to the Access and Mobility Management Function (AMF), indicating it was ready for further communication. The AMF responded with a DownlinkNASTransport carrying a Configuration Update Command, which was sent as a protected (i.e., integrity protected and/or encrypted) message. However, the security header of the message was marked as "Unknown," and crucially, the UE did not respond to this protected downlink message. According to the 3GPP 5G standards, after the completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. The UE is expected to process protected NAS messages and provide an appropriate response, such as a Configuration Update Complete. The fact that the UE did not respond to a protected Configuration Update Command indicates a failure to handle security-protected NAS messages as specified by the standard. This behavior could expose the UE to potential security risks, such as denial of service or loss of synchronization with the network, and does not align with the expected secure operation defined by 3GPP. Therefore, based on the observed interaction and 3GPP requirements, the UE's action is considered insecure. Insecure

197	197	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005860328674316406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	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, which establishes security keys for NAS message protection, had not yet been completed. Despite this, the AMF responded with a deregistration request message that was integrity protected and ciphered, as indicated by the security header in the downlink message. According to the 3GPP 5G standard, the UE should only process protected NAS messages after the successful completion of the 5G-AKA procedure and the establishment of security contexts. Since the AMF sent a protected (integrity protected and ciphered) message before the security context was established, the UE, adhering to 3GPP standards, correctly chose not to respond to this message. This behavior ensures that the UE does not process or respond to potentially invalid or malicious messages that are protected with keys that have not yet been agreed upon, thereby preventing possible security breaches. Therefore, the UE's action in this scenario was secure and compliant with the 3GPP 5G security standards. 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, indicating that NAS security (encryption and integrity protection) should be active for subsequent NAS messages. However, the AMF then sent an Identity Request for the UE's GUTI as a plain (unencrypted) NAS message. According to the 3GPP 5G standard (TS 24.501), once NAS security has been activated, the UE must not accept or respond to plain NAS messages except in specific, well-defined cases (such as initial registration or emergency services before security activation). Since the UE did not respond to the plain (unencrypted) Identity Request after security activation, it correctly followed the 3GPP security requirements by refusing to expose its identity information over an unprotected channel. This behavior prevents potential interception or replay attacks by malicious actors and demonstrates that the UE is enforcing NAS security as mandated by the standard. Therefore, the UE's action in this scenario was appropriate and aligned with the 5G security specifications. 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 the described security test, after completing the 5G-AKA authentication and key agreement procedure, the UE sent a "security mode complete" message, indicating that NAS security context establishment was finalized and subsequent NAS messages should be encrypted and integrity protected. However, the AMF then sent an "identity request" message for the IMEISV in plain (unencrypted) form, bypassing the expected security protections. The UE, upon receiving this unprotected identity request after security activation, did not respond. According to the 3GPP 5G standard (TS 24.501), once the NAS security context is established (after "security mode complete"), the UE must reject any subsequent NAS messages not protected by the agreed security algorithms, especially those requesting sensitive information like IMEISV. The UE's refusal to respond to the unprotected identity request demonstrates proper adherence to the 5G security standard, as responding with its IMEISV over an unprotected channel would expose it to privacy and security risks. Therefore, the UE's action in this scenario was secure and in line with 3GPP requirements. 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 completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be activated for subsequent NAS signaling. Immediately after, the AMF sent an identity request message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) NAS. 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 "security mode complete"), all subsequent NAS messages must be protected using the agreed security context. If the UE receives a plain (unencrypted) NAS message after security activation, it is required by the standard to discard the message and not respond, as responding to a plain message at this stage would constitute a security vulnerability (e.g., exposing identifiers or accepting unauthenticated instructions). Given this, the UE's lack of response to the unprotected identity request demonstrates correct and secure behavior in compliance with 3GPP standards. 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 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message for the IMEI in plain (unencrypted) form, rather than as a protected message. The UE, upon receiving this unprotected identity request after security activation, chose not to respond. According to 3GPP standards (TS 24.501), once NAS security is activated, the UE is required to ignore or not respond to any subsequent NAS messages that are not integrity protected and ciphered, except for a few specific cases (such as service request in certain scenarios). By refusing to send its IMEI in response to an unprotected identity request after security activation, the UE is correctly following the 5G security procedures to prevent exposure of sensitive information over an unprotected channel. This behavior demonstrates adherence to the 3GPP security standards and protects the UE from potential privacy and security risks. 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 successfully completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an identity request message to the UE in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier). According to 3GPP standards (TS 33.501 and TS 24.501), once 5G-AKA is completed and NAS security is activated (i.e., after "security mode complete"), all subsequent NAS messages, including identity requests, must be sent with both integrity protection and encryption. The UE, upon receiving a plain (unencrypted) identity request after security activation, did not respond to the AMF. This behavior aligns with the 3GPP specification, which states that the UE should ignore NAS messages that are not properly protected after security activation, as responding to an unprotected message could expose sensitive information or make the UE vulnerable to attacks such as identity interception or replay attacks. Therefore, the UE's refusal to respond to the plain identity request demonstrates secure behavior in accordance with 3GPP standards. Secure

203	203	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15087509155273438 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15108299255371094 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security (encryption and integrity protection) should be activated 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, in response, did not reply to this request. According to 3GPP 5G standards (TS 24.501), once NAS security is established (after Security Mode Complete), the UE should only accept and respond to NAS messages that are integrity protected and, where required, encrypted. Receiving a plain (unencrypted) Identity Request after security activation is a protocol violation and could be a security risk, as it may be an attempt to exploit the UE to reveal sensitive information without proper protection. By refusing to respond to this plain request, the UE is adhering to the 3GPP security requirements, ensuring that it does not expose its identity information over an unprotected channel. This behavior is secure and aligns with the expected security posture as per the 5G standard. 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 security test scenario, after the successful completion of the 5G-AKA authentication process, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) was established for subsequent NAS messages. However, the AMF then sent an identity request for the IMEISV in the clear (as a plain, unprotected NAS message). According to 3GPP TS 24.501, once NAS security is activated, all subsequent NAS messages exchanged between the UE and the network must be integrity protected and, if confidentiality is activated, also encrypted. The UE, upon receiving a plain (unencrypted, unauthenticated) identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which states that the UE should ignore any unprotected NAS messages after security activation, as responding could expose sensitive information (such as the IMEISV) to potential attackers and compromise user privacy. The UE's refusal to respond to the unprotected identity request demonstrates adherence to the 5G security requirements and protects against downgrade and interception attacks. 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 security test, after the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security procedures and mutual authentication were successfully finished. Following this, the AMF sent an "Identity Request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) NAS signaling. According to the 3GPP 5G standard, after the completion of 5G-AKA, all subsequent NAS messages—especially those requesting sensitive identifiers like the SUCI—must be protected with NAS security (i.e., encrypted and integrity protected). The UE, upon receiving an unprotected identity request post-authentication, did not respond, which aligns with security best practices to prevent the exposure of sensitive information over an unprotected channel. By refusing to respond to an improperly protected identity request after security context establishment, the UE demonstrated secure behavior in accordance with the 3GPP standard and did not risk leaking sensitive data. 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 security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "registration complete" message to the AMF, indicating that the secure NAS context had been established and that subsequent NAS messages should be protected (i.e., encrypted and integrity protected). However, the AMF then sent an "identity request" message over the NAS signaling plane in plain (unencrypted) 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 (TS 33.501), after the completion of 5G-AKA and the establishment of a secure NAS context, the UE is required to reject or ignore any NAS messages that are not protected, as accepting or responding to unprotected messages after security activation could expose sensitive information or open up vulnerabilities to replay or man-in-the-middle attacks. By not responding to the plain (unprotected) identity request after security context activation, the UE correctly followed the 3GPP security requirements and protected itself from a potential security breach. Therefore, the action taken by the UE 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 completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that mutual authentication and key establishment had been successfully performed. Subsequently, the AMF sent an "Identity Request" message to the UE, explicitly requesting the SUCI (Subscription Concealed Identifier), but notably, this message was sent in plain (unencrypted) NAS format, even though the security context should already have been established as a result of the completed 5G-AKA. According to 3GPP 5G security standards (TS 33.501), once the 5G-AKA procedure is complete and a security context is active, all subsequent NAS messages between the UE and AMF must be integrity protected and, where required, encrypted to ensure confidentiality and protect against various attacks, including identity exposure. 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 must ignore or reject NAS messages that are not properly protected after security activation, to prevent potential downgrade or identity theft attacks. Therefore, the UE's refusal to respond to an unprotected identity request after 5G-AKA completion was the correct and secure action according to 3GPP 5G security requirements. 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 completion of the 5G-AKA authentication and security procedure, the UE sent a "registration complete" message to the AMF, indicating that the initial registration and security setup had finished. Subsequently, the AMF sent an "identity request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) form despite the security context having already been established. According to 3GPP 5G standards, after the successful completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where possible, encrypted to prevent exposure of sensitive subscriber information and to maintain the confidentiality and integrity of the communication. The UE, upon receiving a plain (unencrypted) identity request for the SUCI after security activation, correctly chose not to respond, as replying to such a request in plain would violate security requirements and potentially expose sensitive information. Therefore, the UE’s refusal to respond to an improperly protected identity request aligns with 3GPP security standards 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 successfully completing the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, which marks the end of the initial NAS security procedures and the establishment of a secure context for further NAS communication. Immediately after, the AMF sent an "Identity Request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) NAS format, even though a security context should have been established following 5G-AKA completion. As per the 3GPP 5G standard (TS 24.501), once the 5G-AKA is completed and NAS security is active, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. The UE, upon receiving a plain (i.e., unprotected) NAS message after security activation, is required by the standard to ignore such messages and not respond, as responding could expose sensitive information or enable certain attacks. In this test, the UE did not respond to the unprotected identity request from the AMF, which is the correct and secure behavior as specified by 3GPP, since responding to an unprotected message after NAS security establishment would be a security flaw. Therefore, the UE's action was in accordance with the 5G security requirements. 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 security test involving a 5G standalone User Equipment (UE), the 5G-AKA (Authentication and Key Agreement) procedure was completed, establishing security context and keys for subsequent NAS message encryption and integrity protection as per 3GPP standards. After this, the UE sent a "registration complete" message, which was expected and correct. Following this, the AMF sent an "identity request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). However, this identity request was sent in plain (unencrypted) NAS format, even though the security context had already been established after 5G-AKA. According to 3GPP TS 24.501 and TS 33.501, once the security context is in place, all further NAS messages—especially those containing sensitive information such as identity requests and responses—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, which specify that the UE must ignore or silently discard unprotected NAS messages received after security is activated, to prevent possible security breaches such as identity theft or replay attacks. Therefore, the UE's action in not responding to the unprotected identity request was correct and in full compliance with 3GPP security standards. Secure

211	211	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 4.666033029556274 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 4.666288137435913 AMF to UE SACK (Ack=20, Arwnd=106429) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent a Registration Complete message to the AMF, indicating that it had finished the initial security setup and was expecting subsequent NAS messages to be protected (i.e., integrity protected and ciphered). Following this, the AMF sent an Identity Request message to the UE, requesting the TMSI as the identity. However, the packet capture shows that this Identity Request was sent in plain (unencrypted) NAS, even though security context had already been established. According to the 3GPP 5G standard, once 5G-AKA is completed and security context is active, the UE must not accept or respond to any further plain NAS messages except for a very limited set of exceptions (such as Service Reject, Deregistration Accept, etc.), and identity requests are not among these exceptions. The UE correctly did not respond to the unprotected Identity Request, adhering to the standard and protecting its identity information from potential eavesdropping or replay attacks. Therefore, the UE's behavior was secure and compliant with 3GPP requirements. 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 the 5G-AKA authentication and key agreement procedure, 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 format, despite the fact that the security context had already been established due to the completion of 5G-AKA. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed and NAS security is activated, all subsequent NAS messages—including identity requests—must be sent protected (i.e., integrity protected and ciphered). The UE, upon receiving a plain (unencrypted) Identity Request asking for the IMEISV, did not respond to this message. This behavior aligns with the 3GPP specification, which states that the UE should ignore unprotected NAS messages that require protection after security activation, especially when such messages request sensitive information like the IMEISV. By refusing to respond to an insecure request for its IMEISV, the UE prevented a potential security breach (such as IMEISV disclosure over an unprotected channel). This demonstrates that the UE adhered to the security requirements specified by 3GPP and did not expose sensitive information improperly. 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 completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which was followed by an Identity Request from the AMF asking for the SUCI (Subscription Concealed Identifier). Notably, the AMF sent this Identity Request as a plain (unencrypted) NAS message, despite the fact that 5G-AKA had already been completed and therefore NAS security (integrity and encryption) should have been activated according to 3GPP standards (TS 24.501, section 5.4.3.2). The UE, upon receiving this unprotected Identity Request after security mode establishment, did not respond. According to the 3GPP specification, once security is established, the UE must only accept and respond to NAS messages that are integrity protected (and, where required, encrypted). Ignoring plain (unprotected) NAS messages after security activation is the correct and secure behavior, as responding to such messages could expose sensitive information (like SUCI) to potential interception or replay attacks. Therefore, the UE's refusal to respond to a plain Identity Request after completing 5G-AKA aligns with the security requirements of the 5G standard and demonstrates secure handling of NAS messages. 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 security test, after the successful completion of the 5G-AKA authentication procedure, the User Equipment (UE) initiated a UL NAS Transport message, specifically a PDU session establishment request, to the Access and Mobility Management Function (AMF). In response, the AMF sent an Identity Request message in plain (unencrypted) form, requesting the Temporary Mobile Subscriber Identity (TMSI) from the UE. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where applicable, encrypted to ensure the confidentiality and integrity of subscriber information. The UE, upon receiving an unprotected (plain) Identity Request after security context establishment, did not respond. This behavior aligns with 3GPP security recommendations, which state that the UE should not disclose any identity in response to an unprotected identity request after security has been activated, in order to prevent potential exposure of subscriber information to attackers. Therefore, the UE's action—refusing to respond to an unprotected identity request after 5G-AKA completion—demonstrates correct and secure behavior according to the standard. Secure

215	215	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.5246391296386719 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5248539447784424 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5249319076538086 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Downlink NAS Transport containing an Identity Request for the IMEISV (International Mobile Equipment Identity and Software Version). Notably, this Identity Request was sent in plain (unencrypted) NAS, despite the fact that 5G-AKA had already been completed, which should have enabled NAS security (ciphering and integrity protection). According to 3GPP TS 24.501, once security has been activated after 5G-AKA, all subsequent NAS messages, especially those requesting sensitive information such as the IMEISV, must be protected. The UE, upon receiving a plain (unencrypted) Identity Request after security activation, is expected to ignore the request and not respond, as a security measure to prevent the disclosure of sensitive device information over an unprotected channel. In this test, the UE did not respond to the plain Identity Request, demonstrating correct behavior by refusing to transmit the IMEISV without NAS security. This action aligns with 3GPP security requirements and reflects a secure implementation by the UE. Secure
216	216	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.5509819984436035 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5512139797210693 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5513119697570801 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF (under your control) sent an Identity Request message to the UE, requesting the SUCI (Subscription Concealed Identifier). Notably, this Identity Request was sent in plain (unencrypted) NAS, even though the 5G-AKA had already been completed, meaning that a security context should have been established and further NAS messages between the UE and AMF should be encrypted and integrity protected according to 3GPP TS 33.501 and TS 24.501 standards. The UE, upon receiving a plain (unencrypted) Identity Request after security activation, did not respond to the request. This behavior aligns with 3GPP security specifications, which state that after security context activation, the UE must ignore any NAS messages received in plain unless they are allowed exceptions (such as Service Request or Deregistration Request under specific conditions). By refusing to respond to a plain Identity Request after 5G-AKA, the UE is protecting itself from possible replay or interception attacks, ensuring the confidentiality and integrity of its identifiers. Therefore, the UE's actions demonstrate compliance with 3GPP security standards and are considered secure. 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 the described test scenario, after the successful completion of 5G-AKA (Authentication and Key Agreement), the User Equipment (UE) sent an Uplink NAS Transport message to the Access and Mobility Management Function (AMF). Subsequently, the AMF sent an Identity Request message to the UE, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version). Notably, this Identity Request was sent in plain (unencrypted) format, even though the 5G-AKA had already been completed, which means that NAS security (encryption and integrity protection) should have been activated for subsequent NAS messages, as mandated by the 3GPP 5G security specifications (TS 33.501). According to the standard, after security mode command and successful authentication, all further NAS messages, especially those that can reveal sensitive information such as IMEISV, must be protected by NAS security. The UE, upon receiving an unprotected (plain) identity request after security activation, correctly did not respond with its IMEISV, thereby preventing the disclosure of sensitive device information over an unprotected channel. This behavior aligns with the 3GPP security requirements, which state that the UE shall not respond to identity requests sent without NAS security after authentication is complete. Therefore, the UE's action was secure, as it adhered to the standard and protected its identity information from potential exposure. 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 completing the 5G-AKA authentication procedure—which establishes mutual authentication and ciphering keys between the UE and the network—the UE sent an Uplink NAS Transport message. Subsequently, the AMF sent a Downlink NAS Transport message containing an Identity Request for the TMSI, but this message was sent in plain (unencrypted) text. According to the 3GPP 5G standards (TS 24.501), once 5G-AKA is completed, NAS security (integrity protection and ciphering) must be activated for all subsequent NAS messages, except for a few specific procedures such as initial registration, authentication, and security mode command. Since an Identity Request for TMSI after 5G-AKA should be protected, the UE correctly did not respond to an unprotected (plain) Identity Request message, as responding could risk exposing sensitive information. The UE’s refusal to respond to an unsecured identity request demonstrates compliance with 3GPP security requirements and protects the user’s identity from potential interception or replay attacks. Therefore, the UE’s action in this scenario was secure. Secure

219	219	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.5992319583892822 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5994939804077148 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G-AKA authentication procedure—which establishes mutual authentication and keys for NAS encryption and integrity protection—the UE sent an Uplink NAS Transport message to the AMF. The AMF then responded with an Identity Request message, specifically requesting the TMSI, and sent this message in plain (unencrypted) form. The UE, upon receiving this unprotected request for its TMSI after 5G-AKA completion, did not respond. According to 3GPP standards, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where confidentiality is required (such as for identity information), encrypted. By refusing to respond to an unprotected (plain) Identity Request after security context establishment, the UE is correctly enforcing 3GPP security requirements and protecting its identity from potential interception or replay attacks. This behavior demonstrates adherence to the standard and a secure handling of sensitive information. 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, the UE and AMF successfully completed the 5G-AKA authentication procedure, which is a prerequisite for establishing security context and enabling NAS message encryption and integrity protection. Following this, the UE sent a UL NAS Transport message, and the AMF responded with an Identity Request message, specifically requesting the TMSI, but crucially, this Identity Request was sent in plain (unencrypted) form. According to the 3GPP 5G standards (TS 24.501), after the 5G-AKA procedure is completed and a security context is established, all subsequent NAS messages (including Identity Requests) must be integrity protected and, where applicable, encrypted to prevent exposure of sensitive information and to guard against attacks such as impersonation or eavesdropping. In this scenario, the UE did not respond to the plain (unencrypted) Identity Request sent by the AMF after 5G-AKA completion. This behavior aligns with 3GPP security requirements, as the UE should refuse to process or respond to NAS messages that are not properly protected after security activation. By withholding its response, the UE avoided exposing its TMSI in an insecure manner and demonstrated compliance with the standard's security recommendations. Therefore, the action taken by the UE 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 successfully completing 5G-AKA (authentication and key agreement), the UE sent an uplink Service Request message to the AMF. The AMF then responded with a Service Accept message, but crucially, this downlink message was sent in plain (unencrypted) text, as observed in the packet capture. According to the 3GPP 5G security standard (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages, including Service Accept, must be integrity protected and, except for a few specific cases (such as initial registration and certain error messages), should also be encrypted to prevent eavesdropping and tampering. The UE, upon receiving an unprotected (plain) Service Accept message after 5G-AKA, did not respond further. This behavior aligns with the security requirements, as the UE is expected to reject or ignore NAS messages that are not properly protected when protection should be in place. Therefore, the UE's action—refusing to process or respond to an unprotected Service Accept message post-authentication—demonstrates adherence to the 5G security standards and reflects secure behavior. 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, after successfully completing the 5G-AKA authentication and key agreement procedure, the User Equipment (UE) initiated a service request to the Access and Mobility Management Function (AMF), which then responded with a Service Accept message. Notably, the Service Accept message from the AMF was sent in plain (unencrypted) form, even though 5G-AKA had already been completed, which means security context and ciphering keys should have been established. According to 3GPP standards (TS 33.501), after 5G-AKA is completed, all subsequent NAS messages should be integrity protected and, where possible, encrypted to prevent eavesdropping and tampering. Upon receiving the unprotected (plain) Service Accept message, the UE did not respond further. This behavior by the UE aligns with the 3GPP security requirements, as the UE is expected to reject or ignore NAS messages that are not properly protected once a security context is in place. Therefore, the UE's decision not to respond to an unprotected downlink message after security activation demonstrates adherence to 5G security standards and is considered 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.	During this security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which was properly uplinked. In response, the AMF sent a Service Reject message to the UE indicating "UE identity cannot be derived by the network" (5GMM Cause 9). Notably, this Service Reject message was transmitted in plain (unencrypted) format, despite the fact that the 5G-AKA had already been completed, and thus security context for NAS message encryption should have been established between the UE and the AMF. According to the 3GPP 5G standard (TS 24.501), after successful authentication and key establishment, the UE is required to accept only NAS messages that are integrity protected and ciphered, except for a few specific cases (such as certain reject messages sent prior to security context setup). Since the UE received a plain (unencrypted) Service Reject message after security context was available and did not respond or accept it, this indicates that the UE correctly ignored an insecure message in accordance with the 3GPP security requirements. Therefore, the UE's action was secure as it adhered to the standard by not processing a plain message when encryption should have been enforced. 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 5G-AKA (authentication and key agreement), the UE sent a service request to the AMF, which then responded with a service reject message indicating "UE identity cannot be derived by the network" (5GMM Cause: 9). Notably, the service reject message from the AMF was sent in plain (unencrypted) form. According to 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, ciphered (encrypted) to prevent security risks such as eavesdropping or replay attacks. In this test, the UE did not respond to the unprotected, plain service reject message from the AMF. This behavior aligns with 3GPP security recommendations: the UE should ignore or discard any NAS messages received in plain format after security context establishment, as these could be spoofed or tampered with by an attacker. By not responding to the unprotected message, the UE demonstrated proper adherence to the 5G security requirements and protected itself from potential security threats. 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 the 5G-AKA authentication procedure—which should establish security context for NAS message encryption—the UE sent a Service Request message to the AMF. The AMF, under tester control, responded with a Service Reject message, which was sent in plain (unencrypted) form and carried the 5GMM cause code 111 ("Protocol error, unspecified"). According to 3GPP TS 24.501, after 5G-AKA completes, both the UE and the network must protect subsequent NAS messages with integrity and ciphering unless explicitly allowed by the standard (for example, certain initial messages can be in plain, but not after security context establishment). The Service Reject message, being sent in plain, violates this requirement. The UE, upon receiving this unprotected message, did not respond. This behavior aligns with 3GPP security recommendations: the UE should ignore any unprotected NAS messages that should have been protected after security context establishment, to prevent potential security attacks such as replay or tampering. Therefore, the UE's action of not responding to the unprotected Service Reject message demonstrates secure behavior according to the 5G standard. 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 completing the 5G-AKA authentication procedure, the UE sent a service request to the AMF, which is the expected behavior following successful authentication. The AMF then responded with a service reject message, specifically indicating a 5GMM cause of 21 (synchronization failure), and crucially, this downlink NAS message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards (TS 33.501), after 5G-AKA is completed, both the UE and the network must establish NAS security, and all subsequent NAS messages—including service reject—should be integrity protected and, where possible, encrypted. The UE, upon receiving a plain (unencrypted) NAS message after security context is established, should treat it as suspicious and not respond, as accepting such messages could be a security risk (e.g., allowing an attacker to spoof critical network messages). In this case, the UE provided no response to the plain service reject, which aligns with the 3GPP security recommendations to prevent potential replay or spoofing attacks. Therefore, the UE's action in this scenario was secure and in compliance with 5G security standards. 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 the test scenario, after the completion of 5G-AKA authentication (which establishes shared keys for security), the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF issued a Security Mode Command to the UE, indicating the ciphering and integrity algorithms to be used (5G-EA6 and 128-5G-IA2) and included an ABBA value. Crucially, the Security Mode Command from the AMF was marked as "Protected," meaning it was integrity protected (and possibly encrypted) using the keys established during 5G-AKA. According to the 3GPP 5G security standard, after receiving a Security Mode Command, a compliant UE must verify the integrity of the message, derive the security keys as established, and respond with a Security Mode Complete message, also protected. However, in this test, the UE provided no response to the Security Mode Command. This lack of response is not compliant with the expected 3GPP behavior and exposes the UE to potential security risks, such as denial of service or session hijacking, as it fails to establish a secure NAS signaling context. Therefore, the UE's action—failing to respond to a protected Security Mode Command after 5G-AKA completion—demonstrates insecure behavior according to the 3GPP 5G security standard. 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 security test, after completing the 5G-AKA authentication, the UE sent an uplink NAS transport message to the AMF, which is standard procedure. The AMF then sent a Security Mode Command (SMC) message to the UE, intended to establish the NAS security context for subsequent message protection. However, the SMC from the AMF specified the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, meaning that no encryption or integrity protection would be applied to NAS messages. The security header of the SMC was also marked as "Unknown," and crucially, the UE did not respond to this SMC. According to 3GPP 5G standards (TS 24.501 and TS 33.501), after successful 5G-AKA, the UE and AMF must negotiate and activate suitable ciphering and integrity algorithms (other than null) to protect NAS signaling. The use of null algorithms is only permitted in very limited, controlled scenarios (e.g., for emergency services or specific test cases), and generally, the UE is expected to reject or not respond to an SMC proposing only null algorithms unless explicitly allowed. In this test, the UE's lack of response to an insecure SMC (proposing null algorithms) aligns with security best practices as outlined by the standards, as it prevents the establishment of an unprotected NAS security context. Therefore, the UE's action was secure according to the 5G standard. 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 5G-AKA (Authentication and Key Agreement), the UE sent a Service Request to the AMF, which is the expected behavior to resume communication or request resources. Following this, the AMF 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 (Plain NAS message). According to 3GPP 5G standards, specifically 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 applicable, ciphered (encrypted). The purpose of this is to prevent attackers from intercepting or tampering with sensitive signaling messages. In this test, the UE did not respond to the Configuration Update Command that was sent in plain text after 5G-AKA was completed. This behavior aligns with the 3GPP security specifications, as the UE is expected to discard or ignore any NAS messages that are not properly protected after security context establishment. By refusing to process or respond to an unprotected message, the UE upholds the required security posture and prevents potential exploitation of the signaling plane. Therefore, the UE's action in this scenario was secure. Secure

230	230	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.6443009376525879 UE to AMF UplinkNASTransport, Registration complete 0.644589900970459 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command, Unknown code (0x31) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this 5G standalone security test, the UE completed the 5G-AKA authentication procedure and then sent a "Registration Complete" message to the AMF. Following this, the AMF sent a "Security Mode Command" to the UE, but the 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 security standard, after successful completion of 5G-AKA, the NAS security context should be established, and subsequent security-related messages such as "Security Mode Command" must be protected with integrity and, where applicable, confidentiality. The fact that the AMF sent the Security Mode Command in plain text is a protocol violation; however, the focus here is on the UE's response. The UE did not respond to the Security Mode Command sent in plain text, which is the correct and secure behavior as per 3GPP specifications. The UE is required to ignore or discard any security-related NAS messages that are not properly protected after NAS security is activated, in order to prevent potential security attacks such as replay or man-in-the-middle attacks. Therefore, the UE's action—refusing to respond to an insecurely delivered Security Mode Command—demonstrates compliance with the 5G security standard and protects against protocol downgrades or exploitation. 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 security test of a 5G standalone User Equipment (UE), the 5G-AKA authentication procedure was successfully completed, establishing the necessary security context for subsequent NAS message encryption and integrity protection. Following this, the UE sent an Uplink NAS Transport message to the AMF, after which the AMF responded with a Security Mode Command message. Notably, the Security Mode Command was sent as a plain (unencrypted and non-integrity protected) NAS message, which is in accordance with the 3GPP 5G standard (TS 24.501), since the Security Mode Command must be sent in plain NAS before activating NAS security. However, the UE did not respond to the Security Mode Command, which is a deviation from expected behavior; per 3GPP standards, the UE is required to respond with a Security Mode Complete message to confirm the activation of NAS security. The lack of response from the UE means that NAS security was never established for subsequent messages, leaving the communication vulnerable to interception or tampering. This behavior is considered insecure as it fails to fulfill the required security handshake, potentially exposing sensitive information. 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 security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF sent an "authentication reject" message to the UE. Notably, this reject message was sent in plain (unencrypted) form, even though the 5G-AKA had already been completed and security keys should have been established for subsequent NAS message protection. According to the 3GPP 5G standards (TS 24.501), after successful authentication, all subsequent NAS messages—including service requests and rejections—must be integrity protected and, where possible, encrypted. The UE, upon receiving an unprotected (plain) authentication reject after security context establishment, correctly did not respond further, as processing unprotected NAS messages after security activation could be a security risk (such as susceptibility to replay or downgrade attacks). The UE's lack of response aligns with 3GPP security guidelines, which specify that UEs should ignore such messages to prevent exploitation. Therefore, the UE's behavior was secure according to the 5G standard. 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 the described 5G standalone security test, the User Equipment (UE) first completed the 5G-AKA authentication procedure, which establishes a secure context for further NAS message encryption and integrity protection. After this, the UE sent a service request to the AMF, which is the expected behavior to initiate further services. The AMF, under test control, responded with a plain (unencrypted and unprotected) Authentication Reject message, despite the security context having already been established. According to 3GPP standards (TS 24.501), once a security context is in place after 5G-AKA, the UE should only accept NAS messages that are integrity protected (and, if applicable, ciphered). When a plain (unprotected) message is received after security activation, the UE is required to ignore it and not respond, as this could be an attempt to exploit the UE or cause a security breach. In this test, the UE did not respond to the plain Authentication Reject message, which is the correct and secure behavior as per the 3GPP standards. This indicates that the UE properly enforced the security requirements and did not process potentially malicious or non-compliant messages. 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, the 5G standalone User Equipment (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. Subsequently, the AMF sent an identity request to the UE, specifically requesting the TMSI, and this message was transmitted in plain (unencrypted) form, as the security context was not established due to the incomplete 5G-AKA. The UE did not respond to the identity request. According to the 3GPP 5G standard, sensitive information such as subscriber identity should only be sent over an encrypted NAS connection, which is established after the completion of 5G-AKA. The UE’s refusal to respond to a plain (unencrypted) identity request before security activation is the expected and secure behavior, as responding could expose sensitive information to potential interception. Therefore, the UE's action in this scenario was in line with 3GPP security requirements and protected against possible identity disclosure attacks. 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 responded with an identity request for the IMEISV, which was sent as a plain (unencrypted) NAS message. Notably, the 5G-AKA procedure had not yet been completed, which means that NAS security (integrity and encryption) had not been activated for the session. According to the 3GPP 5G standard (TS 24.501), the IMEISV is considered a sensitive identifier, and the UE should only respond to identity requests for the IMEISV over a protected (encrypted) NAS connection, except in certain defined exceptional cases (such as emergency services or initial registration in some scenarios). Since the AMF sent the request in plain NAS before security activation, the UE correctly did not respond with the IMEISV, thereby protecting its privacy and preventing exposure of sensitive information over an unencrypted channel. This behavior aligns with 3GPP security recommendations and demonstrates that the UE is following the standard's security guidelines. 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, the UE and AMF completed the 5G-AKA authentication procedure, after which the UE sent an Authentication Response to the AMF. The AMF then issued a Security Mode Command to the UE, but this message was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard, once authentication is complete, the Security Mode Command is used to establish NAS security (ciphering and integrity protection) between the UE and the AMF. Until the Security Mode Command is accepted and the security context is activated, subsequent NAS messages (such as Deregistration Request) sent by the UE should not be protected. In this test, the UE, upon receiving the Security Mode Command in plain text, immediately sent a Deregistration Request (UE originating) before NAS security was established. This means the Deregistration Request was also sent in plain text, exposing it to potential interception or tampering. According to 3GPP standards, the UE should only send sensitive NAS messages (like Deregistration Request) after NAS security has been activated, i.e., after responding to the Security Mode Command and receiving confirmation that security is in place. Therefore, the UE's action of sending a Deregistration Request before NAS security was established is not compliant with 3GPP security requirements and exposes the communication to security risks. 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 uplink message to the AMF, as expected. The AMF then responded with a Security Mode Command, which is the standard next step to establish NAS security between the UE and the network. According to the test summary, the Security Mode Command message from the AMF was sent as a "Protected" message, using ciphering algorithm 5G-EA5 and integrity algorithm 5G-IA0 (null), with an ABBA value of 0000. Importantly, the UE did not respond to this Security Mode Command. According to 3GPP standards (TS 24.501 and TS 33.501), after 5G-AKA, the Security Mode Command should be sent integrity protected (and optionally ciphered) using the negotiated algorithms. However, using 5G-IA0 (null integrity) is generally not recommended, as it means the message is not integrity protected, which could expose the communication to certain attacks. The UE, upon receiving a Security Mode Command with null integrity protection (5G-IA0), is expected by the standard to reject the command and not proceed with security setup, as this configuration is insecure and not permitted for normal operation. The UE's lack of response aligns with a secure implementation: it did not accept an insecure security configuration (null integrity protection), thereby protecting itself from potential security vulnerabilities. Therefore, based on the 3GPP standard, the action taken by the UE was secure. Secure
238	238	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03967404365539551 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.03995108604431152 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, following which the AMF sent an Identity Request asking for the TMSI. Notably, this Identity Request was sent in plain (unencrypted) NAS signaling, as the 5G-AKA authentication and key agreement process had not yet been completed. According to 3GPP standards (TS 33.501), sensitive information such as the SUPI (permanent identity) must never be transmitted in cleartext, and even temporary identities like the TMSI should preferably be protected. However, before 5G-AKA is completed, there is no established NAS security context, so the initial exchange (including Identity Requests and Responses) may occur in the clear. The UE did not respond to the AMF's plain Identity Request for the TMSI, which is a cautious and security-conscious action, as responding would have exposed the TMSI without any NAS security in place. This behavior aligns with best security practices and the intent of the 3GPP standards, which aim to minimize the exposure of subscriber identities and related information before security is established. Therefore, the UE's action of not responding to a plain Identity Request before completion of 5G-AKA can be considered secure. 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 5G standalone User Equipment (UE) completed the initial NAS steps and responded to an identity request from the AMF by sending an Identity Response. Subsequently, the AMF issued another Identity Request, this time specifically requesting the IMEISV, and sent this message in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. The UE did not respond to this second request for the IMEISV. According to 3GPP 5G security standards, sensitive information such as the IMEISV should not be transmitted in plain text before the security context is established (i.e., before 5G-AKA is completed and NAS security is activated). By refusing to send the IMEISV in response to a plain (unencrypted) identity request prior to the completion of 5G-AKA, the UE adhered to the security guidelines intended to protect user privacy and device identity. Therefore, the UE's action of not responding with the IMEISV in this context was secure and compliant with the 3GPP 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, the 5G standalone User Equipment (UE) and the Access and Mobility Management Function (AMF) performed a typical NAS (Non-Access Stratum) security procedure. After successfully completing the 5G-AKA authentication phase, the UE sent an Authentication Response uplink message to the AMF. Subsequently, the AMF sent a Security Mode Command to the UE, which, according to the packet capture, was transmitted as a plain (unencrypted) NAS message. The Security Mode Command is always sent as a plain NAS message as per the 3GPP 5G standard (TS 24.501, section 9.2.2.2), since it is used to establish the NAS security context (i.e., to negotiate and activate ciphering and integrity protection algorithms). After receiving the Security Mode Command, the UE did not respond. According to 3GPP standards, the UE should only respond to a plain Security Mode Command if it is valid and expected at this stage; otherwise, it should ignore or silently discard unexpected or potentially malicious plain NAS messages after security context is established. Since the Security Mode Command was sent immediately after authentication and before security context activation, the UE's lack of response could indicate that it is correctly refusing to process a plain NAS message outside the expected context, thereby avoiding a potential security risk. This behavior aligns with secure implementation guidelines, as responding to unexpected or replayed plain NAS messages after authentication could expose the UE to security vulnerabilities such as downgrade or replay attacks. Therefore, based on the 3GPP standard and the sequence of events, the UE's action was secure. Secure

241	241	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.16009092330932617 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1604149341583252 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone UE and the AMF completed the 5G-AKA authentication, after which the UE sent a "security mode complete" message to the AMF, indicating that it accepted and activated the negotiated security algorithms (ciphering and integrity protection). Unexpectedly, the AMF then sent another "security mode command" to the UE, but this subsequent command was marked as "protected" and used the previously established security context (Cipher Algorithm: 5G-EA7, Integrity Algorithm: 128-5G-IA2). However, according to the 3GPP 5G standard (TS 24.501), the correct procedure is that once the UE sends "security mode complete," the security mode control procedure is finished, and the AMF should not send another "security mode command" unless a new security context is required (e.g., after a handover or context loss). The UE, in this case, did not respond to the unexpected protected "security mode command," which aligns with the 3GPP security requirements: a compliant UE must ignore or discard any out-of-sequence or redundant security mode commands to prevent downgrade or replay attacks. Therefore, the UE's lack of response demonstrates adherence to the standard and protects against potential protocol misuse or attacks. 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, the 5G standalone User Equipment (UE) and the AMF completed the 5G-AKA authentication procedure, after which the UE sent an Authentication Response to the AMF. Subsequently, the AMF sent a Security Mode Command to the UE, indicating the selection of ciphering and integrity protection algorithms (128-5G-EA1 and 128-5G-IA2, respectively) and including the ABBA parameter. According to the 3GPP 5G standard, after successful authentication, the Security Mode Command is used by the AMF to establish NAS security (encryption and integrity protection) for subsequent NAS messages. The Security Mode Command message from the AMF was sent as "Protected," which is expected after authentication. However, the UE did not respond to this command. According to 3GPP TS 24.501, after receiving a valid Security Mode Command, a compliant UE must respond with a Security Mode Complete message to confirm the establishment of NAS security. The absence of any response from the UE indicates non-compliance with the standard, as it neither accepted nor rejected the security configuration. This behavior could result in a denial of service or a security vulnerability, as the UE is not establishing the required secure NAS context. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. Insecure

243	243	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0293 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.15967893600463867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15994000434875488 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response uplink message to the AMF. Subsequently, the AMF sent a Security Mode Command downlink message to the UE, which was transmitted as a plain (unencrypted) NAS message, as indicated by the security header being set to "Plain NAS message (0)". According to the 3GPP 5G standards (TS 24.501), after 5G-AKA is completed, the Security Mode Command is the first NAS message that establishes the NAS security context (ciphering and integrity protection) between the UE and the AMF. This Security Mode Command must be sent as a plain NAS message since no NAS security context is yet established; only after the UE successfully processes this command and responds (with a Security Mode Complete message) can subsequent NAS messages be encrypted and integrity protected. In this test, the UE did not respond to the Security Mode Command. According to the standard, the UE should only process and respond to a plain Security Mode Command immediately after authentication, and must ignore any unexpected or out-of-sequence plain NAS messages. Since the Security Mode Command was sent at the correct point in the procedure (immediately following authentication), the UE's lack of response is not compliant with 3GPP specifications, as it should have replied with Security Mode Complete. However, from a security perspective, the UE did not prematurely accept or process plain NAS messages outside the expected sequence, nor did it reveal any sensitive information in the clear. The absence of a response does not expose the UE to a security vulnerability, but it does indicate a lack of interoperability or protocol compliance rather than an explicit security flaw. Thus, while the UE did not behave strictly according to the 3GPP protocol, it did not act insecurely in a way that would compromise its security context or expose sensitive data. 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 completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, which is the expected behavior indicating that the UE has accepted the security algorithms and parameters negotiated during the Security Mode Command. However, the AMF then sent another "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 a security context is active, all subsequent NAS messages exchanged between the UE and AMF must be integrity protected and, if required, ciphered, unless the null ciphering algorithm (5G-EA0) is in use, in which case only integrity protection applies. In this test, the ciphering algorithm was set to 5G-EA0 (null), but the integrity algorithm was 128-5G-IA2, so messages should still be integrity protected. The UE, upon receiving a plain, unprotected security mode command 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 unprotected NAS messages after security is established, to prevent downgrade or replay attacks. Therefore, the UE's refusal to respond to the insecure, plain message was the correct and secure action in accordance with the 5G standard. 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, 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. After this, the AMF sent an Identity Request message to the UE, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version), and this message was sent in plain (unencrypted) form because the security context had not yet been established. The UE, in response, did not provide any response to this identity request. According to the 3GPP 5G security standard, sensitive information such as the IMEISV should not be sent in the clear before security activation (i.e., before 5G-AKA is completed and NAS security is established). By refusing to respond to a plain (unencrypted) identity request for the IMEISV, the UE is protecting its sensitive information from potential interception or exposure, as recommended by 3GPP security guidelines. Therefore, the UE's action aligns with the security requirements of the 5G standard and demonstrates secure behavior. 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 message, specifically requesting the TMSI, and this message was sent in plain (unencrypted) form. Importantly, the 5G-AKA authentication procedure had not yet been completed, which means that the NAS security context (encryption and integrity protection for NAS messages) was not yet established. According to the 3GPP 5G security standards, the UE must not send permanent or sensitive identities (such as SUPI or IMSI) in cleartext before a secure context is established, but it may provide a temporary identifier like the TMSI if requested, since this is not considered a permanent identity. However, in this case, the UE did not respond at all to the plain identity request from the AMF. This behavior is actually more secure than responding, as it avoids exposing any identity—even a temporary one—over an unprotected channel, which could be a defense against certain downgrade or impersonation attacks. Therefore, the UE's action demonstrates a cautious and security-conscious approach, adhering to the principle of not disclosing even temporary identities before secure communication is established, which is arguably stricter than the minimum requirements but aligns with a security-first interpretation of the 3GPP standards. 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, which was sent in plain (unencrypted) NAS signaling because the 5G-AKA security procedure had not yet been completed. According to 3GPP standards (TS 33.501), sensitive information such as the IMEISV should only be transmitted after a secure NAS signaling connection has been established, which occurs after the successful completion of the 5G-AKA authentication and key agreement procedures. In this case, since the AMF requested the IMEISV before security was activated, the UE correctly did not respond to the identity request. This behavior aligns with 3GPP security recommendations, which stipulate that the UE must not disclose sensitive identifiers like the IMEISV over an unprotected channel. Therefore, the UE's action was secure and compliant with the 5G standard. 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 5G standalone security test, the 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 cipher (128-5G-EA2) and integrity (128-5G-IA3) algorithms, as indicated in the summary. However, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after successful authentication and upon receiving a protected Security Mode Command, the UE is expected to verify the integrity and correctness of the message and respond with a Security Mode Complete message if the command is valid and the selected algorithms are supported. The absence of any response from the UE suggests that it either failed to process the protected message or did not recognize the security header, which is not compliant with 3GPP specifications. This lack of response could indicate a failure to establish secure NAS security context or an inability to handle protected messages, both of which are security concerns. Therefore, based on the observed behavior and 3GPP requirements, the UE's action in this scenario is considered insecure. Insecure
249	249	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.7274200916290283 UE to AMF UplinkNASTransport, Service request 0.7277319431304932 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF, which is a typical step for initiating a session or resuming communication. The AMF then responded with a Configuration Update Command, but crucially, this downlink NAS message was sent as a plain (unencrypted and unauthenticated) message, as indicated by the "Plain NAS message (0)" security header. According to 3GPP 5G security standards (TS 33.501), after the 5G-AKA procedure is completed and security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, when possible, encrypted. The UE, upon receiving a plain (unprotected) NAS message after security activation, is expected to disregard the message and not respond, as accepting such messages could expose the UE to security threats such as spoofing or replay attacks. In this test, the UE did not respond to the unprotected Configuration Update Command, which is the correct and secure behavior as mandated by the 3GPP standard. This indicates that the UE properly enforced the requirement to only accept protected NAS messages after security context establishment. 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 sent an identity request message to the UE, specifically requesting the IMEISV, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to 3GPP 5G security standards (TS 33.501), sensitive information such as IMEI/IMEISV should not be transmitted over the air in plain text unless ciphering has been activated, which only occurs after successful completion of 5G-AKA. In this test, the UE did not respond to the AMF's plain (unciphered) identity request for the IMEISV, thereby refusing to send sensitive information without encryption. This behavior aligns with the 3GPP security recommendations to protect subscriber privacy and prevent exposure of device identifiers to potential eavesdroppers. Therefore, the UE's action in withholding the IMEISV in the absence of security context demonstrates adherence to best security practices as defined by the standard. 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 UE completed the initial NAS procedures 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) NAS as the 5G-AKA procedure had not yet been completed. According to 3GPP 5G security standards, particularly TS 33.501, sensitive information such as permanent or temporary identities (like TMSI) should only be exchanged over protected (integrity protected and, if possible, ciphered) NAS signaling, which is only established after successful completion of the 5G-AKA authentication and key agreement procedure. Since the UE did not respond to the AMF's subsequent plain Identity Request for the TMSI, it correctly withheld its identity information in the absence of an established NAS security context. This behavior aligns with 3GPP security guidelines, as responding with identity information over unprotected NAS would expose the UE to potential identity interception attacks. Therefore, the UE's action in this scenario was secure and compliant with 5G security standards. 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 security test, after the initial NAS procedures, the UE sent an Identity Response to the AMF, and then the AMF sent another Identity Request, specifically requesting the IMEISV, in plain (unencrypted) NAS messaging. At this point, the 5G-AKA authentication and key agreement procedure had not yet been completed, which means that NAS security (encryption and integrity protection) was not yet established. According to 3GPP 5G standards, the IMEISV (International Mobile Equipment Identity and Software Version) is considered a sensitive identifier and should only be transmitted over a protected (encrypted) NAS connection unless absolutely necessary (such as in exceptional circumstances, e.g., for lawful interception or regulatory compliance). In this scenario, the UE did not respond to the AMF's plain (unencrypted) Identity Request for the IMEISV. This behavior aligns with the security recommendations of the 3GPP standard, which aims to prevent exposure of sensitive device identifiers before a secure channel is established. Therefore, the UE's refusal to send the IMEISV over an unprotected connection demonstrates a secure and standards-compliant action. Secure
253	253	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.7599589824676514 UE to AMF UplinkNASTransport, Service request 0.7601721286773682 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF issued an Identity Request message, specifically requesting the GUTI (Globally Unique Temporary Identifier) from the UE. Notably, the Identity Request was sent in plain (unencrypted) NAS signaling, despite the fact that 5G-AKA (and thus NAS security context establishment) had already been completed. The UE did not respond to this request. According to the 3GPP 5G standard, once the 5G-AKA and security mode procedures are completed, all subsequent NAS messages—including any identity requests—must be protected (integrity protected and ciphered). Sending or responding to identity requests in plain NAS after security activation is a violation of this standard, as it exposes sensitive identifiers to potential interception. The UE's refusal to respond to an unprotected identity request after security activation is therefore compliant with 3GPP security requirements and demonstrates secure behavior. 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 and key agreement), the UE sent an Uplink NAS Transport message to the AMF, specifically a PDU session establishment request. The AMF then responded with a Service Accept message, which, according to the packet capture, was sent as a plain (unencrypted) NAS message. Notably, the UE did not respond to this downlink message. According to the 3GPP 5G security standard (TS 33.501), after 5G-AKA is completed and security mode is established, all subsequent NAS signaling messages between the UE and the AMF must be both integrity protected and ciphered (encrypted), except for a small set of explicitly allowed exceptions (such as certain initial messages before security activation). The Service Accept message is not among these exceptions. By not responding to the unprotected (plain) Service Accept message, the UE demonstrated correct and secure behavior: it refused to process or accept a NAS message that was not properly protected after security activation. This action aligns with the 5G security requirements and helps prevent downgrade or interception attacks. 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 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 sent this message in plain (unencrypted) form. The UE did not respond to this Identity Request. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA has been completed, all subsequent NAS signaling—including identity requests—should be protected by NAS security (i.e., encrypted and integrity protected). The IMEI is considered a sensitive identifier, and transmitting it in the clear after security context establishment would expose the UE to privacy risks, such as device tracking or unauthorized identification. By refusing to respond to a plain (unencrypted) identity request after security establishment, the UE is adhering to the 3GPP security guidelines, which recommend that the UE should not send sensitive information like the IMEI unless the NAS security context is active. Therefore, the UE's action in this scenario is consistent with 3GPP security requirements and demonstrates a secure behavior. 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 a successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "registration complete" message to the AMF, which is the expected behavior according to 3GPP standards. Following this, the AMF (under tester control) sent a GMM status message to the UE with a 5GMM cause value of 97 ("Message type non-existent or not implemented"), and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards (TS 24.501, TS 33.501), once 5G-AKA is completed and security context is established, all subsequent NAS messages between the UE and AMF are required to be integrity protected and, where applicable, encrypted. The UE, upon receiving an unprotected (plain) NAS message after security activation, is expected to ignore the message and not process or respond to it, as a security safeguard against potential attacks or protocol misuse. In this test, the UE did not respond to the unprotected GMM status message from the AMF, which aligns with the secure behavior mandated by the 3GPP specifications. This demonstrates that the UE correctly enforced NAS security requirements by refusing to process or acknowledge messages that violate security expectations after authentication and security mode are established. 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 completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context was established and NAS security should be active. However, the AMF subsequently 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), once the 5G-AKA is completed and a security context is established, all subsequent NAS messages—including identity requests—must be protected (integrity-protected and, if possible, ciphered). The UE is expected to ignore or reject any plain NAS messages received after security activation, as responding to unprotected requests could expose sensitive information and undermine the security guarantees of 5G. Therefore, the UE's refusal to respond to the unprotected "Identity Request" is fully compliant with 3GPP security requirements and demonstrates secure behavior in this context. Secure

258	258	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Plain Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.4842751026153564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4844861030578613 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport 2.688286066055298 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE successfully completed the 5G-AKA authentication and security procedures, which are prerequisites for establishing a secure NAS communication channel as defined by 3GPP standards. Following this, the UE sent a "Registration complete" message, which is standard behavior. The AMF, under test control, then sent a deregistration request to the UE. According to the packet capture, this deregistration request from the AMF was sent as a plain message (i.e., not encrypted), but it had a security header indicating "integrity protected and ciphered (2)." The UE then responded with a Deregistration request (UE originating). Focusing solely on the UE's behavior, after 5G-AKA, the UE continued to send messages using the security context established during authentication, as required by the 3GPP standards. The UE's actions—completing registration and processing deregistration requests—were in line with expected secure procedures, provided that it maintained the integrity and encryption of its own NAS messages after security mode was enabled. Since the UE did not process or respond to any plain (unencrypted) NAS messages after security was established and continued to use protected communication, its behavior adhered to the security requirements outlined by 3GPP for 5G standalone operation. Therefore, the UE's actions in this scenario were secure. 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 successfully completing the 5G-AKA procedure—which establishes mutual authentication and sets up NAS security between the UE and the AMF—the UE sent an Uplink NAS Transport message to the AMF. 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, once NAS security is activated following 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where required, ciphered. The only exception is for certain emergency or initial registration scenarios, which do not apply here since 5G-AKA was already completed. Upon receiving a plain (unencrypted) NAS message after security activation, a standards-compliant UE should ignore the message and not respond, as processing such unsecured messages could expose the UE to security risks such as downgrade or replay attacks. In this test, the UE did not respond to the plain GMM Status message from the AMF, which aligns with the security requirements outlined by 3GPP. Therefore, the UE's action 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 the end of the registration procedure. Immediately after, the AMF (under test control) sent a "5GMM Status" message with cause 101 ("Message not compatible with the protocol state") in plain (unencrypted) format, despite the fact that the 5G-AKA had already been completed, which normally establishes NAS security. Upon receiving this unprotected status message, the UE responded with a "Deregistration Request (UE originating)" uplink message. According to 3GPP 5G security standards (TS 24.501 and TS 33.501), after 5G-AKA is completed, all subsequent NAS messages must be integrity protected and, where required, encrypted. The 5GMM Status message, if sent after NAS security is established, must be protected; unprotected messages after this point are considered abnormal and may indicate a security attack such as a downgrade or replay attack. The expected secure behavior from the UE, as outlined in the standards, is to discard any unprotected NAS message received after security activation, and optionally to log or notify the user or network of the anomaly, but not to react to its content (i.e., not to process or act upon the unprotected message). In this test, the UE processed the unprotected status message and initiated a deregistration procedure in response, which is not compliant with the 5G security requirements and exposes the UE to potential attacks (e.g., forced deregistration by an attacker sending unprotected messages). Therefore, the action taken by the UE was insecure, as it violated the 3GPP security requirements by accepting and acting upon an unprotected NAS message after security activation. 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 security test of a 5G standalone User Equipment (UE), the authentication procedure (5G-AKA) was successfully completed, establishing the necessary security context for protected NAS messaging. Following this, the UE sent a service request to the AMF, which responded with a Security Mode Command message. Notably, this Security Mode Command was sent as a protected (encrypted and integrity-protected) message, with specified ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and an ABBA value of 0101. However, the UE did not respond to the Security Mode Command, and the security header type for the downlink message was reported as "Unknown." According to 3GPP 5G standards, after successful authentication, the UE is expected to process the Security Mode Command and respond with a Security Mode Complete message, confirming acceptance of the negotiated security algorithms and keys. The absence of any response from the UE indicates a failure to proceed with the required security procedure, potentially leaving the connection in an incomplete or vulnerable state. This lack of response is not compliant with 3GPP specifications and could represent insecure behavior, as it prevents the establishment of a fully secure NAS communication channel. Insecure

262	262	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.914944887161255 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.915573835372925 AMF to UE SACK (Ack=13, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF. In response, the AMF sent a Security Mode Command message as a plain (unencrypted and unauthenticated) NAS message, specifying ciphering with 5G-EA0 (null, i.e., no encryption) and integrity protection with 128-5G-IA2, and with the ABBA parameter set to 0000. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF should be integrity protected and, where possible, ciphered (unless ciphering is explicitly not supported or not required for certain messages, but Security Mode Command is a critical message that should be integrity protected). The Security Mode Command is normally sent with a security header to ensure authenticity and integrity, not as a plain NAS message. The UE, upon receiving a Security Mode Command in plain NAS format after authentication, did not respond. This behavior aligns with the 3GPP security requirements, as the UE should reject or ignore NAS messages that are not properly protected after authentication is established, to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to an insecure Security Mode Command was correct and in accordance with the 5G standard. 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 successfully completing the 5G-AKA authentication and key agreement procedure, 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) NAS. Importantly, after receiving this unprotected Registration Reject, the UE did not respond further. According to the 3GPP 5G standard (TS 24.501, section 5.4.1.4.2), after the successful completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted. If the UE receives a Registration Reject message in plain NAS after security has been established, it is required by the standard to ignore it and not act upon it, as this could be a security attack (e.g., a downgrade or spoofing attempt). In this test, the UE's behavior—providing no response to the unprotected Registration Reject after security context establishment—aligns with the 3GPP security requirements and demonstrates correct handling of potentially insecure messages. Therefore, the UE's actions were secure. Secure

264	264	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 6 UE provided: No response The packet capture during the test using wireshark is: 2.427165985107422 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4275641441345215 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4278719425201416 AMF to UE DownlinkNASTransport, Registration reject (Illegal ME) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was completed successfully between the User Equipment (UE) and the Access and Mobility Management Function (AMF), establishing the necessary security context for protected NAS communication. Following this, the UE sent an Uplink NAS Transport message to the AMF, which should have been encrypted and integrity protected per 3GPP TS 33.501 requirements, since the security context was already established. The AMF then responded with a Registration Reject message, carrying a 5GMM cause of 6 (Illegal ME), and this message was sent in plain (unencrypted) form. The UE, upon receiving this unprotected Registration Reject message after security activation, did not respond to it. According to 3GPP standards, after the security context is established, the UE must only accept NAS messages that are both encrypted and integrity protected; any plain (unprotected) messages received after this point should be ignored to prevent security breaches such as downgrade or spoofing attacks. The UE’s refusal to respond to the unprotected Registration Reject message demonstrates compliance with the 5G security requirements, as it correctly ignored a non-secure message following security activation. Therefore, the UE’s behavior in this test was secure. Secure

265	265_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1111 RAND: 0e38a634245d3e4aea72a7f7a7148161 AUTN: 3d9033e57f3e8000d3eb278394dd7c46 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 1.0084679126739502 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0087080001831055 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Authentication request 1.216444969177246 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. The AMF then responded with an authentication request message, which was sent in plain (unencrypted) form and reused the same ngKSI (NAS Key Set Identifier) that was already in use, as indicated by "ngKSI_TSC: Native security context" and "ngKSI_KSI: 5." Upon receiving this, the UE replied with an "Authentication failure (ngKSI already in use)" message. According to the 3GPP 5G security standards, once the 5G-AKA procedure is completed and a security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, if required, encrypted. The reuse of an existing ngKSI for a new authentication request, especially in plain text, could indicate a replay or downgrade attack attempt. The UE's action to detect this and respond with an authentication failure is compliant with the 3GPP security specifications, as it prevents the reuse of an already active security context and avoids potential security breaches. Therefore, the UE's behavior in this scenario is secure, as it correctly identified an abnormal condition and refused to proceed insecurely. 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.	During this security test, the 5G standalone User Equipment (UE) completed the 5G-AKA authentication procedure with the Access and Mobility Management Function (AMF), which typically establishes mutual authentication and cryptographic keys for securing subsequent NAS messages. After authentication, the UE sent an Uplink NAS Transport message (PDU session establishment request) to the AMF. In response, the AMF—under test control—sent an Authentication Reject message to the UE, and this message was sent in plain (unencrypted) format. Notably, the UE did not respond to this plain Authentication Reject message. According to the 3GPP 5G standard (TS 24.501 and TS 33.501), after successful completion of 5G-AKA, NAS messages must be integrity protected and, where applicable, ciphered. If the UE receives a NAS message that is not integrity protected or is sent in plain after security has been activated, the UE is required to discard the message and take no further action, as processing such messages could expose it to security risks like replay or injection attacks. In this test, the UE correctly ignored the unprotected Authentication Reject message, demonstrating compliance with the 5G security standard and protecting itself from potential security threats. Secure

267	267	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.5199449062347412 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201799869537354 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, specifically a PDU session establishment request. In response, the AMF sent an Authentication Reject message to the UE, and this message was transmitted 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. The Authentication Reject message, however, is an exception as per 3GPP TS 24.501, clause 9.11.3.3, which allows the AMF to send this message in plain NAS if security context is not established or if there is a failure in authentication. The critical point in this test is the UE's reaction: upon receiving the plain Authentication Reject message, the UE did not respond further. This is the expected and secure behavior, as the UE should not proceed with any further NAS communications or attempts to establish a session upon receiving an Authentication Reject, particularly when it is sent in plain. The UE's lack of response ensures that it does not inadvertently continue communication in an insecure state or with a potentially compromised network. Thus, the UE acted securely according to the 5G standard. 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, the 5G-AKA authentication and key agreement procedure was successfully completed, establishing a secure context for subsequent NAS messages. The UE then sent a "Registration Complete" message to the AMF, after which the AMF responded with a "Configuration Update Command" message that was indicated as "protected," though the security header was marked as "unknown." Critically, the UE did not respond to this downlink message. According to the 3GPP 5G standard, after security context establishment via 5G-AKA, all subsequent NAS messages must be integrity protected, and, where required, encrypted. If the UE receives a NAS message with an unknown or unexpected security header, or if the message cannot be properly authenticated or decrypted, the UE is required to discard the message and not process it further, as a security measure to prevent potential attacks or unauthorized configuration changes. The UE's lack of response to the configuration update command, given the ambiguity in the security header, aligns with secure behavior as prescribed by the standard, since processing a potentially unprotected or malformed message could expose the UE to risk. Therefore, the UE's action in this interaction was appropriate and secure according to 3GPP requirements. 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 successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior according to the 3GPP 5G NAS protocol. However, the subsequent message from the AMF to the UE was a "Deregistration Accept" message, which was sent in plain (unencrypted) format, even though 5G-AKA had already been completed and security context should have been established. The UE, upon receiving this plain (unencrypted) "Deregistration Accept" message from the AMF, did not respond. According to the 3GPP standard (TS 24.501), after security context establishment, all subsequent NAS messages exchanged between the UE and AMF must be integrity protected and, where required, encrypted. If the UE receives a NAS message that is not protected as mandated by the established security context, it should discard the message and not act upon it, as a security measure to prevent attacks such as replay or spoofing. In this case, the UE's action of not responding to the unprotected "Deregistration Accept" message is compliant with the 3GPP standard and demonstrates secure behavior, as it did not process or acknowledge an insecure message after security was established. 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 security test, after completing the initial NAS procedures, the UE sent an Identity Response message to the AMF, and subsequently, the AMF sent another Identity Request message to the UE, specifically requesting the IMEISV. Importantly, this Identity Request was sent as a plain (unencrypted) NAS message, which is expected since the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning NAS security context was not established. According to the 3GPP 5G standard (TS 24.501), the UE is required to only provide sensitive information such as IMEISV in response to an Identity Request if NAS security (encryption and integrity protection) has already been activated. If the AMF requests the IMEISV before NAS security is established, the UE is expected to withhold this information and not respond with its IMEISV in cleartext to protect its privacy and security. In this test, the UE did not respond to the plain IMEISV request, which aligns with the 3GPP security requirements and demonstrates that the UE correctly protected sensitive information. Therefore, based on the 5G standard and the interaction observed, the action taken by the UE was secure. 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 the described test, the UE and AMF were engaged in NAS communication, but the 5G-AKA authentication procedure had not yet been completed, meaning that NAS messages were still being exchanged in plain (unencrypted) form. After the UE sent an identity response, the AMF sent another identity request, specifically asking for the IMEI, and this request was sent in plain text. Importantly, the UE did not respond to this request. According to the 3GPP 5G standard, sensitive information such as the IMEI should not be transmitted in plain text after the initial authentication and security setup (5G-AKA) has been completed, to prevent exposure of the device's unique identifier to potential attackers. The UE's refusal to respond to the identity request for the IMEI, when the message was sent unencrypted before security procedures were established, aligns with 3GPP security recommendations, which stipulate that UEs should not disclose permanent or sensitive identities over unprotected channels. This behavior helps protect user privacy and device security by ensuring that critical information is not exposed before encryption is in place. Therefore, the UE's action of not responding to the plain identity request for IMEI prior to security activation was in accordance with the 5G standard and demonstrated secure behavior. 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 registration procedure by sending an initial registration request to the AMF. The AMF, under test control, responded with a service accept message, which was sent as a protected (i.e., integrity protected and/or ciphered) NAS message. However, the 5G-AKA authentication procedure, which is required for establishing security contexts and enabling NAS message protection, had not yet been completed. According to the 3GPP 5G standards, specifically TS 24.501, NAS messages should not be protected (encrypted/integrity protected) before the completion of the 5G-AKA authentication and key agreement procedure. The UE, upon receiving a protected service accept message before security context establishment, responded with a deregistration request, effectively aborting the registration process. This behavior demonstrates that the UE correctly identified the premature application of NAS security and refused to proceed with a potentially insecure registration, as per the 3GPP requirements. The UE's action prevented further communication under an invalid security context, showing compliance with the standard and protecting against possible security risks. Secure

273	273	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11984086036682129 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12007284164428711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF immediately sent a deregistration request back to the UE. Notably, this deregistration request was sent with the security header indicating that the message was both integrity protected and ciphered, even though the 5G-AKA procedure—which is responsible for establishing the necessary security context—had not yet been completed. According to the 3GPP 5G standards, specifically TS 24.501 and TS 33.501, security protection (integrity and ciphering) for NAS messages should only be applied after the successful completion of the authentication and key agreement (AKA) process, as this is when the required security keys are derived and shared between the UE and the network. Since the UE did not respond to the deregistration request that was protected before security context was established, it indicates that the UE correctly refused to process a message with security protection prior to the completion of 5G-AKA. This behavior aligns with the 3GPP security requirements, as processing protected messages before establishing a security context could expose the UE to potential attacks or protocol violations. 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, after the UE sent an authentication response to the AMF, the AMF immediately sent a deregistration request with integrity protection, even though the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards, the 5G-AKA authentication process must be fully completed before any NAS security context is established, which is a prerequisite for enabling integrity protection and encryption of NAS messages. Since the 5G-AKA was not completed, the UE had not yet derived the necessary keys to validate or process protected NAS messages. The UE did not respond to the deregistration request, which was sent with integrity protection, indicating that it did not process the message due to the lack of a valid security context. This behavior aligns with the 3GPP standard, as the UE should not accept or process protected messages before authentication and key agreement are finalized. Therefore, the UE’s action in not responding to the protected deregistration request was secure and compliant with the 5G security requirements. 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) (dereg MME) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following 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 its initial registration request to the AMF, the AMF responded with a deregistration request message that was marked as both integrity protected and ciphered (security header type 2). However, the 5G-AKA authentication procedure had not yet been completed, meaning that no security context (keys for integrity and ciphering) should have been established between the UE and the AMF at this stage. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) can only be applied after successful completion of the 5G-AKA authentication and security mode command and procedures, which establish the required keys. Since the AMF sent a protected message before this was allowed, the UE, adhering to the standard, did not respond to the deregistration request. This lack of response indicates that the UE correctly rejected or ignored a message that was improperly protected before security context establishment, thereby maintaining the integrity and security of its communication as per 3GPP specifications. Therefore, the UE's behavior 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, the UE and AMF engaged in initial NAS communication, with the UE sending an identity response and the AMF subsequently sending a Security Mode Command. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that key material for NAS security had not been established. The Security Mode Command from the AMF was sent as a plain (unencrypted, unprotected) NAS message, which is permitted by 3GPP standards prior to the completion of 5G-AKA. The UE did not respond to this Security Mode Command. According to 3GPP TS 24.501 and related specifications, a compliant UE should not accept or respond to a Security Mode Command that attempts to establish NAS security before the authentication and key agreement (5G-AKA) procedure is completed, as this would expose the UE to potential security risks, such as man-in-the-middle attacks. By not responding to the Security Mode Command sent in the clear before 5G-AKA completion, the UE demonstrated correct and secure behavior, adhering to the 3GPP security requirements and protecting itself from possible exploitation. 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 5G standalone User Equipment (UE) successfully completed the initial NAS procedures up to sending an Identity Response to the Access and Mobility Management Function (AMF). Immediately following this, the AMF sent a Configuration Update Command to the UE, with the NAS message marked as "integrity protected" (security header type 1), but the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. According to the 3GPP 5G standards, NAS message protection (integrity and/or ciphering) must only be applied after the successful completion of the authentication procedure (5G-AKA), as this is when the necessary security keys (KAMF) are established. Since the AMF sent a protected NAS message before the security context was established, the UE, following the standard, should not process or respond to such messages, as it cannot validate the integrity protection without the derived keys. The UE's lack of response to the protected Configuration Update Command demonstrates adherence to the 3GPP standard and prevents potential security vulnerabilities that could arise from processing messages with invalid or missing security contexts. Thus, the UE's action in this scenario was in line with the expected secure behavior as per 3GPP specifications. 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, the 5G standalone User Equipment (UE) completed the initial NAS steps and responded to an identity request by sending an identity response to the AMF. At this stage, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that security context establishment (enabling NAS message encryption and integrity protection) was not in place. The AMF, under test control, then sent a configuration update command to the UE using a plain (unencrypted and non-integrity-protected) NAS message, as indicated by the security header type 0. Upon receiving this plain configuration update command, the UE did not process the command but instead initiated a deregistration request, effectively refusing to proceed further in an unsecured state. According to the 3GPP 5G standards (TS 24.501), sensitive NAS messages such as configuration update commands must not be accepted by the UE in plain NAS unless a security context has been established; the UE is expected to either ignore the message or deregister itself to prevent potential security threats. By refusing to process the plain configuration update and deregistering, the UE demonstrated correct and secure behavior as mandated by the standards, thereby protecting itself from possible attacks or misconfigurations in an unprotected state. 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 NAS communication by sending an initial registration request to the AMF, indicating the start of the 5G attach procedure. However, before the 5G-AKA authentication and key agreement process was completed—meaning no NAS security context was established—the AMF (under test control) sent a deregistration accept message to the UE, and this message was sent as "Protected" (i.e., integrity protected and/or encrypted). According to the 3GPP 5G standard, NAS messages can only be protected (i.e., integrity protected and/or ciphered) after the successful completion of authentication and key establishment (5G-AKA), which creates the necessary security context. The UE, upon receiving a protected message before security context establishment, is expected to ignore or discard such a message and not respond, as it cannot verify the protection without keys. In this test, the UE did not respond to the protected deregistration accept message sent before 5G-AKA completion, which aligns with 3GPP security requirements and is the correct, secure behavior. The UE's action prevented a potential security vulnerability where an attacker could send protected messages before security context setup. 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, as expected in the NAS procedure. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is necessary to establish NAS security and enable encryption and integrity protection of NAS messages—the AMF responded with a "deregistration accept" message. This message was sent as "protected" (i.e., with NAS security applied), even though the security context had not yet been established due to the absence of 5G-AKA completion. According to the 3GPP 5G security specifications, the UE should only accept protected NAS messages after a security context has been established, and any protected messages received before authentication and key agreement should be ignored or rejected. In this case, the UE did not respond to the protected deregistration accept message, which indicates that it properly ignored a message that should not be accepted prior to completing 5G-AKA. This behavior aligns with 3GPP security requirements, as it prevents potential security vulnerabilities such as replay or spoofing attacks before mutual authentication and key establishment. 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 an initial registration request to the AMF, which is the expected first step in establishing a 5G connection. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning no security context (i.e., keys for encryption and integrity protection) had been established between the UE and the network. Despite this, the AMF sent a Configuration Update Command to the UE as a protected (integrity protected and ciphered) NAS message, using a new security context (security header type 4). According to 3GPP 5G standards, the UE should only accept and process protected NAS messages after the 5G-AKA procedure is complete and a valid security context is in place. Since the UE did not respond to the AMF's protected message (sent before 5G-AKA had established the necessary keys), it correctly rejected or ignored this message, adhering to the security procedures outlined by 3GPP. This behavior prevents potential security risks such as replay or spoofing attacks during the unauthenticated phase of registration. Therefore, the UE's action was secure and compliant with 3GPP standards. 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 the registration procedure by sending an unprotected initial registration request to the AMF, as is standard before security context establishment. The AMF, under test control, responded with a Configuration Update Command that was integrity protected and ciphered, indicating that it was sent as a secured NAS message. However, according to the 3GPP 5G standard, NAS message protection (integrity and ciphering) can only be applied after successful completion of the 5G-AKA authentication and key agreement procedure, which establishes the necessary security context. Since the 5G-AKA was not completed at the time the AMF sent the protected message, the UE had not yet established the required security keys to decrypt or verify the message. The UE, therefore, did not respond to the protected Configuration Update Command. This behavior aligns with the 3GPP security requirements, as the UE should ignore or not process protected NAS messages received before security context establishment, thereby preventing potential security vulnerabilities. In summary, the UE's action of not responding to the prematurely protected downlink message was secure and compliant with the 5G standard. 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, after the UE initiated registration with the AMF by sending an unprotected initial registration request, the AMF responded with a Service Accept message that was sent as a protected (encrypted and integrity-protected) NAS message. However, the 5G-AKA authentication procedure, which is required to establish security keys for protecting NAS messages, had not yet been completed. According to the 3GPP 5G standard, NAS message protection (encryption and integrity protection) must only be applied after successful completion of the 5G-AKA authentication and key agreement, as this process provides the necessary security context for both the UE and the AMF. Since the AMF sent a protected message before the security context was established, the UE did not respond, which aligns with the expected secure behavior defined by the standard: the UE should ignore or discard protected NAS messages received before security activation. This action prevents the possibility of a security context mismatch or key synchronization issues that could be exploited by attackers. Therefore, the UE's decision to not respond to the protected Service Accept message before 5G-AKA completion demonstrates adherence to the 3GPP security requirements and is considered secure. Secure
284	284	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006928443908691406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2013227939605713 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the User Equipment (UE) initiated a 5G registration procedure by sending an initial registration request to the Access and Mobility Management Function (AMF). The AMF, under tester control, responded with a Service Accept message, which was sent as a protected (i.e., integrity protected and/or ciphered) NAS message. However, the 5G-AKA (Authentication and Key Agreement) procedure, which is responsible for mutual authentication and the establishment of NAS security keys, had not yet been completed at this point in the exchange. According to the 3GPP 5G security standard, specifically TS 33.501, NAS security (which includes encryption and integrity protection of NAS messages) must not be activated before successful completion of 5G-AKA. The UE is required to reject or ignore any protected NAS messages received before NAS security is established, as it cannot verify their authenticity or decrypt them without the necessary security context. In this test, the UE responded to the prematurely protected Service Accept message from the AMF by sending a Deregistration request, effectively aborting the registration process. This behavior aligns with the 3GPP security requirements, as the UE did not proceed with unsecure or unverifiable communication and instead took steps to terminate the session. Therefore, the UE acted securely in this scenario according to 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) (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, after the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected behavior in the authentication phase before security is established. However, the AMF then sent a Deregistration Request message to the UE, marked as "protected" with integrity protection and ciphering (security header type 2), even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must only be applied after security context establishment, which is achieved through successful completion of the 5G-AKA procedure. Since the UE had not yet completed 5G-AKA, it correctly did not respond to the protected Deregistration Request message, as it would not have the necessary security context or keys to process a protected message. If the UE had attempted to process or respond to this message, it would have violated the security procedures outlined by 3GPP. Therefore, the UE's lack of response demonstrates adherence to the standard and is the secure behavior in this context. Secure
286	286	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00036406517028808594 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated the NAS communication by sending an initial registration request to the AMF, which is the expected behavior at the start of 5G standalone procedures. The AMF, under test control, responded with a GMM status message (5GMM Cause: 98, "Message type not compatible with the protocol state") that was marked as protected, even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G standard, security protection (encryption and integrity protection) for NAS messages is only established after successful completion of 5G-AKA, when security context is set up between the UE and the AMF. Since 5G-AKA was not completed, the UE had no security context to decrypt or verify protected messages. The UE's lack of response to the protected GMM status message is correct and secure behavior, as it should not process or respond to protected NAS messages before security activation; doing so could expose it to downgrade or replay attacks. Therefore, the UE's action adheres to the security requirements specified by 3GPP for 5G NAS procedures, ensuring that it does not accept or act on messages that it cannot authenticate. 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, which was under your control for testing, responded with a GMM status message indicating "Illegal UE" (5GMM Cause 3), and this message was sent as "Protected," even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to 3GPP 5G security standards, NAS message protection (encryption and integrity) is only possible after successful completion of 5G-AKA, as this procedure establishes the necessary security context and keys. Since the AMF sent a protected message before 5G-AKA, the UE would not have the keys to decrypt or verify the integrity of the message. The UE did not respond to the protected downlink message, which is the expected and secure behavior according to the standard, as it cannot process protected messages without an established security context. If the UE had attempted to process or respond to the protected message, it would have been a security vulnerability. Thus, the UE's action—providing no response—demonstrates adherence to 3GPP security requirements and is considered secure. 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 registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under tester control, responded with a Security Mode Command that was integrity protected using the 128-5G-IA2 algorithm but employed 5G-EA0 (null) for ciphering, meaning no encryption was applied. Importantly, the 5G-AKA authentication procedure had not yet been completed, so a valid security context was not established. Upon receiving the Security Mode Command, the UE replied with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, the Security Mode Command must be sent after successful authentication and establishment of a security context, and messages should not be protected with a new security context before authentication is complete. The UE correctly detected an invalid situation (attempt to use a new security context before 5G-AKA completion) and responded with a status message indicating the error, rather than proceeding insecurely. This behavior aligns with 3GPP security requirements, as the UE did not accept the insecure context and flagged the protocol violation. Therefore, the UE's action 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 completing the initial NAS procedures but before the completion of 5G-AKA authentication, the UE responded to an initial identity request from the AMF by sending an identity response. Subsequently, the AMF issued another identity request, this time requesting the GUTI, and sent this message in plain (unencrypted) form. The UE did not respond to this second identity request. According to the 3GPP 5G security standard, sensitive information such as the GUTI (Globally Unique Temporary Identifier) should not be transmitted in plain text after the initial identity exchange, and ideally, after the establishment of a security context via successful 5G-AKA authentication. The UE's refusal to respond to an unprotected identity request after the initial exchange aligns with the 3GPP security requirements, as responding could expose sensitive identifiers to potential interception. Therefore, the UE's action demonstrates adherence to the standard by not disclosing the requested identity information in an insecure context prior to the completion of the authentication and security setup. 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 security test, 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, which was sent as a plain (unencrypted) NAS message because the 5G-AKA authentication procedure had not yet been completed. The UE did not respond to this plain Identity Request. According to the 3GPP 5G standard, sensitive information such as the IMEISV must not be sent in plain text over the air interface; it should only be transmitted after NAS security has been established, which occurs after successful completion of 5G-AKA. By refusing to respond to an unprotected Identity Request for the IMEISV, the UE correctly adhered to the security requirements defined by 3GPP, thereby preventing potential exposure of sensitive device information. This demonstrates that the UE's behavior was secure and compliant with the standard. Secure

291	291	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03981208801269531 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04005002975463867 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the initial NAS procedures, the UE sent an Identity Response to the AMF, and then, before 5G-AKA authentication was completed, the AMF sent another 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 subsequent Identity Request. According to the 3GPP 5G standard, sensitive information such as the TMSI (Temporary Mobile Subscriber Identity) should not be transmitted in cleartext after the security context has been established, which only occurs after successful completion of 5G-AKA and the activation of NAS security. Since the 5G-AKA was not yet completed and the AMF sent the Identity Request in plain text, the UE's refusal to respond is consistent with the standard's security requirements, as responding could have exposed sensitive information over an unprotected channel. Therefore, the UE's action of not responding to the plain (unencrypted) Identity Request prior to security activation demonstrates adherence to 3GPP security guidelines and shows secure behavior in this context. 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) [illegible] This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on 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 AMF, indicating that the authentication procedure was ongoing. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is required to establish NAS security (encryption and integrity protection)—the AMF sent a Deregistration Request message to the UE. This message was sent with the security header indicating "integrity protected," but not encrypted, as encryption cannot be enabled until after successful completion of 5G-AKA. Crucially, the UE did not respond to this Deregistration Request. According to the 3GPP 5G standards (e.g., TS 24.501), the UE is required to ignore NAS messages that are "integrity protected" but received before security context is established (i.e., before 5G-AKA is complete), since the UE cannot verify their authenticity or integrity without the necessary keys. By not responding, the UE demonstrated correct and secure behavior, as responding could have exposed it to security risks such as replay or spoofing attacks. Therefore, the UE's action in this scenario aligns with the security requirements of 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 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the NAS security context should now be active for subsequent NAS messages. The AMF, under test control, then sent a "Configuration Update Command" to the UE as a plain (unencrypted and unauthenticated) NAS message, as indicated by the Security Header Type set to 0 (Plain NAS message). According to 3GPP standards (TS 24.501), after the completion of 5G-AKA and establishment of the NAS security context, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted. When the UE receives a plain NAS message after security activation, it should consider this a protocol error and must not process the message or respond to it, as processing plain messages in this context could open up significant security vulnerabilities (e.g., replay or injection attacks). In this test, the UE did not respond to the plain "Configuration Update Command" message, which is the correct and secure behavior as per 3GPP requirements, since processing or responding to such a message would be a security risk. 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 successfully completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the security parameters and was ready to begin protected communication. However, the AMF subsequently sent an "authentication request" message to the UE in plain (unencrypted) form, which is not the expected sequence according to the 3GPP 5G standard. Once the security mode is complete, all subsequent NAS messages between the UE and AMF should be integrity protected and, if negotiated, encrypted. The UE did not respond to this unprotected authentication request, which aligns with 3GPP security requirements: the UE should ignore or drop any plain NAS messages received after security activation, as processing such messages could expose it to downgrade or replay attacks. By refusing to respond to an unprotected message after security was established, the UE demonstrated correct and secure behavior as specified by the standard. Secure

295	295	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.16016411781311035 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16040301322937012 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that both sides had agreed on the security context and that subsequent NAS messages should be protected (integrity protected and, if configured, ciphered) according to the 3GPP 5G security standards. However, the AMF then sent a "service reject" message with 5GMM Cause 111 ("protocol error, unspecified") in plain (unencrypted and unprotected) form. According to the 3GPP TS 24.501 specification, after security mode is completed, the UE should only accept NAS messages that are integrity protected and, where applicable, ciphered. Since the "service reject" message from the AMF was sent in plain text after security context establishment, the UE correctly did not respond to this unprotected message, thereby preventing a potential security breach (such as a downgrade or spoofing attack). This behavior is in line with 3GPP security requirements, which mandate that the UE must ignore unprotected NAS messages once security is activated. Therefore, the UE's actions were secure and compliant with the 5G standard. 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 successfully completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had agreed to the selected NAS security algorithms and was ready to establish a protected NAS security context. However, the AMF then sent an "authentication request" message to the UE in plain (unencrypted) form, which is not compliant with the 3GPP 5G standards. According to 3GPP TS 24.501, once the NAS security mode is completed and a security context is established, all subsequent NAS messages must be integrity protected and, if required, encrypted. The UE did not respond to the plain "authentication request" message sent by the AMF after security mode completion. This behavior is consistent with the 3GPP specifications, as the UE should reject or ignore any unprotected NAS messages after a security context has been established to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to the unprotected authentication request was secure and compliant with the standard. 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 successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should be active for subsequent NAS messages. However, the AMF responded with a "deregistration accept" message that was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once NAS security has been activated (after security mode complete), the UE should only accept NAS messages that are integrity protected and, where required, encrypted. If the UE receives a plain NAS message after security activation, it should discard the message and not process or respond to it. In this test, the UE did not respond to the unprotected "deregistration accept" message, which indicates that it correctly followed the 3GPP security requirements by refusing to process a plain message after security activation. This behavior prevents potential security vulnerabilities, such as replay or forgery attacks, that could arise from accepting unprotected messages after NAS security is established. 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 completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should be active for subsequent messages. However, the AMF then sent an "authentication reject" message to the UE in plain (unencrypted) form. The UE, upon receiving this unauthenticated and unprotected message after security activation, did not respond. According to 3GPP standards (TS 24.501), once NAS security is activated, the UE must only accept NAS messages that are integrity protected (and, if required, encrypted); any plain messages received after security activation should be ignored or discarded by the UE. The UE's lack of response to the plain "authentication reject" message demonstrates compliance with the 3GPP security requirements, as it did not process or act upon an insecure message that could be spoofed or tampered with. This behavior protects against potential security threats such as replay or man-in-the-middle attacks. Therefore, the UE's action was secure and in line with 3GPP standards. 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 transmitted a Security Mode Complete message to the AMF, indicating that it had accepted the negotiated NAS security algorithms and was ready for secure communication. Subsequently, the AMF sent an Authentication Reject message to the UE; notably, this message was transmitted in plain (unencrypted) NAS format, despite the fact that security context establishment (via Security Mode Complete) had already occurred. According to the 3GPP 5G standard, specifically TS 24.501 and TS 33.501, after the Security Mode Complete message, all subsequent NAS signaling messages—except for a few exceptions such as Service Reject and Deregistration Accept—must be integrity protected and, where applicable, ciphered. The Authentication Reject message is not one of these exceptions and, therefore, must be sent with NAS security protection once the security context is active. The UE, upon receiving a plain (unprotected) Authentication Reject after security activation, did not respond, effectively ignoring the message. This behavior aligns with 3GPP security recommendations, which specify that the UE should discard any unprotected NAS messages that are required to be protected after security mode is complete, in order to prevent downgrade or spoofing attacks. Therefore, the UE's action in this scenario was secure and in compliance with the 5G standard. 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 completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that both sides had agreed on the security context and that NAS security (encryption and integrity protection) should be active for all subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE requesting the TMSI, but this message was sent in plain (unencrypted) NAS, rather than as a protected message. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), after the security mode procedure is completed, all subsequent NAS messages must be integrity protected and, where applicable, encrypted. When the UE receives a plain (unprotected) NAS message after the security context is established, it is required by the standard to discard the message and not respond, to prevent downgrade or replay attacks. In this test, the UE did not respond to the unprotected identity request, which indicates that it correctly followed the 3GPP security requirements and did not expose its identity in an insecure manner. Therefore, the UE's action was secure and compliant with the 5G standard. Secure