UE Response Evaluation Report: Test time: 2025-07-17 11:08:46

SL	Test Name	Test content	Remark
1	1	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006918907165527344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated registration with the AMF by sending an InitialUEMessage containing a registration request. In response, the AMF (under test control) sent an Identity Request message, specifically requesting the IMEI, and this message was sent in plain (unencrypted) form since the 5G-AKA authentication procedure had not yet been completed. The UE did not respond to this identity request. According to the 3GPP 5G standard (TS 24.501), before the security context is established through 5G-AKA, identity requests from the network are sent in plain text, and the UE is expected to respond with the requested identity (such as IMEI) even if the message is not encrypted. However, from a security perspective, the standard also recognizes that revealing the IMEI in plain text exposes the device to potential privacy risks, such as device tracking or fingerprinting. Some UEs may therefore implement additional privacy protections by refusing to send the IMEI in plain text before security activation, even if this is stricter than the baseline standard. In this test, the UE chose not to respond to the plain-text IMEI request, thereby prioritizing device privacy over strict standard compliance. This action enhances the security and privacy of the UE by preventing the exposure of a persistent device identifier over an unprotected channel. Therefore, the UE's action can be considered secure as it avoids unnecessary disclosure of sensitive information before a secure context is established. Secure
2	2	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0011980533599853516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2027890682220459 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an initial registration request to the AMF. The AMF, under test control, responded with an identity request, specifically requesting the Subscription Concealed Identifier (SUCI) from the UE. Notably, this identity request was 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 sending an identity response containing the requested SUCI. According to the 3GPP 5G security standard (TS 33.501), before the completion of 5G-AKA, the NAS messages between the UE and the AMF are not yet protected with encryption or integrity algorithms. However, the standard mandates that the UE should never send the permanent subscriber identifier (SUPI) in the clear; instead, it must send the SUCI, which is a concealed (encrypted) version of the SUPI, designed specifically for this pre-authentication phase to protect user privacy. In this test, the UE complied by providing the SUCI, not the SUPI, in response to the plain identity request. Therefore, based on the 3GPP standard, the UE's actions were secure and in line with expected behavior, as it did not expose sensitive permanent identity information before establishing a secure channel. 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 registration procedure by sending an initial Registration Request message to the AMF, which is expected behavior when joining a 5G network. However, instead of proceeding with the 5G-AKA authentication procedure, the AMF immediately responded with an Authentication Reject message, which was sent in plain (unencrypted) NAS, as the security context had not yet been established. According to the 3GPP 5G standard, until the authentication and key agreement (5G-AKA) is completed, messages between the UE and AMF are not protected by NAS security (i.e., they are sent in plain). The UE, upon receiving an Authentication Reject before security activation, is expected to silently discard the message and not respond, as per 3GPP TS 24.501, section 5.4.2.7.2. In this test, the UE did not respond to the plain Authentication Reject, which aligns with the standard's security requirements and mitigates the risk of reacting to potentially spoofed or malicious messages before a secure context is established. Therefore, the UE's action in this scenario was secure. Secure
4	4	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0012979507446289062 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20431208610534668 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated registration with the AMF by sending an InitialUEMessage containing a Registration Request. In response, the AMF sent an Identity Request message requesting the SUCI (Subscription Concealed Identifier) from the UE. Notably, this Identity Request was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed; thus, no NAS security context was established at this stage. The UE then responded with an Identity Response message containing the requested SUCI. According to the 3GPP 5G standard (TS 24.501), the initial NAS messages exchanged before the completion of 5G-AKA (including registration and identity procedures) are permitted to be sent in plain text because encryption and integrity protection are only activated after a security context is established. The use of SUCI, which is a privacy-preserving, encrypted version of the permanent subscriber identity (SUPI), ensures that the user's permanent identity is not exposed even though the messages are unprotected at this stage. Therefore, the UE's actions were compliant with 3GPP security standards, as it did not reveal sensitive information and followed the expected protocol flow. Secure

5	5	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006351470947265625 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Protocol error, unspecified) 0.20275402069091797 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a plain (unencrypted) registration reject message with 5GMM cause 111 (protocol error, unspecified), before the 5G-AKA authentication and key agreement procedure had been completed. After receiving this registration reject, the UE responded by sending a deregistration request (UE originating) to the AMF. According to the 3GPP 5G standards, NAS messages are permitted to be sent in plain text prior to the completion of the 5G-AKA procedure, as security context has not yet been established. The UE's behavior—sending a deregistration request upon receiving a plain registration reject before authentication and key establishment—is consistent with the expected 3GPP standard behavior. The UE did not proceed with any sensitive operations or accept network services without security, and its response to an early registration reject was appropriate, as the security context was not yet set up. Therefore, the UE's actions did not introduce any security vulnerabilities or deviate from the 5G standard procedures in this context. 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 security test, the UE initiated a registration procedure by sending an InitialUEMessage containing a Registration Request to the AMF. However, before the 5G-AKA authentication and key agreement procedure was completed, the AMF responded with a Registration Reject message (5GMM Cause: 22, indicating congestion) sent in plain (unencrypted) form. Following this, the UE responded with a Deregistration Request (UE originating). According to the 3GPP 5G standards, specifically TS 24.501, it is expected that Registration Reject messages sent before the completion of 5G-AKA (i.e., before security context establishment) are transmitted in plain text, as there is no established security context for encryption or integrity protection at this stage. Furthermore, the UE is required to accept and process such plain Registration Reject messages, and it is permitted to respond with a Deregistration Request in plain text as well. Since the UE followed the expected behavior by accepting the unprotected Registration Reject message and responding appropriately, and did not attempt to establish a security context before authentication, the UE's actions are in line with the security procedures outlined by the 3GPP standard. Therefore, the UE's actions in this scenario were secure. Secure

7	7	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 00000000000000000000000000000000 AUTN: 32303030007f0000ee555cc720560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.203125 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, which was under test control, responded with an authentication request message that was sent in plain (unencrypted) form and included non-standard or suspicious parameters such as an all-zero RAND value and ABBA field, as well as an AUTN value that does not conform to typical 5G authentication vectors. The UE, upon receiving this authentication request, did not proceed with 5G-AKA authentication. Instead, it responded with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it detected the authentication challenge as invalid or insecure according to 3GPP 5G security standards. According to the 3GPP specifications, the UE must only accept valid and secure authentication requests and should reject any authentication attempt that appears to be non-compliant or potentially malicious, especially when no security context has been established and the messages are unprotected. The UE’s behavior demonstrates adherence to the security requirements by refusing to engage in authentication under suspicious or insecure conditions, thus protecting itself from potential attacks or misconfigurations. Therefore, based on the 3GPP 5G standard, the action taken by the UE was secure. Secure

8	8	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 313030300000000078742b94d4550000 AUTN: 0000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005857944488525391 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20240378379821777 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) initiated a registration procedure by sending an initial registration request to the Access and Mobility Management Function (AMF). In response, the AMF sent an authentication request message to the UE. Notably, this authentication request from the AMF was sent in plain (unencrypted) form, and the critical authentication parameter AUTN was set to all zeros, which is invalid as per 3GPP standards. The UE, upon receiving this malformed and unprotected authentication request, did not proceed with the authentication procedure (5G-AKA was not completed) and instead responded with a 5GMM status message indicating "Invalid mandatory information." This response from the UE is in line with 3GPP security requirements: the UE is expected to validate the integrity and correctness of received NAS messages, especially before the establishment of a security context, and should not proceed with authentication if the received parameters are invalid or missing. By refusing to process the invalid authentication request and notifying the AMF with a status message, the UE avoided potential security risks such as replay or downgrade attacks. Therefore, the UE's actions adhered to the security guidelines outlined in the 3GPP specifications and did not compromise its security posture during the interaction. Secure

9	9	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after the initial NAS procedures, 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 SUCI (Subscription Concealed Identifier), and the UE again provided an identity response. Importantly, this exchange occurred before the completion of the 5G-AKA authentication procedure, meaning that NAS security (encryption and integrity protection) had not yet been established. According to 3GPP standards, before 5G-AKA is completed, only protected (concealed) identifiers such as SUCI should be sent by the UE, and never the cleartext SUPI (Subscription Permanent Identifier). The SUCI is specifically designed to protect the subscriber's identity even when sent in the clear, prior to NAS security activation. Based on the information provided, the UE responded to the AMF's request for the SUCI, and there is no indication that it exposed the SUPI or any unprotected identifier. Therefore, the UE's action aligns with 3GPP security requirements for this stage of the NAS procedure. The UE's behavior was secure, as it only provided the SUCI before NAS security was established, thereby protecting the subscriber's permanent identity as intended by the standard. Secure

10	10	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3100 RAND: 313131313131313131006f90d2550000 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 0.039749860763549805 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399777889251709 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2409358024597168 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and the AMF engaged in a standard NAS procedure where, after the UE sent an identity response, the AMF issued an authentication request. Notably, the authentication request was sent in plain (unencrypted) form, as the 5G-AKA (Authentication and Key Agreement) procedure had not yet completed, which is expected since encryption and integrity protection of NAS messages are only mandated after successful authentication. Upon receiving the authentication request, the UE responded with an "Authentication failure (ngKSI already in use)" message, indicating that it detected the ngKSI (NAS key set identifier) provided by the AMF was already in use and therefore refused to proceed with authentication under potentially insecure or replayed parameters. According to the 3GPP 5G standards (notably TS 24.501 and TS 33.501), the UE is expected to check for reuse or replay of ngKSI values to prevent certain attacks, and should reject authentication attempts using an ngKSI that is already in use. By refusing to proceed and explicitly notifying the AMF of the issue, the UE correctly adhered to the security guidelines, ensuring that authentication was not performed under potentially compromised circumstances. Therefore, the UE's actions were in line with 3GPP security requirements and demonstrated a secure response to the situation. 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 standalone User Equipment (UE) participated in NAS communication with the Access and Mobility Management Function (AMF). After completing initial NAS procedures, the UE sent an Identity Response message to the AMF in plaintext, as the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed. The AMF, under test control, then sent a Service Reject message with cause "PLMN not allowed" (5GMM Cause 11), also in plaintext. The UE, upon receiving this Service Reject message, did not respond further. According to the 3GPP 5G standard, messages exchanged before the completion of 5G-AKA (and thus before the establishment of NAS security context) are not encrypted and are expected to be sent in plaintext. The UE's behavior—sending an Identity Response before security activation and ceasing communication after receiving a Service Reject—aligns with standard-compliant procedures, as it did not proceed to send any sensitive information or NAS messages that require encryption before security was established. Therefore, based on the 3GPP standard and the actions observed, the UE acted securely in this test scenario. 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 security test of a 5G standalone User Equipment (UE), the UE first sent an identity response to the AMF, after which the AMF (under test control) sent another identity request, specifically requesting the SUCI (Subscription Concealed Identifier). The AMF's identity request message was sent in plain (unencrypted) form, which is standard behavior before the completion of the 5G-AKA authentication procedure, as encryption and integrity protection of NAS messages are only enabled after successful authentication and key establishment. The UE, upon receiving the identity request, again responded with an identity response, presumably providing the SUCI as requested. According to 3GPP standards (TS 33.501 and TS 24.501), before the completion of 5G-AKA, identity procedures (including the transmission of SUCI) are performed in plain text, as there are not yet established NAS security keys. The SUCI itself is designed to protect the subscriber's permanent identifier (SUPI) by encrypting it with the home network's public key, specifically to prevent exposure of sensitive information even when sent in the clear. Therefore, the UE's action of providing the SUCI in response to an unprotected identity request, prior to security activation, is in line with 3GPP security requirements and does not expose the subscriber's permanent identity. Thus, the UE's behavior in this scenario is considered secure. Secure
13	13	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.03993391990661621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04019308090209961 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected behavior when the network requests the UE's identity. Following this, the AMF sent an Authentication Reject message in plain (unencrypted) NAS signaling, which is permitted by the 3GPP 5G standard before the completion of the 5G-AKA authentication procedure, as ciphering and integrity protection are not yet established at this stage. The UE, upon receiving the Authentication Reject message, did not respond further, which aligns with the expected behavior defined in 3GPP TS 24.501: upon receiving an Authentication Reject before security is activated, the UE should not proceed with further NAS communication and should treat the attach/registration as failed. This behavior prevents the UE from revealing any sensitive information or progressing with procedures before mutual authentication and security activation. Therefore, the UE's actions were secure and compliant with 3GPP standards, as it did not respond to the unauthenticated network after receiving the reject message in plain text. 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 and responded to an identity request from the AMF by sending an identity response. Immediately after, the AMF sent a registration reject message with cause 22 (indicating congestion), and this message was sent in plain (unencrypted) NAS. Since 5G-AKA (Authentication and Key Agreement) had not yet been completed, mutual authentication and the establishment of NAS security (ciphering and integrity protection) were not in place. According to 3GPP standards, until 5G-AKA is complete, all NAS messages—including registration reject—are permitted to be sent in plain text, as security context has not yet been established. The UE's behavior of not responding further after receiving the registration reject is correct, as per 3GPP specifications, and no sensitive information was transmitted after the identity response. The UE did not perform any insecure actions; it followed the expected protocol flow for an unprotected NAS session prior to authentication. Therefore, based on the described interaction and adherence to the 3GPP standard, the UE's actions were secure in this context. Secure
15	15	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 30303030303030007844783aae550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.03972196578979492 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24048709869384766 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response, the AMF replied with an authentication request that was not properly constructed for 5G-AKA: the AUTN (Authentication Token) field was all zeros, and the message was sent in the clear (plain NAS), prior to the completion of the 5G-AKA procedure. The UE, upon receiving this authentication request, responded with "Authentication failure (Non-5G authentication unacceptable)," indicating that it rejected the authentication method as not conforming to 5G security requirements. According to 3GPP standards, a UE must not proceed with authentication or accept security contexts unless the authentication request is valid, properly formatted, and uses the correct cryptographic parameters. The UE's rejection of an invalid or insecure authentication request protects it from potential downgrade or spoofing attacks, demonstrating correct adherence to the 5G security model. Therefore, the UE's action was appropriate and aligned with 3GPP security standards, as it refused to engage in an authentication procedure that did not meet the expected security criteria. 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 5G standalone security test, the UE and AMF completed the 5G-AKA authentication procedure, after which the UE sent an authentication response to the AMF. The AMF then sent a Security Mode Command to the UE, but this command was transmitted as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value "Plain NAS message (0)". The UE did not respond to this plain Security Mode Command. According to the 3GPP 5G standard (TS 24.501), after the successful completion of 5G-AKA, the Security Mode Command is permitted to be sent as a plain NAS message, since NAS security context has not yet been established at this point. However, once the Security Mode Command is received, the UE is expected to respond with a Security Mode Complete message, which should be protected using the agreed NAS security algorithms. In this test, the UE did not respond at all to the plain Security Mode Command. This action is not compliant with the 3GPP standard, as the UE is expected to proceed with the NAS security setup by responding to the Security Mode Command. While ignoring unprotected messages after security context establishment is correct, in this case, the Security Mode Command is the trigger for starting NAS security and is allowed to be sent in the clear. Therefore, the UE's lack of response is not secure, as it prevents the establishment of NAS security and does not follow the standard procedure. Insecure
17	17	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.35177087783813477 UE to AMF UplinkNASTransport, Authentication response 0.35199785232543945 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an authentication response to the AMF as part of the 5G-AKA authentication process. However, before the authentication and key agreement (5G-AKA) was completed, the AMF sent a Service Reject message with cause 111 ("Protocol error, unspecified") in plain (unencrypted) NAS, and the UE did not respond to this message. According to the 3GPP 5G security standards, NAS messages exchanged before the successful completion of 5G-AKA are permitted to be sent in plain text, as security contexts and encryption keys have not yet been established. The UE's lack of response to the plain Service Reject message is consistent with expected behavior, as it is not required to respond to a Service Reject and should not process further requests until a valid security context is established. Therefore, the UE's actions in this scenario align with the 3GPP security specifications and do not expose it to undue risk or protocol violation at this stage of communication. Secure

18	18	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 4.243709087371826 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 4.243997097015381 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Identity request 4.445895195007324 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF), the UE first completed the initial NAS steps and sent an authentication response to the AMF, indicating that the authentication phase of 5G-AKA was in progress but not yet completed. Following this, the AMF sent an identity request for the Subscription Concealed Identifier (SUCI) to the UE, and this message was sent in plain (unencrypted) form. The UE responded with an identity response containing the requested SUCI. According to the 3GPP 5G security standard, specifically TS 33.501, NAS message encryption and integrity protection are only activated after the successful completion of the 5G-AKA authentication and key agreement procedure. Before this, NAS messages, including identity requests and responses, are sent in plain text. However, the standard also mandates that the UE should never send its Subscription Permanent Identifier (SUPI) in clear text; instead, it must send a SUCI, which is a privacy-preserving, encrypted, and concealed version of the SUPI designed for use over unprotected channels. In this test, the UE correctly provided the SUCI in response to a plain identity request prior to the establishment of a secure NAS connection, which aligns with the security requirements of the 5G standard. Therefore, based on the actions taken by the UE—providing only the SUCI and not the SUPI in plain text—the UE's behavior was secure and compliant with 3GPP specifications. Secure
19	19	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11986708641052246 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12012410163879395 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3239710330963135 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command to the UE, specifying the use of the 5G-EA0 (null) cipher algorithm (meaning no encryption) and the 128-5G-IA2 integrity algorithm, with the security header indicating "integrity protected with new security context." Upon receiving this command, the UE responded with a Security Mode Reject message, citing "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G security standards (notably TS 33.501 and TS 24.501), after successful authentication, the UE is expected to negotiate ciphering and integrity algorithms with the AMF. The use of 5G-EA0 (null ciphering) is only permitted in very specific scenarios, such as emergency calls or when ciphering is explicitly not required; otherwise, the UE should reject the use of null ciphering to prevent unprotected transmission of user data and NAS messages. In this case, the UE rejected the Security Mode Command that would have resulted in unencrypted communication, thereby adhering to the security requirements mandated by the 3GPP standard. This action demonstrates that the UE is correctly enforcing security policies by refusing to accept insecure ciphering configurations. Therefore, the UE's behavior in this scenario was secure. Secure

20	20	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 2f4b62abf69d8352398c608fb3a89563 AUTN: 062d8ab6b7549000811f4ee8b8da8440 ngKSI_TSC: Native security context ngKSI_KSI: 6 UE provided: Authentication response The packet capture during the test using wireshark is: 1.9198977947235107 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Authentication response 1.9201328754425049 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.120612859725952 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and the AMF are engaged in the NAS authentication procedure as part of the 5G-AKA process. The UE first sends an authentication response to the AMF, after which the AMF (under your control) sends a subsequent authentication request back to the UE. Notably, this authentication request from the AMF is sent as a plain (unencrypted) message, and the 5G-AKA procedure has not yet been completed, meaning that NAS security context has not been established. According to 3GPP standards (TS 24.501, TS 33.501), NAS messages prior to the completion of authentication and security mode command are allowed to be sent in plain text, as security context is not yet available. The UE, upon receiving a new authentication request (still before security activation), responds again with an authentication response. This behavior is compliant with the 3GPP specification, as the UE is expected to process authentication requests and send responses in plain text until NAS security context is established. Therefore, the actions taken by the UE in this scenario are secure and in line with the 5G standard, as it did not send any protected messages before security activation nor did it skip any required authentication steps. Secure

21	21	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 303030303030300078d431f251560000 AUTN: 4953cc15a85a90008f0a1f4e8f0a3310 ngKSI_TSC: Native security context ngKSI_KSI: 4 UE provided: Authentication failure (MAC failure) The packet capture during the test using wireshark is: 1.8795151710510254 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, Authentication response 1.8797390460968018 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.0836050510406494 UE to AMF UplinkNASTransport, Authentication failure (MAC failure) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, the UE and AMF engaged in a 5G-AKA authentication sequence, with the UE first sending an authentication response to the AMF. Subsequently, the AMF issued another authentication request, which was sent in plain (unencrypted) form before the 5G-AKA procedure had been completed. The UE, upon receiving this authentication request, responded with an "Authentication failure (MAC failure)" message. According to the 3GPP 5G security standard, the UE is required to check the integrity of authentication requests using the Message Authentication Code (MAC) and must reject any authentication request that fails this check or is not properly protected, especially if received before a security context is established. In this scenario, the UE correctly identified the MAC failure and refused to proceed, thus preventing any potential security breach that could arise from accepting unauthenticated or tampered messages. This behavior aligns with 3GPP's security requirements, as the UE must not accept plain or invalid authentication requests prior to the completion of the 5G-AKA process and establishment of a secure context. Therefore, the UE's action was secure and in compliance with the 5G standard. Secure

22	22	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3200 RAND: 303030303030300078b457a1d8550000 AUTN: 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 the described security test, after completing the initial NAS procedures, the UE sent an Authentication Response to the AMF, expecting the next step in the 5G-AKA authentication sequence. However, instead of proceeding as per the standard, the AMF sent another Authentication Request to the UE, and notably, this message was sent as a plain (unencrypted) NAS message. Upon receiving this, the UE replied with an Authentication Failure message, specifically indicating "Non-5G authentication unacceptable." According to the 3GPP 5G security standards, the NAS messages that carry sensitive information must be protected, and the authentication process must follow the defined 5G-AKA flow. The UE is required to reject any authentication attempts that do not conform to the 5G authentication procedures or are delivered in an insecure manner. By refusing to proceed with a plain-text authentication request and responding with an explicit failure cause, the UE demonstrated correct and secure behavior as per the standard, protecting itself from potential downgrade or replay attacks. Therefore, the UE's action was secure. Secure

23	23	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11994004249572754 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12018203735351562 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.32151198387145996 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G Authentication and Key Agreement (5G-AKA) procedure, the User Equipment (UE) responded to the Authentication Request with an Authentication Response, as expected. The Access and Mobility Management Function (AMF) then sent a Security Mode Command to the UE, which was protected with integrity using the new security context established during 5G-AKA. However, the Security Mode Command specified the use of the null ciphering algorithm (5G-EA0), meaning that no encryption would be applied to the subsequent NAS messages, while integrity protection was set to 128-5G-IA2. Upon receiving this command, the UE rejected it by sending a Security Mode Reject message with the cause "security mode rejected, unspecified." According to the 3GPP 5G security standards, UEs are required to reject security mode commands that attempt to establish a null ciphering algorithm (5G-EA0) unless explicitly allowed by local policy, as transmitting unencrypted NAS messages exposes the communication to eavesdropping and other attacks. The UE's rejection of the Security Mode Command under these circumstances demonstrates compliance with the 3GPP security requirements and shows that it does not allow unprotected communication unless specifically permitted. This behavior is secure, as it prevents the establishment of insecure communication channels and protects user data and signaling integrity. 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 the described test scenario, the UE initially completed the expected NAS steps and sent an authentication response to the AMF. However, the AMF, instead of proceeding with the next step of the 5G-AKA authentication protocol (such as sending a Security Mode Command to establish ciphering and integrity protection), sent another authentication request back to the UE in plain (unencrypted) form. The UE responded to this subsequent authentication request with another authentication response, also in plain text, as observed in the packet capture. According to the 3GPP 5G standard, after the successful completion of the authentication and key agreement (5G-AKA), all subsequent NAS messages between the UE and the AMF should be protected with integrity and, where applicable, ciphered to ensure confidentiality and security. The fact that the UE responded to a repeated, unprotected authentication request after already completing authentication, and did so in plain text, indicates a deviation from the expected secure behavior. Ideally, the UE should have rejected or ignored the redundant authentication request, especially since it was not protected and the authentication process was not properly progressing. This behavior could potentially expose the UE to replay or downgrade attacks, as it is willing to process and respond to repeated, unprotected authentication requests. Therefore, the UE's actions do not align with the security requirements outlined by 3GPP for 5G NAS communication after authentication. 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, after the initial NAS procedures, the UE sent an Authentication Response to the AMF, indicating its willingness to proceed with mutual authentication as part of the 5G-AKA procedure. However, instead of continuing the authentication process, the AMF immediately responded with an Authentication Reject message, which was sent in plain (unencrypted) NAS as 5G-AKA had not yet been completed and security context was not established. Upon receiving this Authentication Reject, the UE did not attempt to proceed with further NAS procedures or retry authentication; instead, it sent a Deregistration Request to the AMF, signaling its intention to detach from the network. According to the 3GPP 5G standards, if the UE receives an Authentication Reject before security activation, it is required to abort the ongoing registration or authentication attempt and should not respond to any further NAS messages except for a deregistration or re-registration. The UE's behavior aligns with these requirements, as it did not respond inappropriately to the plain (unencrypted) Authentication Reject and initiated a deregistration process, thus preventing potential exploitation of unprotected signaling. This approach ensures that the UE does not expose itself to further security risks when authentication fails and before a secure context is established. 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, the 5G standalone User Equipment (UE) first completed the 5G-AKA authentication and key agreement procedure, establishing a secure context for subsequent NAS messaging. After this, the UE sent a Security Mode Complete message, which indicates that it accepted the security algorithms and is ready to use the negotiated ciphering and integrity protection for NAS messages. The Access and Mobility Management Function (AMF), under test control, then sent a Deregistration Request message to the UE. Importantly, this message was protected with both integrity protection and ciphering, as indicated by the NAS security header type (2), meaning it was encrypted and authenticated. The UE responded with a Deregistration Accept message, also protected by the established security context. According to the 3GPP 5G standards (TS 24.501), after the security mode procedure, all subsequent NAS messages between the UE and the AMF must be integrity protected and, when required, ciphered. The UE's actions—accepting the security mode, responding only to protected messages, and sending a protected Deregistration Accept—demonstrate correct implementation of the 5G security requirements. There is no evidence of the UE accepting or responding to unprotected messages after security context establishment, nor any deviation from the standard protocol. Thus, the UE's behavior in this scenario aligns with 3GPP security expectations. 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 completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (integrity protection and ciphering) had been successfully established. The AMF, under test control, then sent a "deregistration request" message to the UE, which was protected with both integrity and ciphering (as indicated by the security header type 2). The UE responded with a "deregistration accept" message, signaling that it acknowledged and accepted the deregistration request. All subsequent NAS messages following the security mode complete were exchanged with NAS security enabled, as required by the 3GPP 5G standard (TS 24.501), which mandates that sensitive NAS signaling, such as deregistration procedures, must be protected after security context establishment. There is no indication that the UE accepted or acted upon any unprotected NAS messages after security establishment, nor did it prematurely send sensitive information before security activation. Therefore, the actions taken by the UE are in compliance with the 5G security requirements, and the communication can be considered secure. Secure

28	28	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16000795364379883 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602778434753418 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36232805252075195 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Security Mode Complete" message to the AMF, indicating that it accepted the negotiated security parameters and was ready to proceed with protected NAS signaling. However, the AMF subsequently sent another "Security Mode Command" message, this time protected with the newly established security context (as indicated by the security header), specifying ciphering with 128-5G-EA2 and null integrity protection (5G-IA0). Upon receiving this, the UE responded with a "Security Mode Reject" message, refusing the new security mode for an unspecified reason. According to the 3GPP 5G standard, it is critical that both integrity and confidentiality protections are enabled after authentication, as integrity protection ensures that messages have not been tampered with. The AMF's attempt to set the integrity algorithm to null (5G-IA0) after authentication and security context establishment is a significant security risk, as it exposes the connection to potential attacks. The UE, by rejecting the security mode that did not include integrity protection, acted in accordance with best security practices and the 3GPP standard, which expects the UE to reject insecure configurations. Therefore, the UE's action was secure, as it correctly refused to operate without integrity protection, thereby maintaining the security of the NAS signaling. 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.	During the test, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms and that the NAS security context was established. However, the AMF then sent another "security mode command" message to the UE, this time protected using the null cipher (5G-EA0) and null integrity (5G-IA0) algorithms, and marked the security header as "Integrity protected with new security context." Upon receiving this, the UE responded with a "security mode reject" message, specifying "security mode rejected, unspecified." According to the 3GPP 5G standard, after the 5G-AKA procedure, all subsequent NAS messages must be protected using the agreed-upon security algorithms, and the use of null algorithms (EA0/IA0) is only allowed under specific, tightly controlled circumstances, typically during initial registration or emergency services. If the network attempts to downgrade security or requests the use of null algorithms when a security context is already established, the UE is expected to reject such requests to prevent potential security breaches or downgrade attacks. Therefore, the UE's action to reject the security mode command that attempted to use null algorithms after security context establishment was correct and in line with 3GPP security requirements, ensuring the integrity and confidentiality of the communication. Secure

30	30	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the proposed security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity). However, the AMF, under test control, responded with a new "security mode command" instead of proceeding to the next expected NAS step. According to 3GPP standards, after the UE sends a "security mode complete," the AMF should not send another "security mode command" unless a new security context is required, such as after a handover or if the previous procedure failed. The UE, upon receiving this unexpected second "security mode command," should have rejected it or at least not responded with another "security mode complete" unless it had clear justification per the protocol. The packet capture shows that the UE sent another "security mode complete" in response, which is not compliant with the expected sequence in the 5G NAS security procedures. This behavior could potentially be exploited by an attacker to trigger repeated security re-negotiations, leading to downgrade or replay attacks. Therefore, the UE's action in this scenario is considered insecure as it did not properly enforce the 3GPP-defined security procedure flow and allowed an unexpected and potentially malicious security mode command to proceed. 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 User Equipment (UE) first completed the 5G-AKA authentication and then sent a Security Mode Complete message to the Access and Mobility Management Function (AMF), indicating that it had accepted the security parameters (ciphering and integrity algorithms) negotiated during the Security Mode Command procedure. However, after this, the AMF sent another Security Mode Command, which was protected (i.e., encrypted and/or integrity protected) according to the security context established. The UE, instead of responding with a Security Mode Complete or rejecting the unexpected command, immediately sent a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G standard, once the security context is established (after 5G-AKA and the first Security Mode Complete), all subsequent NAS messages must be protected using the agreed ciphering and integrity algorithms. In this case, the ciphering algorithm was 5G-EA4, but the integrity algorithm was 5G-IA0 (null), which means no integrity protection was applied. The UE's action to deregister upon receiving a second, unexpected Security Mode Command can be interpreted as a defensive measure to avoid potential security risks, such as a replay or downgrade attack. However, the use of the null integrity algorithm (5G-IA0) is not recommended in commercial deployments, as it leaves NAS messages vulnerable to tampering. While the UE did not process the suspicious command and instead deregistered, its use of null integrity protection for NAS signaling is not compliant with best security practices outlined by 3GPP, which recommends integrity protection for all NAS signaling. Therefore, while the UE's decision to deregister may have prevented a security breach, the lack of integrity protection renders its communication insecure under the 3GPP standard. Insecure

32	32	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.1595141887664795 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15984320640563965 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G Authentication and Key Agreement (5G-AKA) procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS signaling. Subsequently, the AMF sent another "security mode command" message to the UE, which was protected (integrity protected and ciphered) using the agreed algorithms (5G-EA4 for ciphering and 128-5G-IA3 for integrity). According to the 3GPP 5G standards, once the security mode complete message has been sent and security is activated, the UE should only accept NAS messages that are integrity protected (and ciphered, if applicable), and it should not expect to receive another security mode command unless there is a valid reason, such as a security context re-establishment. The fact that the UE did not respond to the unexpected, subsequent security mode command indicates that it correctly ignored an out-of-sequence or possibly malicious message, adhering to the 3GPP security requirements to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to the second security mode command after security activation demonstrates secure behavior in accordance with the 5G standard. 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 reques 0.1606900691986084 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Illegal ME) 0.36391305923461914 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (ciphering and integrity protection) was now active for subsequent messages. The AMF then sent a protected "gmm status" message with a 5GMM cause value of 6, which corresponds to "Illegal ME" (Mobile Equipment). Upon receiving this, the UE responded by sending a "Deregistration request (UE originating)" message to the AMF. According to the 3GPP 5G standards, once NAS security is established, the UE should only process protected NAS messages and should react appropriately to status messages that indicate critical errors, such as "Illegal ME." The UE's action to deregister itself upon receiving an "Illegal ME" status is compliant with the standard, as this cause indicates that the network has determined the UE is not allowed to access the network, and the correct behavior is for the UE to initiate deregistration. All communications after the 5G-AKA procedure were protected, and the UE did not process any unprotected NAS messages. Therefore, the UE's response was both secure and compliant with the 3GPP 5G standard. Secure

34	34	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15963101387023926 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15987801551818848 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (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 5G-AKA authentication, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security procedures (integrity protection and ciphering) had been established. Subsequently, the AMF sent a Deregistration Request (UE terminated), which was integrity protected and ciphered as indicated by the security header. The UE responded with a Deregistration Accept message, completing the deregistration procedure. According to the 3GPP 5G standards, once the 5G-AKA and security mode command procedures are completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, when applicable, ciphered. In this interaction, the UE only proceeded with deregistration after a properly protected Deregistration Request was received from the AMF, and its response (Deregistration Accept) would also be sent under the established security context. This behavior aligns with 3GPP requirements, as the UE did not process any unprotected or suspicious messages and adhered to the expected security procedures. Therefore, based on the observed actions and adherence to security protocols, the UE's behavior 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 completion of the 5G Authentication and Key Agreement (5G-AKA) procedure, the User Equipment (UE) sent a "security mode complete" message to the Access and Mobility Management Function (AMF), indicating that it had accepted the negotiated security algorithms and was ready to begin protected NAS communication. Following this, the AMF sent a "service accept" message to the UE, which was transmitted as a protected (i.e., integrity protected and/or encrypted) NAS message. According to the 3GPP 5G standard, after the security mode command is successfully completed, all subsequent NAS messages between the UE and the AMF should be protected using the agreed-upon security context. In this scenario, the UE did not respond to the protected "service accept" message from the AMF. This lack of response from the UE is a deviation from expected behavior, as the UE should be able to process protected messages after security activation. The absence of a response may indicate that the UE either failed to decrypt or verify the integrity of the protected message, or it did not recognize the message as valid. This behavior suggests a potential security issue or implementation flaw in the UE, as it is unable to handle protected NAS messages as required by 3GPP specifications after 5G-AKA and security mode completion. Insecure

36	36	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5051651000976562 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5054340362548828 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7091829776763916 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the User Equipment (UE) sent a "Registration Complete" message to the Access and Mobility Management Function (AMF), indicating the end of the registration process. The AMF then sent a "Deregistration Request (UE terminated)" to the UE, which was both integrity protected and ciphered, as indicated by the security header (2). The UE responded with a "Deregistration Accept (UE terminated)" message. According to the 3GPP 5G standards, after the completion of the authentication and key agreement (5G-AKA), all subsequent NAS messages exchanged between the UE and the AMF must be protected by both integrity and ciphering to ensure confidentiality and authenticity. The packet capture confirms that the deregistration request from the AMF was indeed protected, and the UE responded appropriately with a deregistration accept message. Since the UE only responded to a properly protected and encrypted deregistration request, and did not accept or process any unprotected or suspicious messages, its actions were in line with the 3GPP security requirements. Therefore, the UE's behavior in this scenario was secure. Secure
37	37	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5078079700469971 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080060958862305 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Service accept 0.7117960453033447 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration complete" message to the AMF, followed by the AMF sending a "Service accept" message back to the UE, which was indicated as a protected (i.e., integrity protected and/or encrypted) NAS message. Subsequently, the UE sent a "Deregistration request (UE originating)" message to the AMF. According to the 3GPP 5G standard, once 5G-AKA is completed, NAS security procedures are established, and all subsequent NAS messages between the UE and AMF should be integrity protected and, where required, encrypted. The packet capture shows that the UE’s deregistration request was sent after security activation, meaning it should have been protected by NAS security. There is no indication in the summary or the packet capture that the UE sent any unprotected NAS messages after the security context was established. Therefore, based on the information provided, the UE acted according to 3GPP security requirements by ensuring that its NAS messages, including the deregistration request, were sent only after a secure context was established. This behavior aligns with the 5G security standards and does not reveal any insecure action by the UE in this interaction. Secure

38	38	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.5716309547424316 UE to AMF UplinkNASTransport, Registration complete 0.5718338489532471 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" uplink NAS message to the AMF, indicating that the initial registration process had concluded. Following this, the AMF sent a "Security Mode Command" downlink NAS message to the UE, which was protected using integrity protection with a new security context, as indicated by the security header type (3). The message specified the use of the null ciphering algorithm (5G-EA0) but enabled integrity protection with 128-5G-IA2. Notably, after receiving this protected command, the UE did not respond. According to the 3GPP 5G standards (TS 24.501, TS 33.501), the UE is expected to process the Security Mode Command and respond with a Security Mode Complete message if the command is valid. However, if the security parameters are unacceptable (for example, if only the null ciphering algorithm is proposed when stronger algorithms are available and supported), the UE may reject the command or remain silent as a protective measure. Since the AMF requested null encryption (5G-EA0) immediately after authentication, the UE’s lack of response suggests it refused to downgrade security, thereby preventing a potential security vulnerability (such as a ciphering algorithm downgrade attack). This behavior aligns with 3GPP security recommendations, which state that the UE should not accept weak security configurations when stronger options are available. Therefore, the UE’s action in this scenario is considered secure. 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 security test for a 5G standalone User Equipment (UE), the interaction began with the successful completion of the 5G-AKA authentication procedure, which is a prerequisite for establishing security keys used for NAS (Non-Access Stratum) message protection. Following the authentication, the UE sent a "registration complete" message to the AMF, indicating the completion of its registration process. The AMF then responded with a "configuration update command," which, according to the packet capture and test summary, was sent as a protected message—specifically, it was integrity protected and ciphered, as indicated by the security header value of 2. The UE subsequently replied with a "configuration update complete" message, confirming receipt and processing of the configuration update. Since the 5G-AKA was completed before any protected NAS messages were exchanged, and all subsequent sensitive NAS messages (such as the configuration update command) were both ciphered and integrity protected, the UE adhered to the 3GPP 5G security requirements for NAS message protection. This means the UE only accepted and responded to configuration updates that were properly protected after security activation, thus maintaining the confidentiality and integrity of its communication with the AMF. Based on this analysis, the actions taken by the UE were secure according to the 5G standard. 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 5G standalone security test, the UE first completed the 5G-AKA authentication process, which is essential to establish security keys for NAS message encryption and integrity protection as specified by 3GPP standards. Following the successful authentication, the UE sent a "Registration Complete" uplink NAS message to the AMF. The AMF then responded with a "Configuration Update Command" downlink NAS message, which was marked as both integrity protected and ciphered, indicating that it was sent using the established security context. The UE responded appropriately with a "Configuration Update Complete" message. Since the 5G-AKA procedure was completed before any sensitive NAS communication, and all subsequent messages (including the configuration update command) were protected by both encryption and integrity mechanisms, the UE’s actions demonstrate adherence to 3GPP security requirements for NAS message protection. The UE did not transmit or accept any unprotected sensitive messages after the security context was established, which is the expected secure behavior in 5G networks. Therefore, based on the captured interaction and the 3GPP 5G security standards, the UE's actions were secure. Secure

41	41	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0272 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 6.938914060592651 UE to AMF UplinkNASTransport, Registration complete 6.939129114151001 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Security mode command 7.142905950546265 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 7.143115997314453 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE first completed the 5G-AKA authentication and then sent a "registration complete" message to the AMF, as expected. Afterward, the AMF sent a "security mode command" message, which was properly protected (integrity protected with a new security context and using the correct cipher and integrity algorithms). According to the 3GPP 5G standard, after successful authentication and security mode command, the UE is expected to respond to the security mode command (typically with a "security mode complete" message) to establish the agreed security context before any further NAS communication. However, in this scenario, the UE did not respond to the security mode command at all. Instead, the next message from the UE was an "InitialUEMessage" (Service request), which occurred without the security mode being completed. This is not compliant with the 3GPP security procedures, as the UE must not send further NAS messages (especially sensitive ones like service requests) before the security context is confirmed and active. The lack of response to the security mode command and the subsequent sending of an unprotected service request exposes the UE to potential security risks, such as replay or impersonation attacks, undermining the integrity and confidentiality guarantees of the 5G NAS protocol. Therefore, based on the 3GPP standard and the observed behavior, the UE's actions in this scenario are considered insecure. Insecure
42	42	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.513239860534668 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5140058994293213 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5144908428192139 AMF to UE DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an UplinkNASTransport message to the AMF, which was followed by the AMF sending a protected Deregistration Accept message back to the UE. Notably, the UE did not respond to the Deregistration Accept message. According to the 3GPP 5G NAS protocol (TS 24.501), after the UE initiates a deregistration request or receives a Deregistration Accept message (especially when the deregistration is UE-initiated or UE-terminated as indicated here), the UE is expected to locally release the NAS signaling connection and not send any further NAS messages unless it wishes to re-register or initiate new procedures. The fact that the Deregistration Accept was protected indicates that the security context established by 5G-AKA was used, and the UE's lack of response aligns with the standard, as the protocol does not require an explicit acknowledgment from the UE after receiving a Deregistration Accept. Therefore, based on the sequence of events and adherence to 3GPP procedures, the UE's actions were secure and compliant with the 5G standard. 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 completing the 5G-AKA authentication and key agreement, the UE sent an UplinkNASTransport message, which was followed by the AMF sending a Configuration Update Command. According to the packet capture, the Configuration Update Command from the AMF was protected—specifically, it was both integrity protected and ciphered, as indicated by the security header type (2). This means that the NAS security context was active, and both encryption and integrity protection were being applied to the NAS messages, which is a requirement after successful 5G-AKA as per 3GPP TS 33.501. Subsequently, the UE responded with a Deregistration Request (UE originating), which was also sent after the NAS security context was established. The sequence of messages and the application of security protection to the downlink message demonstrate that the UE adhered to the 3GPP security requirements by only sending and accepting protected messages after 5G-AKA. The UE did not process or respond to any unprotected or insecure messages, and it initiated deregistration in a secure context. Therefore, based on the observed behavior and alignment with 3GPP standards, the actions taken by the UE were secure. Secure
44	44	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 6.589772939682007 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.5903379917144775 AMF to UE SACK (Ack=18, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.590748071670532 AMF to UE DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 6.793751955032349 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, following the successful completion of the 5G-AKA authentication procedure, the UE initiated uplink NAS transport messages to the AMF, including a PDU session establishment request. The AMF, under test control, subsequently sent a deregistration request to the UE. This deregistration request was protected, as indicated by the security header specifying integrity protection and ciphering, which is consistent with 3GPP security requirements post-authentication. Upon receipt of this protected deregistration request, the UE responded with a deregistration accept message, thereby terminating its registration as instructed. According to 3GPP standards, specifically TS 24.501, after the security context is established via 5G-AKA, all subsequent NAS signaling, including deregistration procedures, must be integrity protected and ciphered. The UE's behavior—processing only a protected deregistration request and responding appropriately—demonstrates compliance with these security requirements. The UE did not process any unprotected or suspicious messages and only acted upon a securely delivered command, which aligns with the expected secure operation defined by the 5G standard. Based on this analysis, the actions taken by the UE were secure. Secure

45	45	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5155510902404785 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5157649517059326 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5159080028533936 AMF to UE DownlinkNASTransport, Configuration update command 0.7195420265197754 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the User Equipment (UE) initiated a protected NAS communication by sending an UplinkNASTransport message. The Access and Mobility Management Function (AMF), under test control, responded with a Configuration Update Command, which was transmitted using a security header indicating both integrity protection and ciphering, as per security header type 2. The UE then responded with a Configuration Update Complete message, also sent as an UplinkNASTransport. Given that 5G-AKA was completed prior to these exchanges, the NAS security context should have been established, ensuring that subsequent NAS messages are both encrypted and integrity protected. The packet capture confirms that the Configuration Update Command from the AMF was indeed protected, and there is no indication that the UE accepted or processed any unprotected or improperly protected messages. According to the 3GPP 5G standard, it is mandatory for the UE to only process NAS messages that are integrity protected (and, where required, ciphered) after the security context is established. The UE's behavior in this test aligns with these requirements, as it only responded to a properly protected message and followed the expected protocol steps. Therefore, the actions taken by the UE in this test were secure and compliant with the 3GPP standard. Secure
46	46	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.425251007080078 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4254679679870605 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4255969524383545 AMF to UE DownlinkNASTransport, Configuration update command 2.629240036010742 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication and security setup, the UE sent a UL NAS Transport message to the AMF, indicating that the NAS security context was already established. Following this, the AMF issued a Configuration Update Command to the UE, which was protected with both integrity and ciphering, as indicated by the security header (value 2: "integrity protected and ciphered"). The UE responded with a Configuration Update Complete message, which was also sent within the established NAS security context. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed and security is activated, all subsequent NAS messages must be integrity protected and, where required, ciphered. The packet capture confirms that the Configuration Update Command was indeed protected, and the UE's response followed the expected secure communication procedures. Therefore, the actions taken by the UE adhered to the 5G security requirements, ensuring that sensitive NAS signaling was not exposed or vulnerable to interception or tampering. Based on this analysis, the UE's behavior was secure and compliant with the 3GPP standard. Secure

47	47	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.4281399250030518 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4283440113067627 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.428462028503418 AMF to UE DownlinkNASTransport, Configuration update command 2.6321370601654053 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE proceeded to send 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 message details, was transmitted as a protected NAS message—specifically, it was both integrity protected and ciphered, as indicated by the security header (2). The UE then responded with a Configuration Update Complete message, also encapsulated in an Uplink NAS Transport message. According to the 3GPP 5G security standards, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected using both integrity protection and ciphering to ensure confidentiality and integrity of the signaling. The packet capture confirms that the Configuration Update Command from the AMF was indeed protected, and the UE responded appropriately with a Configuration Update Complete message, which, based on the sequence and context, would also be expected to be protected as per standard procedure. Therefore, the actions taken by the UE align with the 3GPP requirements for secure NAS signaling post-authentication, indicating that the UE maintained the expected security posture throughout the interaction. Secure

48	48	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3200 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 2.4352028369903564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4353890419006348 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.435595989227295 AMF to UE DownlinkNASTransport, Security mode command 2.6392359733581543 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE proceeded with uplink NAS transport messages, indicating that it had successfully established a security context with the AMF. The AMF then sent a Security Mode Command to the UE, protected using the negotiated security algorithms (Cipher: 5G-EA4, Integrity: 128-5G-IA2) and with the security header indicating "Integrity protected with new security context." Upon receiving this, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified." According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept the Security Mode Command if it is correctly protected using the newly established security context and valid algorithms. A Security Mode Reject is only expected if there is an error, such as an unsupported algorithm or an improperly protected message. Since the Security Mode Command was properly protected and used supported algorithms (as per the test setup), the UE's rejection without a specific cause ("unspecified") suggests non-standard behavior or a potential security issue, as it should have accepted the command under normal circumstances. Therefore, the action taken by the UE does not align with the secure behavior expected by 3GPP standards, as it could indicate a failure to establish secure communication or improper handling of the security context. **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 sent a service request to the AMF. In response, the AMF issued a Security Mode Command (SMC) message that was integrity protected, specifying the use of the null cipher algorithm (5G-EA0) and integrity algorithm 128-5G-IA2, with the security header indicating a new security context. Upon receiving this, the UE rejected the security mode command with an unspecified reason. According to the 3GPP 5G security standard (TS 33.501), the use of the null ciphering algorithm (5G-EA0) is permitted only under specific conditions, such as emergency services or regulatory requirements, and UEs are allowed (and in some cases required) to reject SMCs that propose null encryption outside of those scenarios. Since the AMF attempted to establish a security context with no encryption (5G-EA0) after successful authentication, and the UE responded by rejecting this insecure configuration, the UE's action demonstrates proper adherence to the security requirements of the standard. Thus, the UE behaved securely by refusing to proceed with an unencrypted security context, thereby protecting user data and signaling. 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 successful completion of 5G-AKA authentication and security procedures (which establish NAS security context), the UE sent a protected Service Request message to the AMF, indicating a request to resume or establish a service. In response, the AMF sent a protected Deregistration Accept message to the UE. The packet capture confirms that the Service Request was sent uplink from the UE, and the Deregistration Accept was sent downlink from the AMF, both after security activation. Critically, after receiving the protected Deregistration Accept, the UE did not respond with any further NAS messages. According to 3GPP standards (TS 24.501), upon receiving a Deregistration Accept from the network, the UE is expected to release its NAS signaling connection and not send further NAS messages unless reinitiating registration or another procedure. The absence of a response from the UE is therefore compliant with the standard and does not indicate any security weakness; it simply means the UE accepted the deregistration and ceased communication as required. The use of protected (encrypted and integrity-protected) messages after 5G-AKA is also in accordance with 3GPP security requirements. Thus, the UE's actions in this interaction were secure and standards-compliant. 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 the 5G-AKA authentication and key agreement procedure, the UE sent a service request to the AMF, indicating it was ready to initiate a session or resume connectivity. In response, the AMF sent a deregistration request (UE terminated), which was integrity protected and ciphered, indicating that NAS security had been established and all subsequent NAS messages were required to be secured. The UE, upon receiving this protected deregistration request, responded appropriately with a deregistration accept message, also under NAS security protection. According to the 3GPP 5G standards (TS 24.501 and TS 33.501), the UE must only accept and process deregistration requests that are integrity protected and ciphered after security mode is established. The UE's actions—processing only a protected deregistration request and replying with a protected deregistration accept—demonstrate compliance with these security requirements. Therefore, the UE's behavior was secure, as it adhered to the 5G standard's expectations for message protection and state management in NAS communication. Secure
52	52	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 11.176167011260986 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 11.17656421661377 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command 11.383517980575562 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is the expected behavior for establishing or resuming a session. The AMF responded with a Configuration Update Command, which was sent as a protected NAS message, specifically marked as "integrity protected and ciphered," indicating that both confidentiality and integrity of the message were ensured as per 3GPP security requirements. Upon receiving this protected message, the UE responded by sending a Deregistration Request (UE originating) via an UplinkNASTransport message. Since the 5G-AKA had already been completed, all subsequent NAS messages, including the service request, configuration update command, and deregistration request, were expected to be protected (integrity protected and ciphered) according to 3GPP TS 33.501. The UE's actions demonstrate adherence to the security procedures outlined by 3GPP, as it did not proceed with any unprotected NAS communication after the establishment of security context. There is no indication that the UE accepted or acted upon any unprotected or tampered messages, and its deregistration request followed proper protected NAS signaling. Thus, based on the sequence of events and the security protections in place, the UE's actions were secure and compliant with the 5G standard. Secure

53	53	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 17.000593185424805 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.001089096069336 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal UE) 17.204612970352173 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the User Equipment (UE) initiated a service request to the Access and Mobility Management Function (AMF). In response, the AMF sent a deregistration request (with the cause "UE terminated" and marked as "Illegal UE") to the UE. Importantly, this deregistration request was transmitted as a protected NAS message, meaning it was both integrity protected and ciphered, as indicated by the security header type (2). The UE, upon receiving this protected deregistration request, responded with a deregistration accept (UE terminated) message, also via a protected NAS message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS signaling—especially those involving sensitive operations such as deregistration—must be both integrity protected and ciphered to ensure confidentiality and authenticity. In this interaction, the UE correctly processed and responded only to a protected deregistration request and sent its own protected deregistration accept, demonstrating compliance with the security requirements of the 5G standard. Therefore, the actions taken by the UE were secure, as it did not accept or respond to any unprotected or improperly protected NAS messages, and all sensitive exchanges were properly encrypted and integrity checked. Secure
54	54	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 100 UE provided: No response The packet capture during the test using wireshark is: 1.321023941040039 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.3216829299926758 AMF to UE DownlinkNASTransport, 5GMM status (Conditional IE error) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successful completion of 5G-AKA (meaning security context was established and NAS messages could be protected), the UE sent a Service Request to the AMF. In response, the AMF sent a protected (i.e., integrity protected and possibly encrypted) GMM Status message with a 5GMM Cause value of 100, which indicates a "Conditional IE error" as per 3GPP TS 24.501. The UE did not respond to this message. According to the 3GPP 5G NAS specification, upon receiving a GMM Status message (even if protected) with certain error causes such as "Conditional IE error," the UE is not required to respond and may simply ignore the message, especially if the error does not impact ongoing procedures or requires no corrective action from the UE. Since the UE did not send any further NAS messages in response and did not process or act on the potentially suspicious or malformed message, it behaved in accordance with the 3GPP security requirements for NAS message handling. This cautious approach prevents the UE from being manipulated or tricked by unexpected or erroneous messages, thus upholding the security principles of the 5G standard. Secure

55	55	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003898143768310547 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, the UE initiated a registration procedure by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with an Authentication Reject message that was sent in plain (unencrypted) form. At this stage, the 5G-AKA authentication and key agreement procedure had not yet been completed, so no security context was established and thus no encryption or integrity protection was possible for NAS messages. According to the 3GPP 5G standard (TS 24.501), before authentication and security setup, the UE is required to accept and process certain NAS messages, including Authentication Reject, even if they are sent in plain text, as it has no means to verify or reject them securely at this stage. The UE, in this test, did not respond further after receiving the Authentication Reject, which is the expected and secure behavior as per the standard: upon receiving an Authentication Reject, the UE should abort the registration attempt and not proceed with further communication. Therefore, the UE's actions were in line with 3GPP security requirements for this scenario, ensuring that it did not expose itself to further risk or protocol misuse. Secure
56	56	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00040602684020996094 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF, which is the expected first step in establishing a NAS connection. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form before the 5G-AKA authentication procedure was completed. According to the 3GPP 5G security architecture, specifically TS 33.501, NAS messages sent before the completion of authentication and key agreement (5G-AKA) are not protected by ciphering or integrity protection, and the initial registration request is expected to be sent in plain. Importantly, Authentication Reject is a legitimate message that can be sent by the network if authentication fails or is not allowed, and it is also permitted to be sent in plain before security context establishment. The UE, upon receiving the Authentication Reject, did not respond further, which aligns with 3GPP expectations—after receiving an Authentication Reject, the UE should abort the registration and not proceed with further communication. This behavior prevents the UE from processing potentially malicious or spoofed network requests, thereby protecting itself from possible attacks such as downgrade or replay. Therefore, the UE's action—sending the initial registration request and then not responding to an unauthenticated Authentication Reject—demonstrates compliance with the 3GPP security requirements for pre-authentication NAS procedures. 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 procedure by sending an initial registration request to the AMF. The AMF, under tester control, responded with an Authentication Reject message sent in plain (unencrypted) form, prior to the completion of the 5G-AKA authentication and key agreement procedure. According to the 3GPP 5G security standards (TS 33.501), until 5G-AKA is completed, NAS messages are not protected by integrity or encryption, and the UE must treat any plain NAS message received before authentication as potentially insecure. Specifically, the standard mandates that upon receiving an Authentication Reject message before security context establishment, the UE must not respond further and should consider the network potentially malicious or compromised. In this test, the UE did not respond after receiving the plain Authentication Reject, which aligns with the security requirements to prevent downgrade or denial-of-service attacks from a rogue or compromised AMF. Therefore, the UE's behavior was secure and compliant with the 3GPP 5G security standard. Secure
58	58	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003209114074707031 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under tester control, responded with an Authentication Reject message sent in plain (unencrypted) form, prior to the completion of the 5G-AKA authentication procedure. According to 3GPP standards, specifically TS 24.501, before the 5G-AKA is completed, all NAS messages between the UE and AMF are sent in plain text because security context and ciphering keys have not yet been established. Upon receiving an Authentication Reject message in this state, the UE is expected to take no further action in response, as the reject indicates that authentication has failed or is not permitted. The UE correctly provided no response to the Authentication Reject, which aligns with the 3GPP recommendation that the UE should abort the registration attempt and not proceed further. This behavior prevents potential security issues such as responding to potentially spoofed or unauthorized messages, especially since ciphering and integrity protection are not yet active at this stage. Therefore, the UE acted securely according to the 5G standard. 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 a Registration Request to the AMF, which was transmitted in plain text as the 5G-AKA authentication procedure had not yet been completed. In response, the AMF sent an Authentication Reject message, also in plain text. Critically, after receiving the plain-text Authentication Reject, the UE did not respond or proceed with further actions. According to the 3GPP 5G security standards, before the completion of 5G-AKA, NAS messages—including Registration Request and Authentication Reject—are not protected by encryption or integrity, and this is expected behavior. Furthermore, 3GPP specifies that upon receiving an Authentication Reject before authentication is completed, the UE should not respond and should abort the registration procedure, which is exactly what the UE did in this test. This behavior prevents the UE from acting on potentially spoofed or malicious messages received before a secure context is established. Therefore, the UE's actions were consistent with 3GPP security requirements and did not expose it to additional risk in this scenario. 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 5G standalone User Equipment (UE) initiated a registration process 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 sent in plain (unencrypted) form before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should not accept or respond to any NAS messages that are sent in plain text after the initial registration request, except for a limited set of allowed messages prior to authentication (such as Authentication Request/Reject and Identity Request). However, since the Authentication Reject message is one of the few exceptions allowed to be sent in plain text before security is activated, the UE's refusal to respond further is in line with expected secure behavior: it did not proceed with any further communication or take any action that could compromise its security context. The UE's action of not responding to the plain Authentication Reject message demonstrates compliance with the 3GPP standard and protects against potential security threats such as false base station attacks or replay attacks at this stage. 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 the registration process by sending an initial registration request to the AMF. At this stage, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that mutual authentication and the establishment of NAS security (encryption and integrity protection) were not yet in place. The AMF, under test control, responded with a registration reject message, which was sent in plain (unencrypted) form, as is permitted by the 3GPP 5G standard (TS 24.501) prior to the completion of authentication and key establishment. The UE, upon receiving this plain registration reject message with a 5GMM cause code of 111 (protocol error, unspecified), did not respond further. According to the 3GPP standard, the UE is required to accept certain NAS messages, including registration reject, in plain form before security is activated, and it should not send further NAS messages in response to a registration reject. The UE's behavior aligns with these requirements, as it did not respond after receiving the reject message. Therefore, the UE acted in accordance with the security expectations of the 5G standard by not attempting to proceed with an unprotected NAS session or responding to a protocol error before authentication and security establishment. Secure
62	62	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.596633911132812 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.597079038619995 AMF to UE SACK (Ack=14, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE initiated a service request, which is a normal step for requesting network services. In response, the AMF sent a "deregistration accept" message, indicating that the network was instructing the UE to consider itself deregistered. Importantly, the test summary states that the downlink "deregistration accept" message from the AMF was sent as "Protected," meaning it was integrity protected and/or encrypted, as required by the 3GPP 5G security specifications after 5G-AKA completion. The UE, upon receiving this protected deregistration message, provided no response, effectively ceasing further communication. According to 3GPP standards (TS 24.501), the UE is required to process protected deregistration messages and should not respond to a valid, integrity-protected "deregistration accept" from the network, as this indicates the end of the NAS security context and the deregistration procedure is complete. Therefore, the UE's action—no response to a protected deregistration—aligns with the expected secure behavior defined by the 5G standard, ensuring that it only acts on protected messages after authentication and does not respond to messages that would compromise its security context. 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 completing the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which is the expected behavior as per the 3GPP 5G security procedures. Subsequently, the AMF sent a Security Mode Command message to the UE, which was protected using integrity and ciphering algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity), with the security header indicating that a new security context was established. The ABBA parameter was also present, as required for certain security contexts. After receiving the Security Mode Command, the UE responded with a Deregistration Request (UE originating). According to the 3GPP standard, after the security context is established (post-Security Mode Command), all subsequent NAS messages from the UE must be integrity protected and, if required, ciphered. The Deregistration Request was sent after the security context was set up, which means it should have been protected according to the negotiated algorithms. Since the packet capture does not indicate any security anomalies and the sequence of events aligns with the 3GPP-defined procedures (authentication, security context establishment, and protected NAS messaging), the UE's actions were secure and compliant with the standard. Secure
64	64	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.12326717376709 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.123653173446655 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure—which establishes security context for NAS message protection—the UE sent a Service Request uplink message to the AMF, initiating a service procedure. The AMF responded with a Service Accept message, which was correctly sent as a protected (i.e., integrity protected and ciphered) NAS message, as required by 3GPP standards once 5G-AKA is completed. However, the UE did not respond to the protected Service Accept message from the AMF. According to the 3GPP 5G NAS protocol specifications (TS 24.501), after receiving a protected Service Accept message, the UE is expected to process and acknowledge the message, potentially proceeding with further signaling or user data transfer. The lack of response from the UE to a properly protected downlink message indicates that the UE failed to handle a legitimate, standards-compliant message as expected. This behavior could leave the UE unable to properly establish or resume services, which may expose it to denial-of-service or interoperability issues. Based on this analysis, the UE's action was **insecure** because it did not comply with the expected secure behavior defined by 3GPP for NAS message handling after security activation. Insecure

65	65	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.15958499908447266 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16092395782470703 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36401796340942383 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) successfully completed the 5G-AKA authentication and then sent a Security Mode Complete message to the Access and Mobility Management Function (AMF), indicating acceptance of the negotiated security algorithms and the establishment of a new security context. However, contrary to the expected protocol flow, the AMF responded with another Security Mode Command, this time protected with integrity and ciphering using the new security context (as indicated by the security header value 3). Upon receiving this protected Security Mode Command, the UE responded with a Security Mode Reject (Security mode rejected, unspecified). According to the 3GPP 5G standards, once the Security Mode Complete is sent and the security context is established, the AMF should not send another Security Mode Command for the same context unless a new context is being established or there is a valid protocol reason. The UE, upon receiving an unexpected or redundant Security Mode Command, correctly rejected it, as accepting such messages could open up vulnerabilities to replay or downgrade attacks. The UE's action to reject the message, even though the reason was unspecified, aligns with secure protocol behavior to prevent unauthorized or suspicious security context changes. Therefore, the UE's response demonstrates adherence to secure communication practices as outlined by the 3GPP standard. Secure

66	66	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0322 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 2.5863499641418457 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.5868079662323 AMF to UE SACK (Ack=9, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.5871849060058594 AMF to UE DownlinkNASTransport, Security mode command 2.7903499603271484 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message, indicating it was ready to proceed with further communication. The AMF then sent a Security Mode Command to the UE, which was protected using the negotiated security algorithms (128-5G-EA1 for ciphering, 128-5G-IA2 for integrity, and ABBA: 0322), and the security header indicated that the message was integrity protected with a new security context. Upon receiving this message, the UE responded with a Security Mode Reject, citing an unspecified reason for the rejection. According to the 3GPP 5G standard (TS 24.501), a UE must reject a Security Mode Command if it detects any issues—such as mismatched algorithms, unsupported parameters, or failures in integrity/ciphering checks—to prevent establishing communication with potentially insecure or misconfigured network entities. Since the Security Mode Command was protected and the UE still chose to reject it, this action suggests that the UE detected an anomaly or could not accept the proposed security context. This cautious behavior aligns with the security requirements of the standard, where the UE must not accept potentially insecure security contexts, even after successful authentication. Therefore, the UE's action demonstrates secure behavior, as it did not proceed with a potentially compromised or misconfigured security setup. 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 the 5G-AKA authentication and security procedures, the UE initiated a service request, which is a standard step in establishing 5G NAS communication. The AMF, under controlled test conditions, responded with a protected (encrypted) GMM status message containing 5GMM cause 98, which indicates "Message type not compatible with the protocol state." Upon receiving this, the UE replied with its own 5GMM status message, echoing the same cause. According to 3GPP standards (TS 24.501), when a UE receives a GMM status message with a cause value indicating a protocol error, it is permitted to respond with a status message indicating the error, especially if the received message was protected (i.e., integrity protected and/or ciphered). The UE's response demonstrates that it validated the protocol state, recognized the incompatibility, and reported it using a protected channel, which aligns with the 3GPP security requirements for NAS message handling. This behavior indicates that the UE did not process an invalid or unexpected message in an insecure manner, but rather followed standard protocol by reporting the error securely. Therefore, based on the interaction and adherence to 3GPP-defined security procedures, the UE's actions in this test 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.	In this test scenario, the UE first completed the 5G-AKA authentication procedure, establishing a secure context for subsequent NAS communication. Following this, the UE sent a service request to the AMF, which responded with a configuration update command. The packet capture shows that the configuration update command from the AMF was sent as a protected message, specifically integrity protected, as indicated by the security header. The UE then replied with a configuration update complete message, and also sent a registration request. According to the 3GPP 5G standard, after the successful completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF must be integrity protected, and, depending on the message type and security context, may also be ciphered. In this case, the configuration update command was integrity protected, and the UE appropriately responded with a configuration update complete message, which is the expected behavior. There is no indication in the capture that the UE sent or accepted unprotected or insecure messages after the security context was established. Therefore, based on the described interaction and adherence to the 3GPP security requirements, 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 successful completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF. The AMF then issued a Security Mode Command, indicating the use of 5G-EA0 (null ciphering, i.e., no encryption) for the ciphering algorithm, and 128-5G-IA2 for integrity protection, with the security header set to "integrity protected with new security context." The Security Mode Command was sent as a protected message. Upon receiving this, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified." According to the 3GPP 5G security standards, after 5G-AKA, the UE and network must negotiate security algorithms for both ciphering and integrity protection. While integrity protection was enabled, the choice of 5G-EA0 (no ciphering) means that user data would not be encrypted over the air, which exposes the UE to potential eavesdropping. The 3GPP standard (TS 33.501) allows the UE to reject a Security Mode Command if it considers the proposed algorithms or security context to be unacceptable or insecure. By rejecting the Security Mode Command when only null ciphering was offered, the UE demonstrated correct and secure behavior by refusing to operate in a mode that would leave its communications unencrypted. This aligns with best security practices and the intent of the 5G security architecture to protect user confidentiality. 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.	During this test, after the completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had successfully registered. Immediately after, the AMF sent a "Security Mode Command" message to the UE, which was protected (integrity protected and ciphered with a new security context), using the null ciphering algorithm (5G-EA0) and integrity algorithm 128-5G-IA2. The security header indicated that this message was both integrity protected and ciphered with the new context, but the ciphering algorithm selected was null, meaning no encryption was applied to the message payload. The UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after successful authentication, the AMF initiates security mode control to establish NAS security, and the UE is expected to respond to a properly protected Security Mode Command. The use of 5G-EA0 (null ciphering) is permitted in certain circumstances, but it is generally discouraged unless required for specific reasons (such as emergency services or regulatory requirements), and the UE should still respond to the Security Mode Command as long as integrity protection is applied. The fact that the UE did not respond to a valid, protected Security Mode Command (even with null ciphering) is a deviation from the expected 3GPP behavior, as it could indicate that the UE is not properly handling security procedures or is refusing to operate without encryption even when integrity protection is present. This could potentially be considered insecure, as it may leave the UE unable to proceed with secure communication or vulnerable to denial of service if it cannot handle permitted security configurations. 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 5G standalone security test, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Security Mode Command to the UE. The Security Mode Command from the AMF was sent as a protected message, using cipher algorithm 128-5G-EA3 and integrity algorithm 5G-IA0 (null), with the security header indicating both integrity protection and ciphering. However, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after 5G-AKA, the UE and network must negotiate and activate NAS security (ciphering and integrity protection) through the Security Mode Command procedure. The use of 5G-IA0 (null integrity) is permitted but not recommended for most deployments, as it does not provide integrity protection. More critically, the UE is expected to respond to the Security Mode Command with a Security Mode Complete message; failure to do so means the UE is not properly participating in the security procedure. This lack of response prevents the establishment of a secure NAS signaling connection and leaves the session in an incomplete and potentially vulnerable state. Therefore, the UE's action—specifically, its failure to respond to the Security Mode Command—was not in line with 3GPP security procedures and represents insecure behavior, as it does not ensure the mutual agreement and activation of security protections for further NAS communication. Insecure

72	72	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 6.590965032577515 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.591464042663574 AMF to UE SACK (Ack=25, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.5918920040130615 AMF to UE DownlinkNASTransport, Security mode command 6.7950029373168945 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	During the test, after the successful completion of the 5G-AKA authentication procedure, the UE sent an UplinkNASTransport message, indicating it was ready to proceed with secure NAS communication. The AMF, under test control, then sent a Security Mode Command with the ABBA parameter set to 3300, specifying the use of cipher algorithm 5G-EA5 and integrity algorithm 128-5G-IA2, and marked the message as "integrity protected with new security context." Upon receiving this, the UE responded with a Security Mode Reject, specifying the reason as "Security mode rejected, unspecified." According to 3GPP 5G standards (TS 24.501), a UE should only reject a Security Mode Command if it detects an issue such as an unsupported algorithm, an invalid security context, or other security-related inconsistencies. The "unspecified" reason code does not provide detailed information, but the rejection itself is a secure behavior if the UE detected any anomaly or non-compliance with expected security parameters—especially since the Security Mode Command was sent as protected, indicating the AMF was following the protocol. Since the test was controlled and the AMF could have been configured to use unusual or unsupported parameters, the UE's action to reject the security mode setup rather than proceeding insecurely or with unsupported algorithms demonstrates adherence to security principles, as it avoids establishing a compromised or misconfigured security context. Thus, the UE's response aligns with secure behavior as outlined by the 3GPP standard, even though the specific rejection reason is not detailed. Secure

73	73	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1599750518798828 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602010726928711 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3605461120605469 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of 5G-AKA (authentication and key agreement), the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the previously negotiated security algorithms and parameters. Unexpectedly, the AMF then sent another "security mode command" message, which was protected using integrity protection (128-5G-IA2) but specified the null ciphering algorithm (5G-EA0), meaning user data would not be encrypted. Upon receiving this, the UE responded with a "security mode reject," citing an unspecified reason. According to the 3GPP 5G security standard, the use of 5G-EA0 (null ciphering) is discouraged except in specific, limited scenarios (such as emergency services or where local policy allows), and UEs are expected to reject security mode commands that attempt to establish a null ciphering algorithm unless explicitly permitted. The UE's action to reject the security mode command when 5G-EA0 was proposed aligns with these security principles, as accepting it would have resulted in unencrypted communication and a potential security risk. Therefore, the UE's behavior demonstrates adherence to the 5G security requirements and best practices as outlined by 3GPP. Secure

74	74	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03b3 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11993098258972168 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12021493911743164 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3277699947357178 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G Authentication and Key Agreement (5G-AKA) procedure, the UE sent an authentication response to the AMF, indicating successful authentication. The AMF then sent a Security Mode Command to the UE, which was integrity-protected and indicated the use of specific ciphering (128-5G-EA3) and integrity (128-5G-IA2) algorithms, with a new security context established. Upon receiving this, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, the UE is expected to verify the integrity and validity of the Security Mode Command, including checking the supported algorithms and the correctness of the security context. If the UE detects any anomaly, such as unsupported algorithms, an invalid ABBA parameter, or any inconsistency in the security context, it is mandated by the standard to reject the security mode command to prevent potential security breaches. Since the UE did not blindly accept the new security context and instead rejected it upon detecting an unspecified issue, its action aligns with secure behavior as specified by 3GPP, prioritizing the protection of the communication and preventing the establishment of a potentially insecure session. Secure

75	75	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0392 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.4745960235595703 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4750940799713135 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.47630810737609863 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent an uplink NAS transport message to the AMF, which was followed by the AMF sending a Security Mode Command (SMC) message to the UE. The SMC was integrity protected and used the new security context established during 5G-AKA, with the specified cipher and integrity algorithms (5G-EA5 and 128-5G-IA1, respectively), and a security header indicating "Integrity protected with new security context." According to the 3GPP 5G standards, once the SMC is received, the UE is expected to process it, derive the security keys, and respond with a Security Mode Complete message, thereby confirming the activation of the negotiated security algorithms. However, in this test, the UE did not respond to the SMC, which means it did not acknowledge or activate the negotiated security algorithms, nor did it confirm the protection of subsequent NAS messages. This lack of response is not compliant with 3GPP security procedures and could leave the session in an insecure state, as the security context is not confirmed or operational. Therefore, based on the actions taken by the UE, the communication was insecure. Insecure
76	76	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.16002702713012695 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16026616096496582 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF responded with an identity request for the SUCI (Subscription Concealed Identifier). Importantly, this identity request was sent as a plain (unencrypted) NAS message, as the 5G-AKA authentication procedure had not yet been completed; thus, NAS security had not been activated. According to 3GPP 5G security standards (TS 33.501), the SUCI is a privacy-preserving identifier and is designed to be sent over the air even before NAS security is established, as it is already encrypted using the home network's public key. However, the UE did not respond to the AMF's plain (unencrypted) identity request for the SUCI. From a security perspective, the UE's refusal to send the SUCI in response to a plain identity request is actually more restrictive than required by the standard, since the SUCI is specifically designed to be transmitted in the clear without compromising user privacy. The 3GPP standard allows, and even expects, the SUCI to be provided in this scenario. Therefore, while the UE's action does not introduce a security vulnerability (it does not expose the SUPI or other sensitive identifiers), it is stricter than necessary and may cause interoperability issues. In summary, the UE's behavior is secure, as it does not leak sensitive information, but it is more restrictive than the 3GPP standard requires. Secure

77	77	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0004799365997314453 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20071196556091309 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under tester control, responded with an identity request, specifically requesting the SUCI (Subscription Concealed Identifier). The UE responded with an identity response containing the requested information. Importantly, this exchange occurred before the 5G-AKA authentication procedure was completed, meaning that NAS security context had not yet been established and the messages were exchanged in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), it is expected that the initial registration and identity request/response procedures may occur before security activation, and the UE must use SUCI (a privacy-preserving, encrypted form of the SUPI) when responding to identity requests prior to security context establishment. The SUCI is specifically designed to protect the subscriber's permanent identity even when sent in the clear. Thus, the UE's actions—sending the SUCI in response to a plain identity request before 5G-AKA—are compliant with 3GPP security expectations, as the SUCI ensures the subscriber identity is not exposed even without NAS security. Therefore, the UE's actions in this scenario were secure. Secure
78	78	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1600642204284668 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16033601760864258 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36293601989746094 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the security parameters established during the NAS security setup. Unexpectedly, the AMF then issued another "security mode command" to the UE, this time specifying the use of the null ciphering algorithm (5G-EA0), meaning no encryption, while still applying integrity protection (128-5G-IA2) and marking the security header as "integrity protected with new security context." Upon receiving this command, the UE promptly responded with a "security mode reject" message, refusing to accept the new security mode and citing an unspecified reason for the rejection. According to the 3GPP 5G security standards, after 5G-AKA, the UE and network must negotiate and activate a mutually acceptable security context, which includes both ciphering and integrity algorithms. The use of 5G-EA0 (null ciphering) is only permitted under strict conditions, typically for emergency services or in limited fallback scenarios, and should not be used for normal communications as it leaves user data unencrypted and vulnerable. The UE's refusal to accept a security mode that would result in unencrypted communication (by rejecting the null ciphering algorithm) demonstrates adherence to security best practices and compliance with 3GPP guidelines, as it avoids downgrading the security context and protects user confidentiality. Therefore, the UE's action in rejecting the insecure security mode command is considered secure. 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, the 5G User Equipment (UE) completed the 5G-AKA authentication process and sent an authentication response to the Access and Mobility Management Function (AMF). Subsequently, the AMF sent a Security Mode Command to the UE, which was protected with integrity (using 128-5G-IA2) but specified the use of the null ciphering algorithm (5G-EA0), meaning that confidentiality protection (encryption) would not be applied to subsequent NAS messages. The UE responded to this Security Mode Command by sending a Security Mode Reject message, indicating "Security mode rejected, unspecified" as the cause. According to 3GPP standards (TS 33.501 and TS 24.501), after 5G-AKA, the UE and network must negotiate security algorithms for both integrity and confidentiality, and the use of the null ciphering algorithm (5G-EA0) is only permitted under very specific circumstances, such as when explicitly allowed by the UE's policy or configuration. In practice, UEs are expected to reject security mode commands that attempt to establish a security context with no encryption unless this is explicitly allowed, in order to prevent downgrade attacks and protect user confidentiality. Given this, the UE's action to reject the security mode command with 5G-EA0 (null ciphering) is consistent with secure behavior as defined by 3GPP, as it prevents the establishment of an unencrypted NAS security context and upholds the confidentiality of user communication. Secure
80	80	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.7228279113769531 UE to AMF UplinkNASTransport, Service request 0.723160982131958 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.9268310070037842 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (which establishes mutual authentication and sets up the security context for integrity and encryption), the UE sent a Service Request to the AMF. The AMF, under tester control, responded with a Configuration Update Command that was integrity protected and used a new security context, as indicated by the security header. The UE, upon receiving this message, replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G standard, the UE is expected to verify the validity and compatibility of received NAS messages with its current protocol state. If the message is not expected or is incompatible, the UE should respond with a status message highlighting the issue, which is precisely what occurred here. Additionally, since the 5G-AKA procedure was completed before these exchanges, the messages were protected as required by the standard, and the UE did not process an unexpected or possibly malicious command. Therefore, the UE's behavior aligns with the security expectations of the 5G standard: it did not accept an invalid message, responded appropriately, and maintained the integrity of the communication. Secure

81	81	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 2222 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.1596660614013672 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1599440574645996 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then responded with a Security Mode Command. The Security Mode Command was sent as a protected message, but notably, both the ciphering and integrity algorithms selected were 5G-EA0 and 5G-IA0, which are null algorithms (i.e., they provide no encryption or integrity protection). The security header indicated "integrity protected" (1), but with 5G-IA0, this protection is effectively absent. The ABBA value was set to 2222, and after receiving the Security Mode Command, the UE did not respond. According to 3GPP standards, after authentication, the Security Mode Command is used to establish NAS security, and the use of null algorithms (EA0/IA0) is only permitted under specific, controlled scenarios (e.g., for emergency services or as a fallback). In normal operation, the UE should reject or not respond to a Security Mode Command that proposes null algorithms, as this would leave the communication unprotected and vulnerable to interception or tampering. The UE's action to not respond to the Security Mode Command aligns with secure behavior as outlined by the 3GPP standard, as it avoids establishing a session with no security. Therefore, the UE's behavior in this scenario was secure. Secure

82	82	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0363 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1200721263885498 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12030816078186035 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3220691680908203 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then responded with a Security Mode Command message. The Security Mode Command specified the use of ciphering algorithm 128-5G-EA3 for encryption and 5G-IA0 (null) for integrity protection, with the security header indicating that the message was integrity protected with a new security context. Upon receiving this command, the UE replied with a Security Mode Reject message, indicating "Security mode rejected, unspecified" as the cause. According to 3GPP 5G security standards (TS 33.501), the use of 5G-IA0 (null) as the integrity protection algorithm is not recommended for normal operation, as it provides no integrity protection for NAS signaling, leaving the communication vulnerable to tampering or replay attacks. The UE's decision to reject the security mode command when only a null integrity algorithm was proposed aligns with the security best practices outlined by 3GPP, which expect UEs to reject insecure or non-compliant security configurations to prevent potential security breaches. Therefore, the UE acted securely by refusing to proceed with a session that would have lacked proper integrity protection. 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 completing the 5G-AKA authentication and key agreement procedure, the UE sent a Service Request message to the AMF, which is a typical next step in establishing NAS signaling for service access. The AMF then responded with a Service Accept message, which, according to the packet capture, was sent as a "Protected" message, indicating that NAS security (integrity and/or ciphering) was applied as per 3GPP standards after 5G-AKA completion. However, the UE did not provide any response to this Service Accept message. According to the 3GPP 5G NAS procedures, after receiving a protected Service Accept message from the AMF, the UE is expected to acknowledge or proceed with the next steps in the service procedure, depending on the context (for example, initiating user plane setup or sending further NAS messages). The lack of any response from the UE could suggest a failure to process the protected message, a protocol handling error, or a security-related issue (such as a rejection of the message due to failed integrity/cipher checks). If the UE simply dropped the message without valid reason or failed to continue the procedure as specified by 3GPP, this would be considered insecure, as it indicates non-compliance with expected secure NAS handling and could expose the device to denial-of-service or protocol downgrade vulnerabilities. Based on this analysis, the UE's action in not responding to a properly protected Service Accept message after 5G-AKA completion 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 5G standalone security test, the User Equipment (UE) and the Access and Mobility Management Function (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, which was properly protected using the negotiated ciphering (128-5G-EA2) and integrity (128-5G-IA2) algorithms, with the security header indicating that the message was integrity protected with a new security context. However, upon receiving the Security Mode Command, the UE responded with a Security Mode Reject message, citing an unspecified reason for the rejection. According to the 3GPP 5G security standard, a UE is expected to accept the Security Mode Command if the parameters (algorithms, ABBA value, etc.) are valid and consistent with the security context established during 5G-AKA. The rejection of the Security Mode Command—especially with an unspecified cause—suggests that the UE either detected an inconsistency, an unsupported algorithm, or a possible security concern, or there may be an implementation or configuration issue on the UE. From a security perspective, if the UE cannot verify the integrity or validity of the Security Mode Command, it is correct and secure for it to reject the command to avoid entering a potentially insecure state. Unless there is evidence that the UE rejected a valid and correctly protected command, the action taken by the UE aligns with secure behavior as per 3GPP standards, prioritizing security over connectivity in the face of uncertainty or potential attack. 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 this test scenario, after successfully completing the 5G-AKA authentication process, the UE sent a Security Mode Complete message to the AMF, indicating that it had accepted the negotiated security parameters. However, instead of proceeding with normal operation, the AMF sent another Security Mode Command, this time with the ABBA parameter set to 1111 and both the ciphering and integrity algorithms set to 5G-EA0 and 5G-IA0, which are null algorithms (i.e., no encryption or integrity protection). This command was also marked as "integrity protected with new security context," meaning it was presented as a legitimate, protected message. Upon receiving this, the UE responded with a Security Mode Reject message, refusing to accept the requested security configuration and indicating the rejection was "unspecified." According to 3GPP standards, the use of null algorithms (EA0/IA0) is only allowed in certain exceptional cases, such as emergency services or if the UE explicitly supports it and the network policies allow it. In normal operation, the UE is expected to reject any attempt to establish a security context with null algorithms, as this would leave user data and signaling unprotected, exposing the connection to eavesdropping and manipulation. Therefore, the UE's action to reject the security mode command with null algorithms aligns with 3GPP security requirements and demonstrates secure behavior in this context. Secure

86	86	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered (2) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15096688270568848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15124177932739258 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.35789990425109863 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone UE, 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 security parameters (cipher and integrity algorithms) provided earlier. However, the AMF, under test control, responded with another "security mode command" message, which is an unexpected behavior since, according to the 3GPP 5G standard, the security mode command should only be sent once after authentication, and any additional security mode commands should only occur if there is a justified change in security context. The UE, upon receiving this second security mode command, responded again with a "security mode complete" message. This sequence suggests that the UE accepted and processed the repeated security mode command without any indication of error or rejection. According to the 3GPP standards (TS 24.501), the UE is expected to reject or ignore an unexpected or duplicate security mode command after a security context is already established, as accepting it could expose the UE to replay or downgrade attacks, thereby compromising the integrity and confidentiality of the communication. Therefore, the UE's action of accepting and responding to a repeated security mode command is not aligned with secure behavior as required by the 5G standard. Insecure

87	87	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7935822010040283 UE to AMF UplinkNASTransport, Service request 0.793781042098999 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.9976592063903809 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information), InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.9985220432281494 AMF to UE DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication and security setup, the UE sent a Service Request to the AMF. In response, the AMF sent a Deregistration Request, which was properly protected (integrity protected and ciphered), indicating that the NAS security context was active. The UE, upon receiving this protected Deregistration Request, responded with a 5GMM Status message indicating "Invalid mandatory information," suggesting that the UE detected a problem with the received message (e.g., missing or malformed mandatory information elements). This 5GMM Status message is a standard, defined mechanism in 3GPP for UEs to report protocol errors, and it is allowed to be sent in response to protected messages when the NAS security context is active. The UE did not process the deregistration or attempt to continue with an insecure or undefined procedure; instead, it correctly flagged the protocol error. According to the 3GPP specifications (TS 24.501), this is the expected and secure behavior, as the UE did not accept a potentially malformed or suspicious message and did not expose itself to further risk. The UE maintained the integrity of the secure channel and handled the error according to standard procedures. Secure
88	88	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.1599421501159668 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1602020263671875 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request 0.36409711837768555 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF issued an identity request asking for the SUCI (Subscription Concealed Identifier). Notably, this identity request was sent in plain (unencrypted) form because the 5G-AKA authentication procedure had not yet been completed, which means that NAS security context (encryption and integrity protection) was not yet established. The UE responded by providing the requested identity (SUCI) in the subsequent uplink message. According to 3GPP 5G security standards, the SUCI is specifically designed to be a privacy-preserving, concealed identifier that can be safely transmitted in the clear, even before the establishment of encryption, to prevent exposure of the permanent subscriber identity (SUPI). Therefore, the UE's action in responding with the SUCI prior to NAS security activation is compliant with 3GPP security requirements and does not expose sensitive information. This means the UE acted securely within the context of the 5G standard for this phase of the authentication and identity procedure. 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 procedures and sent an Authentication Response to the AMF, but the 5G-AKA authentication process was not yet completed. Immediately after, the AMF sent an Identity Request asking for the SUCI, and the UE responded with an Identity Response. According to the 3GPP 5G security standards, messages containing sensitive information, such as the SUCI or SUPI, must be protected by NAS security, which is only established after the successful completion of the 5G-AKA authentication and key agreement. In this case, since the 5G-AKA was not completed, NAS security (encryption and integrity protection) was not yet in place, and the UE responded to a plain (unencrypted) Identity Request by sending its SUCI in plain text. This exposes the UE to potential interception and privacy risks, as the SUCI could be captured by an attacker on the radio interface. Therefore, the UE's action of sending the SUCI before NAS security was established is not compliant with 3GPP security requirements and is considered insecure. **Insecure**
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 the described test, after the UE sent an authentication response to the AMF, the AMF sent an identity request asking for the SUCI (Subscription Concealed Identifier). This identity request was transmitted in plain (unencrypted) form because the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security had not been activated. The UE responded with an identity response as requested. According to the 3GPP 5G standard (TS 33.501), before the completion of 5G-AKA and activation of NAS security, initial NAS messages—including identity requests and responses—are allowed to be sent in plain text. Importantly, the SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) during transmission, even when sent in the clear, by using public key cryptography to conceal the SUPI. As such, the UE's action of providing the SUCI in response to a plain identity request before NAS security activation aligns with the security expectations and procedures defined by the standard. Therefore, the UE's behavior is secure in this scenario. 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 the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a typical step for accessing network services. In response, the AMF sent a deregistration request, which was integrity protected and ciphered, indicating that NAS security had been activated as per standard 3GPP requirements. The deregistration request from the AMF indicated that the UE was considered "Illegal UE." Upon receiving this, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G NAS protocol specifications (TS 24.501), upon receipt of a protected NAS message that the UE cannot process due to invalid or missing mandatory information, the UE is expected to send a 5GMM status message to the AMF, reporting the error. The UE's response aligns with this requirement, as it did not process the deregistration request with invalid mandatory information but instead reported the protocol error in a secure, protected manner. This behavior ensures that the UE does not act on potentially malformed or malicious messages, maintaining the integrity and security of its operations as defined by the standard. Therefore, the UE's actions in this scenario are in compliance with the 3GPP security requirements for NAS message handling. Secure
92	92	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.7997009754180908 UE to AMF UplinkNASTransport, Service request 0.7998991012573242 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 1.0037281513214111 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was successfully completed, establishing a secure context for subsequent NAS messages. The UE then initiated a Service Request, which was sent to the AMF. In response, the AMF issued a Deregistration Request message, marked as both integrity protected and ciphered, indicating that it was sent using the established NAS security context. Upon receiving this protected deregistration command, the UE responded with a Deregistration Accept message, completing the deregistration process as specified in the 3GPP standards. According to 3GPP TS 24.501, after the security context is established via 5G-AKA, the UE is required to accept and process protected NAS messages from the network, including deregistration requests, and respond appropriately. Since the UE only responded to a deregistration request that was properly protected and did not accept or respond to any unprotected or suspicious messages, the UE's actions align with the security requirements of the 5G standard. This demonstrates that the UE acted securely by adhering to the expected protocol behavior and only processing messages that had the correct security protections in place. 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.	During the security test, after the completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating acceptance of the previously negotiated security parameters. However, the AMF then sent another "security mode command" message, this time protected, specifying the cipher algorithm 5G-EA4 and the integrity algorithm 5G-IA0 (null), with the security header indicating "integrity protected with new security context." Upon receiving this, the UE responded with a "security mode reject" message, citing "UE security capabilities mismatch" as the reason. According to the 3GPP 5G standard, the UE is required to verify that the security algorithms proposed by the network (AMF) do not exceed the UE's declared capabilities and that integrity protection is not disabled unless explicitly supported. In this scenario, the AMF selected the null integrity algorithm (5G-IA0), which may not be supported or allowed by the UE for the given context, especially if the UE does not permit disabling integrity protection after security context establishment. The UE's rejection of the security mode command due to a capabilities mismatch demonstrates that it correctly enforced its security policy and did not accept potentially insecure parameters. This behavior aligns with the 3GPP standard, which mandates that the UE must reject any security mode command that requests unsupported or unacceptable security algorithms. Therefore, the UE's action was secure. Secure
94	94	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00028896331787109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20491886138916016 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, the UE initiated a 5G standalone registration by sending an initial NAS registration request to the AMF. In response, the AMF issued an Identity Request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE then replied with an Identity Response containing the requested identity. Importantly, this exchange occurred before the completion of the 5G-AKA authentication procedure, meaning that NAS security (encryption and integrity protection) had not yet been established, and the messages—including the identity response—were sent in plain (unencrypted) format. According to the 3GPP 5G security standard, the UE is designed to send the SUCI (which is a privacy-preserving, encrypted form of the permanent identifier SUPI) in the clear prior to the establishment of NAS security, precisely to protect subscriber privacy even when NAS security is not yet active. The use of SUCI instead of the cleartext SUPI is a core enhancement in 5G to mitigate the risks of IMSI catchers and similar attacks. Since the UE provided only the SUCI as requested, and not the SUPI, and since this is compliant with the 3GPP standard for pre-authentication identity procedures, the UE's action was secure and in accordance with best practices for 5G network access. 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, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE initiated a Service Request, which is a normal step in the NAS communication. The AMF, under test control, responded with a Deregistration Request (UE terminated), a message type that, according to the 3GPP 5G NAS protocol, is only valid in certain protocol states and contexts. Notably, the Deregistration Request was sent with both integrity protection and ciphering, indicating that it was protected using the NAS security context established during 5G-AKA. The UE, upon receiving this protected Deregistration Request, responded with a Deregistration Accept message, thus following the protocol's expected behavior when such a request is received in a secure context. According to 3GPP TS 24.501, the UE is required to process protected NAS messages that are valid and respond accordingly; the security of the communication relies on the integrity and confidentiality provided by the NAS security context. Since the UE only accepted and processed the Deregistration Request after successful 5G-AKA and with proper NAS security protection in place, it did not violate any security expectations of the standard, even if the message type was unexpected in this state. The UE's actions demonstrate adherence to the security requirements of the 5G standard, as it did not accept or process any unprotected or unauthenticated NAS messages. Thus, the UE's behavior in this test was secure. 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) completed the initial NAS procedures and responded to an identity request from the Access and Mobility Management Function (AMF) by sending an Identity Response message. The AMF, under tester control, then sent another Identity Request, specifically requesting the SUCI (Subscription Concealed Identifier), and the UE responded again with an Identity Response. Notably, the 5G-AKA (Authentication and Key Agreement) procedure, which establishes NAS security and encryption, had not yet been completed at this point in the exchange. According to the 3GPP 5G standard, before 5G-AKA is finished, NAS messages—including identity requests and responses—are transmitted in plain (unencrypted) form, and the UE is required to comply with these requests. The SUCI is designed to be a privacy-preserving identifier, concealing the permanent subscriber identity (SUPI) even when transmitted over an unprotected channel. Therefore, the UE's behavior of responding to the plain identity request with a SUCI, prior to the establishment of NAS security, aligns with the 3GPP specifications and does not expose sensitive information. This means the UE's actions were secure and compliant with the standard. Secure

97	97	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03965497016906738 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0398409366607666 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24122309684753418 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initially responded to an identity request from the AMF by sending an identity response, after which the AMF, still prior to completing 5G-AKA authentication, sent a subsequent identity request for the SUCI (Subscription Concealed Identifier). The UE responded again with an identity response. As per the 3GPP 5G standard, before the completion of 5G-AKA, NAS messages—including identity requests and responses—are transmitted in plain (unencrypted) form, as there is not yet a shared key established between the UE and the network. The SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) from exposure, even over unprotected channels, by encrypting the SUPI with the home network's public key. Therefore, the UE's action—providing a SUCI in response to an identity request sent in plain text before AKA was completed—is in line with the 3GPP standard and does not expose sensitive information. The UE did not send its SUPI or any other unprotected permanent identifier, thus maintaining the intended level of security for this stage of the procedure. Based on this analysis, the UE's actions were secure according to the 5G standard. 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 completion of 5G-AKA (authentication and key agreement), the UE initiated a Service Request to the AMF, which is a standard procedure for resuming or establishing a session. The AMF then responded with a Configuration Update Command message, which was sent as a protected downlink message with integrity protection and a new security context, indicating that security activation had been completed and the message was properly secured according to 3GPP requirements. However, upon receiving this message, the UE responded with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to the 3GPP TS 24.501 standard, the UE is required to check the validity and compatibility of received NAS messages with its current protocol state; if an unexpected or out-of-sequence message is received, the UE should respond with a Status message indicating the incompatibility. This behavior helps prevent protocol confusion attacks and ensures that the UE does not process potentially harmful or out-of-context messages, thereby maintaining the integrity of the NAS layer. The UE's actions—rejecting the message as incompatible and sending a 5GMM Status—are in line with the security procedures outlined by 3GPP for robust protocol state management and error handling. Therefore, the UE's behavior was secure and correctly followed the 3GPP protocol for handling unexpected messages after security activation. Secure

99	99	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.5202081203460693 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204141139984131 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the User Equipment (UE) initiated an Uplink NAS Transport message to the AMF, specifically a PDU session establishment request. The AMF responded with a Downlink NAS Transport message containing a Service Accept, which was sent as a protected (encrypted and integrity protected) message. Notably, the UE did not respond to this protected Service Accept message from the AMF. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted to ensure confidentiality and authenticity. The AMF fulfilled this requirement by sending the Service Accept message as protected. The UE, however, failed to respond to this protected message, which is not compliant with 3GPP standards; the UE is expected to process protected messages after security activation. This lack of response could indicate that the UE did not properly recognize or process the protected NAS message, potentially exposing it to security risks such as replay or man-in-the-middle attacks if it were to accept unprotected messages instead. Therefore, based on the UE's actions in this interaction, the behavior is considered insecure according to the 5G standard. Insecure
100	100	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 92 UE provided: No response The packet capture during the test using wireshark is: 0.4685640335083008 UE to AMF UplinkNASTransport, Registration complete 0.4687800407409668 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Insufficient user-plane resources for the PDU session) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication and key agreement (indicating that security context was established and subsequent NAS messages should be integrity protected and ciphered), the UE sent a "registration complete" message to the AMF. The AMF then responded with a "gmm status" message, specifically indicating a 5GMM cause of 92 ("Insufficient user-plane resources for the PDU session"), and this message was sent as a protected (integrity protected and ciphered) NAS message. The UE, upon receiving this protected status message from the AMF, did not provide any further response. According to 3GPP TS 24.501, the "gmm status" message is used by the network to inform the UE of certain conditions or errors, and the standard specifies that, for most status causes, the UE is not required to respond to a protected status message unless the message indicates an error that requires corrective action or retransmission. Since the message was properly protected and the UE did not respond unnecessarily, the UE's behavior aligns with the expected and secure operation as defined by the 5G standard. The UE maintained the security context and did not leak information or respond inappropriately to a protected status message, thereby upholding the security requirements of 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 security test, after the successful completion of the 5G-AKA authentication procedure, the UE initiated an Uplink NAS Transport message to the AMF, specifically a PDU session establishment request. Following this, the AMF sent a Security Mode Command to the UE, which was properly protected using the negotiated security algorithms (ciphering with 128-5G-EA3 and integrity protection with 128-5G-IA2) and a new security context, as indicated by the security header. However, the UE did not provide any response to this Security Mode Command. According to the 3GPP 5G standard, once the Security Mode Command is received and verified as authentic and protected, the UE is required to respond with a Security Mode Complete message to confirm acceptance and activation of the new security context. The absence of any response from the UE is not compliant with the expected behavior and may indicate a failure to establish a secure NAS security context, potentially leaving the session vulnerable or incomplete. This lack of response could be interpreted as insecure handling of the security procedure, as it fails to confirm the mutual establishment of security between the UE and the AMF, which is critical for subsequent encrypted and integrity-protected communication. 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 the described test scenario, after the successful completion of 5G-AKA authentication, the UE sent a service request to the AMF. The AMF responded with a Security Mode Command, which was protected using the null cipher (5G-EA0) and null integrity (5G-IA0) algorithms, but with a security header indicating "Integrity protected with new security context (3)." Upon receiving this, the UE replied with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard (TS 24.501), after authentication, the Security Mode Command is used to establish ciphering and integrity protection for subsequent NAS messages. However, the use of 5G-EA0 and 5G-IA0 (null algorithms) means that no actual encryption or integrity protection is applied, which is only permitted in specific, restricted scenarios (such as emergency services or when explicitly configured). In normal operation, the UE should reject the Security Mode Command if null algorithms are proposed, as this exposes NAS signaling to potential interception and manipulation. The UE's response with a 5GMM status message indicating "Invalid mandatory information" suggests it detected the improper use of null algorithms and refused to proceed, which aligns with the security requirements of the standard. Therefore, the UE's action was secure as it did not accept unprotected communication after authentication. Secure
103	103	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5199828147888184 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5202269554138184 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message, specifically a PDU Session Establishment Request, to the AMF. The AMF then responded with a Deregistration Request message, which was integrity protected and ciphered, as indicated by the security header (2), meaning both encryption and integrity protection were applied according to 3GPP standards. Notably, upon receiving this protected deregistration request, the UE provided no response. According to the 3GPP 5G NAS protocol, when a UE receives a deregistration request that is properly protected (integrity protected and ciphered) after security context establishment (i.e., after 5G-AKA), it is required to process the request and respond appropriately (typically with a deregistration accept or a related message). The UE’s failure to respond to a valid, protected network-initiated deregistration request constitutes a deviation from expected secure behavior as defined by the standard, since it may leave the session in an inconsistent state or open to security risks such as denial of service or replay attacks. Therefore, the UE’s action in this scenario does not fully align with the secure handling of NAS procedures as specified by 3GPP. 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 security test, after the successful completion of the 5G-AKA authentication procedure, the User Equipment (UE) sent an Uplink NAS Transport message to the Access and Mobility Management Function (AMF), specifically a PDU session establishment request. In response, the AMF sent a Deregistration Request (UE terminated) message, which was integrity protected and ciphered, ensuring confidentiality and integrity as per 3GPP 5G security standards. The UE, upon receiving this protected deregistration request, did not respond further. According to 3GPP specifications, when a UE receives a deregistration request that is properly protected after a secure context has been established (i.e., after 5G-AKA), the UE should process the request, deregister, and not send any further NAS messages unless required (for example, a Deregistration Accept, which is optional for certain cases). The absence of a response from the UE in this context aligns with secure behavior, as it avoids unnecessary communication after a legitimate, protected deregistration instruction. Thus, the UE's actions demonstrate compliance with the expected secure behavior as per the 3GPP 5G standards. Secure
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 completing the 5G-AKA authentication and key agreement procedure, the User Equipment (UE) initiated an Uplink NAS Transport message, specifically a PDU session establishment request, to the Access and Mobility Management Function (AMF). Following this, the AMF responded with a Configuration Update Command, which, according to the packet capture and test summary, was sent as a protected message with both integrity protection and ciphering enabled (Security header type 2). The UE then replied with a Configuration Update Complete message. Since the 5G-AKA procedure was completed prior to these exchanges, the security context (including encryption and integrity keys) was already established. According to the 3GPP 5G NAS security specifications (TS 24.501), after successful authentication, all subsequent NAS signaling messages between the UE and the AMF must be integrity protected, and, where required, ciphered. The packet capture confirms that the Configuration Update Command from the AMF was indeed protected, and the UE responded appropriately within the secure context. Thus, the UE's actions were in line with 3GPP security requirements, as it only exchanged protected NAS messages after the security context was established. Secure

106	106	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7586648464202881 UE to AMF UplinkNASTransport, Service request 0.7588739395141602 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9626758098602295 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was integrity protected and indicated the use of the 5G-EA4 ciphering algorithm and 128-5G-IA3 integrity algorithm, with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing a "UE security capabilities mismatch." According to the 3GPP 5G standard, when the network proposes security algorithms in the Security Mode Command that the UE does not support or that do not match the UE's declared capabilities (as indicated earlier in the registration process), the UE is required to reject the command with an appropriate cause value, such as a capabilities mismatch. This behavior prevents the UE from accepting unsupported or potentially insecure security parameters, thereby protecting the integrity and confidentiality of the communication. The UE's action to reject the security mode command due to a mismatch is therefore consistent with the 3GPP security requirements and is considered a secure response. Secure
107	107	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.46604204177856445 UE to AMF UplinkNASTransport, Registration complete 0.466264009475708 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Restricted service area) 0.6700358390808105 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G Authentication and Key Agreement (5G-AKA) procedure, which establishes the necessary security context, the UE sent a "Registration Complete" message to the AMF. Subsequently, the AMF issued a "Deregistration Request (UE terminated)" message to the UE, which was transmitted with a security header indicating that it was both integrity protected and ciphered, as per security header type 2. The UE then responded with a "Deregistration Accept (UE terminated)" message. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA, all subsequent NAS signaling messages are expected to be integrity protected and ciphered, except for a few initial messages before security is established. In this interaction, the UE only responded to a protected deregistration request, and its actions aligned with the expected behavior—accepting a deregistration only after ensuring the message was properly secured. There is no indication that the UE accepted or acted upon any unprotected or insecure messages. Therefore, based on the outlined 5G standards and the observed message flow, the UE’s behavior was secure. Secure

108	108	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5200989246368408 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204448699951172 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7219538688659668 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test scenario, the 5G standalone User Equipment (UE) completed the 5G-AKA authentication, which establishes the security context necessary for encrypting and integrity-protecting NAS messages. Following this, the UE sent an Uplink NAS Transport message, and the AMF responded with a Configuration Update Command that was integrity protected using the new security context, as indicated by the security header. The UE, upon receiving this command, replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G standard, the UE is required to check the validity and compatibility of received NAS messages with its current protocol state. If it receives a message that is not compatible with its state, it should respond with a 5GMM Status message, as was done here. This behavior ensures that the UE does not process potentially invalid or malicious commands, thereby maintaining protocol integrity and adhering to security best practices. The UE's action of rejecting the incompatible message and notifying the AMF is in line with the 3GPP specifications and demonstrates secure handling of NAS messages after the security context is established. 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, the UE sent an Uplink NAS Transport message to the AMF, indicating that the NAS security context was established and subsequent NAS messages should be integrity protected and ciphered. The AMF, under test control, then sent a protected GMM Status message with a 5GMM Cause value of 98, which corresponds to "Message type not compatible with the protocol state." Upon receiving this, the UE responded with its own 5GMM Status message, echoing the cause and indicating that the received message type was not compatible with its current protocol state. According to 3GPP standards (TS 24.501), after NAS security is activated, all subsequent NAS messages must be integrity protected and, if required, ciphered. The UE's response—sending a status message in reply to an unexpected or invalid message type—is standard-compliant behavior, as it informs the network of protocol inconsistencies while maintaining security protections. Therefore, the UE's actions were consistent with the 3GPP security requirements, as it did not process or act upon an invalid message beyond reporting the error, and all communications were protected after 5G-AKA completion. Based on this analysis, the UE acted securely within the context 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 security test, after successfully completing the 5G-AKA authentication and security procedures, the User Equipment (UE) sent a "Registration Complete" message to the Access and Mobility Management Function (AMF), indicating that the initial NAS security context was established and all subsequent NAS messages should be protected (integrity protected and ciphered). The AMF then responded with a protected "GMM Status" message containing a 5GMM Cause value of 101 ("Message not compatible with the protocol state"). According to the 3GPP 5G standard (TS 24.501), upon receiving a protected GMM Status message with this cause, the UE is not required to respond, as it indicates that the received message is not compatible with its current protocol state. The UE's lack of response aligns with the standard's expectations, as responding to such a status message could expose it to unnecessary processing or potential security risks. Therefore, the UE's behavior in this interaction was secure and compliant with 3GPP specifications, as it did not react to an unexpected or protocol-incompatible message after security activation. Secure
111	111	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7300009727478027 UE to AMF UplinkNASTransport, Service request 0.7302379608154297 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9340109825134277 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message that was integrity protected and included the ciphering algorithm 5G-EA5 and the null integrity algorithm 5G-IA0. The UE then rejected the Security Mode Command, citing a "UE security capabilities mismatch." According to the 3GPP 5G standard (TS 24.501), the UE is required to verify that the security algorithms selected by the network are among those it supports and has indicated in its capability exchange. If there is a mismatch or the network selects algorithms not supported by the UE (for example, choosing null integrity protection, which may not be allowed by the UE's security policy), the UE must reject the Security Mode Command with an appropriate cause. This behavior prevents the establishment of a security context that does not meet the UE's security requirements, thereby protecting the UE from being forced into a potentially insecure state. Therefore, the UE's action of rejecting the Security Mode Command due to a security capabilities mismatch is in full compliance with the 5G standard and demonstrates secure behavior in this context. Secure

112	112	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7296979427337646 UE to AMF UplinkNASTransport, Service request 0.7299599647521973 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9337029457092285 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the negotiated ciphering (5G-EA5) and integrity (128-5G-IA2) algorithms, and indicated a new security context via the security header. Upon receiving this command, the UE responded with a Security Mode Reject message, specifying a "UE security capabilities mismatch." According to the 3GPP 5G standard (TS 24.501), the UE is required to verify that the security algorithms proposed by the AMF match its own capabilities, which were previously communicated during the registration or authentication phase. If there is a mismatch—meaning the AMF requests algorithms not supported by the UE—the standard dictates that the UE must reject the security mode command with the appropriate cause value, as seen here. This behavior is a critical security measure to prevent the use of unsupported or potentially weaker algorithms, thereby protecting the UE from downgrade or misconfiguration attacks. Therefore, the UE's action of rejecting the security mode command due to a capabilities mismatch strictly adheres to the 3GPP 5G security specifications and demonstrates a secure implementation of the protocol. 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 successfully completing the 5G-AKA procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the newly established security context, employing the 128-5G-EA1 ciphering algorithm and the 128-5G-IA2 integrity algorithm. The security header was set to indicate "integrity protected with new security context," as per 3GPP standards. Upon receiving this message, the UE rejected the security mode command, responding with a Security Mode Reject message and specifying the rejection cause as "unspecified." According to 3GPP TS 24.501, the UE is permitted to send a Security Mode Reject message if it detects an issue with the security mode command, including unsupported algorithms, mismatched security contexts, or other abnormal conditions; however, the use of the "unspecified" cause without a more detailed reason may indicate the UE either could not process the message or detected an anomaly. Since the UE did not proceed with establishing a potentially insecure or mismatched security context and instead chose to reject the request, it acted conservatively to protect itself against possible misconfiguration or security threats. This behavior aligns with the security principles of 3GPP, which allow the UE to reject security procedures if something is amiss, thus preventing exposure to insecure states. Therefore, the action taken by the UE in this scenario was secure. Secure
114	114	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5208940505981445 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215411186218262 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7234148979187012 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Configuration Update Command. The AMF's downlink message was protected, as indicated by the security header specifying integrity protection and ciphering (value 2), and the UE replied with a Configuration Update Complete message. According to the 3GPP 5G security architecture, NAS messages exchanged after the successful completion of 5G-AKA must be both integrity protected and ciphered to ensure confidentiality and integrity of signaling data. The packet capture confirms that the Configuration Update Command from the AMF to the UE was indeed sent as a protected message, and the UE responded as expected with a Configuration Update Complete. Since all NAS messages after authentication were properly protected and the UE did not process or respond to any unprotected or improperly secured messages, the UE's actions align with 3GPP security requirements for 5G standalone operation. Therefore, the UE's behavior in this test was secure. Secure

115	115	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 14.061744928359985 UE to AMF UplinkNASTransport, Service request 14.062045097351074 AMF to UE SACK (Ack=16, Arwnd=106496) , DownlinkNASTransport, Security mode command 14.26575493812561 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was correctly protected using the negotiated ciphering (5G-EA4) and integrity (128-5G-IA3) algorithms, and included a security header indicating "integrity protected with new security context," as per 3GPP standards. However, upon receiving this protected Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to 3GPP TS 24.501, upon receiving a Security Mode Command, the UE is expected to process it, verify the integrity and correctness of the message, and, if valid, respond with a Security Mode Complete message. If the message is invalid (e.g., missing mandatory IE), the UE may respond with a 5GMM status message indicating the error. In this test, the UE did not proceed with the security context establishment but instead reported an error. While this is a defined behavior for handling protocol errors, the key security concern is whether the UE accepted or applied a potentially malformed or malicious Security Mode Command. By refusing to proceed and reporting the error, the UE avoided establishing a potentially insecure context, which aligns with the security goals of the standard: to not accept invalid or tampered security configuration. Therefore, the UE's action of rejecting the invalid Security Mode Command and reporting the issue is considered secure behavior according to 3GPP specifications. Secure

116	116	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00d2 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.480457067489624 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48129701614379883 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.6844742298126221 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Security Mode Command. This Security Mode Command was sent as a protected message, indicating that it was integrity protected using the newly established security context, with the ciphering and integrity algorithms (128-5G-EA2 and 128-5G-IA2) specified. Upon receiving this, the UE responded with a Security Mode Reject message, citing an unspecified rejection cause. According to 3GPP 5G standards, the UE is expected to accept the Security Mode Command if the security context is valid and the message is properly protected; otherwise, in cases of integrity check failure, unsupported algorithms, or other security issues, the UE should reject the security mode procedure to prevent the establishment of an insecure connection. The fact that the UE rejected the Security Mode Command, especially with an unspecified cause, suggests that it detected something anomalous or potentially insecure in the received message or the context. This behavior aligns with the 3GPP security principle of "fail securely," meaning the UE should not proceed with potentially insecure communications. Therefore, the UE's action of rejecting the Security Mode Command, rather than accepting a potentially compromised or misconfigured security context, demonstrates secure behavior according to the 3GPP 5G security standards. Secure

117	117	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.5606789588928223 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5618300437927246 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described 5G standalone security test, the User Equipment (UE) successfully completed the 5G-AKA authentication procedure, after which it sent a UL NAS Transport message to the Access and Mobility Management Function (AMF). The AMF responded with a Security Mode Command message, which was sent as a protected (integrity protected and ciphered) NAS message using the newly established security context, specifically with cipher algorithm 5G-EA5 and integrity algorithm 128-5G-IA1. However, after receiving this message, the UE failed to provide any response. According to the 3GPP 5G security standards, once the Security Mode Command is received and successfully decrypted and verified, the UE is expected to respond with a Security Mode Complete message to confirm the establishment of the security context. The absence of any response from the UE, especially after the Security Mode Command was sent in a protected manner following a completed 5G-AKA, indicates a failure to proceed with the secure NAS signaling as specified by the standard. This could expose the UE to potential security vulnerabilities, such as denial of service or improper establishment of secure channels. Therefore, based on the 3GPP requirements and the observed behavior, the UE's action in this scenario was not secure. Insecure
118	118	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 6.6406471729278564 UE to AMF SACK (Ack=8, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 6.641204118728638 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Configuration update command 6.843037128448486 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, which establishes security keys for NAS message protection, the UE initiated an Uplink NAS Transport message to the AMF. In response, the AMF sent a Configuration Update Command, which was protected with both integrity protection and ciphering, as indicated by the security header value of 2. The UE then responded with a Configuration Update Complete message. According to 3GPP 5G standards (TS 24.501), once the 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected using the negotiated security context—specifically, with integrity protection and, where required, ciphering. The packet capture confirms that after 5G-AKA, the downlink Configuration Update Command from the AMF was indeed sent as protected, and the UE responded appropriately. The UE’s action of sending the Configuration Update Complete message after receiving a protected command, and within the expected security context, aligns with the 3GPP security requirements for NAS message protection. Therefore, the UE’s actions in this interaction were secure and compliant with the 5G standard. 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 and key agreement procedure, the UE sent a UL NAS Transport message to the AMF, initiating further NAS communication. The AMF then responded with a Security Mode Command message, which was protected and proposed the use of the 5G-EA0 ciphering algorithm (which provides no encryption) and the 128-5G-IA1 integrity algorithm. The Security Header Type indicated that the message was integrity protected with a new security context. Upon receiving this, the UE responded with a Security Mode Reject message, citing "Security mode rejected, unspecified" as the reason. According to the 3GPP 5G standard (TS 24.501 and related specifications), the use of 5G-EA0 (null ciphering) is only permitted in very specific situations (such as emergency services or when explicitly allowed by operator policy), and UEs are expected to reject Security Mode Commands that attempt to establish a security context with no encryption in normal circumstances. The UE's action to reject the security mode establishment when only null encryption was proposed aligns with the security requirements of the 5G standard, as it prevents the establishment of an insecure communication channel. Therefore, the UE's behavior in this test scenario was secure. Secure
120	120	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.46767306327819824 UE to AMF UplinkNASTransport, Registration complete 0.46790289878845215 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration complete" message to the AMF, which is the expected behavior after registering to the network. The AMF, under test control, then responded with a "Deregistration accept" message, which was sent as a protected (integrity protected and/or ciphered) NAS message. According to the 3GPP 5G standard (TS 24.501), the UE is required to process protected NAS messages only if they are valid and expected within the state machine of the protocol. In this case, since the UE had not initiated a deregistration procedure, it should not expect a "Deregistration accept" message from the network. The fact that the UE did not respond to this unsolicited and unexpected "Deregistration accept" message indicates that it correctly ignored an out-of-sequence or potentially malicious network command. This behavior aligns with the security requirements of 5G, which mandate that the UE should not process or act upon protected NAS messages that do not correspond to its current state or ongoing procedures, thereby preventing possible denial-of-service or session hijacking attacks. Therefore, based on the observed actions, the UE's behavior was secure according to the 3GPP 5G standard. Secure

121	121	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 1.719182014465332 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 1.7194299697875977 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) and the Access and Mobility Management Function (AMF) engaged in NAS communication. The UE, following the initial NAS procedures, sent an Authentication Response uplink message to the AMF before the 5G-AKA (Authentication and Key Agreement) procedure was completed. In response, the AMF sent a Service Reject message with a 5GMM Cause 111 ("Protocol error, unspecified") in plain (unencrypted) format. The UE did not provide any further response after receiving the Service Reject. According to the 3GPP 5G standard, NAS signaling messages sent before the completion of 5G-AKA (i.e., before security context establishment) are allowed to be sent and received in plain text, as encryption and integrity protection are not yet active. The critical security consideration at this stage is whether the UE, upon receiving a Service Reject in plain text prior to security activation, refrains from taking any further action that could compromise its security or privacy. In this case, the UE correctly did not respond to the Service Reject, adhering to the standard and not exposing itself to additional risk. Thus, the UE's behavior was compliant with 3GPP security requirements and did not introduce any security vulnerability in this scenario. Secure
122	122	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003769397735595703 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration procedure by sending an initial registration request to the AMF. The 5G-AKA (Authentication and Key Agreement) procedure, which establishes mutual authentication and security context for NAS message encryption and integrity protection, had not yet been completed at this stage. In response, the AMF sent a Service Reject message with 5GMM Cause 9 ("UE identity cannot be derived by the network") as a plain (unencrypted) NAS message, which is allowed by the 3GPP standard before security activation. The UE did not respond further after receiving this message. According to 3GPP TS 24.501 and TS 33.501, it is expected and secure for the UE to accept unprotected NAS messages before the completion of 5G-AKA, as security context is not yet established. The UE's lack of further response is also compliant, as it must not retransmit or proceed with registration after a Service Reject with cause 9. Therefore, the UE's actions were in line with 5G security procedures and did not expose any security weaknesses during this interaction. Secure

123	123	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.03993701934814453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04126906394958496 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24338102340698242 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE first responded to an identity request from the AMF by sending an identity response. Following this, the AMF sent a Security Mode Command, which was protected (integrity protected and ciphered) and indicated the use of new security context, specifying algorithms for ciphering (5G-EA4) and integrity (128-5G-IA1). However, at this stage, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, which means the necessary security keys for encryption and integrity protection were not yet established between the UE and the network. According to the 3GPP 5G standards, the Security Mode Command should only be sent after successful authentication, as the security context required for protecting NAS messages is established during 5G-AKA. Since the AMF sent a protected Security Mode Command before authentication was completed, the UE correctly identified this as a protocol violation and responded with a Security Mode Reject, specifying that the rejection was "unspecified" (as per standard behavior when the cause is not explicitly defined). This action by the UE prevents the establishment of a potentially insecure security context and mitigates the risk of accepting commands without proper authentication. Therefore, the UE's response was secure and in compliance with the 3GPP standard, as it refused to proceed with security mode setup before proper authentication and key establishment. Secure
124	124	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF exchanged NAS messages as part of the initial registration and identity verification procedures. The UE first sent an identity response to the AMF. Subsequently, the AMF, still before the completion of 5G-AKA (authentication and key agreement), sent another identity request for the SUCI (Subscription Concealed Identifier), and the UE responded accordingly. All these messages, including the identity response from the UE, were sent in the clear (plain), as the 5G-AKA procedure had not yet been completed and thus NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard, specifically TS 24.501, it is expected that certain NAS messages, such as initial registration and identity procedures, may be sent unprotected before authentication and security context establishment. However, the UE is expected to never send the cleartext SUPI (Subscription Permanent Identifier) before security activation, but it is permitted to send the SUCI, which is a privacy-preserving, concealed identifier, even in unprotected messages. In this scenario, the UE sent an identity response containing the SUCI in response to the AMF's identity request, which aligns with the 3GPP security requirements since the SUCI is specifically designed to be safe for transmission even before security is activated. Therefore, based on the actions taken by the UE—providing the SUCI in plain NAS messages before 5G-AKA is completed—the UE behaved in a manner that is secure and compliant with 3GPP standards. **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 registration by sending an initial registration request to the AMF. The AMF, controlled by the tester, responded with an Authentication Reject message sent in plain (unencrypted) form before the 5G-AKA authentication procedure was completed. According to the 3GPP 5G security standards, NAS message encryption and integrity protection are not established until after the successful completion of the 5G-AKA authentication and key agreement process. Therefore, it is expected and compliant with the standard for the UE to send and receive certain NAS messages, including Authentication Reject, in plain text prior to authentication. The UE, upon receiving the Authentication Reject, did not respond further, which is the correct behavior as specified by the 3GPP standards—the UE should cease further communication upon receiving this message since it indicates a failed or invalid authentication attempt. As such, the UE's actions were in line with 5G security protocols, and no sensitive user data was exposed or transmitted insecurely. Therefore, the UE's behavior in this scenario was secure. Secure
126	126	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5059909820556641 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5062329769134521 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7099969387054443 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test of a 5G standalone User Equipment (UE), the interaction began with the successful completion of the 5G-AKA authentication procedure, which establishes the security context necessary for subsequent NAS message encryption and integrity protection. After this, the UE sent a "registration complete" message, indicating the end of the registration process. The AMF, under test control, then sent a "deregistration request" message to the UE, which was properly protected with both integrity and ciphering, as shown by the security header (type 2). The UE responded appropriately with a "deregistration accept" message, indicating it processed the deregistration request and terminated its registration as instructed. According to 3GPP standards (TS 24.501), after security context establishment, sensitive NAS messages such as deregistration requests and responses must be integrity protected and ciphered to prevent tampering and eavesdropping. The UE’s actions—processing only protected messages after AKA completion and responding correctly to a legitimate, protected deregistration request—are in line with these security requirements. There is no evidence of the UE accepting unprotected messages or failing to comply with the security procedures specified by 3GPP. Therefore, the UE’s behavior in this test scenario adheres to the expected security standards for 5G NAS communication. Secure

127	127	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.03972792625427246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Identity Response message to the AMF, but the 5G-AKA authentication and key agreement procedure had not yet been completed. Immediately after receiving the Identity Response, the AMF sent a Deregistration Accept message to the UE in plain (unencrypted) form, which the UE received but did not respond to. According to 3GPP 5G security standards, NAS messages are only protected (encrypted and integrity protected) after successful completion of the 5G-AKA procedure, which establishes the necessary security context. Since the 5G-AKA was not completed, it is expected and compliant for both the UE and AMF to exchange messages in plain text at this stage. The UE's lack of response to the Deregistration Accept message is also in line with standard behavior, as the Deregistration Accept is a final message that does not require an acknowledgment from the UE. Therefore, the UE's actions in this interaction were consistent with 3GPP security requirements, and no security violation occurred during this exchange. 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 and the AMF completed the initial NAS steps, with the UE sending an identity response to the AMF. The AMF then issued an authentication request to the UE, but notably, this message was sent in plain (unencrypted) text and used all-zero values for both the RAND and AUTN fields, which are critical for the 5G-AKA authentication procedure. The UE, upon receiving this suspicious and non-standard authentication request, responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G security standards, the authentication request should contain valid, random RAND and properly constructed AUTN values, and the UE should only proceed with authentication if these fields are valid. By rejecting the malformed authentication request and not proceeding further, the UE demonstrated correct and secure behavior as per the 5G standard, preventing potential exploitation or unauthorized access attempts. Secure

129	129	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3100 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11980295181274414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12005805969238281 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.321152925491333 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was integrity protected and indicated the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm, along with a new security context. The UE responded to this by rejecting the Security Mode Command, providing a "Security mode rejected, unspecified" message to the AMF. According to the 3GPP 5G standards (specifically TS 33.501), after authentication, the UE and the network negotiate ciphering and integrity algorithms, and the use of the null ciphering algorithm (5G-EA0) is only permitted in exceptional circumstances, such as emergency services or when ciphering is not required. In normal operation, the UE should reject the use of 5G-EA0 to ensure user plane and NAS message confidentiality. In this test, the UE correctly identified the use of a null ciphering algorithm in a context where ciphering should be applied and securely rejected the Security Mode Command to prevent unencrypted communication. This behavior aligns with the security requirements outlined by 3GPP, ensuring that user data and signaling remain protected. Therefore, the UE's action was in accordance with the 5G standard and demonstrated secure behavior. 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 security test, after the initial NAS procedures, the UE responded to an identity request by sending an identity response to the AMF. The AMF then sent an authentication request message to the UE, but notably, this message was sent in plain (unencrypted) text, and the 5G-AKA authentication procedure had not yet been completed. Upon receiving this plain authentication request, the UE replied with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, specifically TS 33.501, the authentication and establishment of a secure NAS security context using 5G-AKA are mandatory before any sensitive or security-relevant NAS messages can be exchanged in an unencrypted manner. The UE is expected to reject any authentication procedure that does not conform to 5G security requirements, such as receiving a plain authentication request without an established security context, as this could expose it to interception or replay attacks. By refusing to proceed with the authentication in this insecure scenario, the UE demonstrated compliance with the 3GPP security guidelines and protected itself from potential threats. Therefore, the action taken by the UE was secure. Secure
131	131	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00038909912109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G NAS registration by sending an initial registration request to the AMF, which is standard procedure for establishing a connection in a 5G standalone network. The AMF, under test control, responded with a registration reject message, specifically with 5GMM Cause 26 ("Non-5G authentication unacceptable"), and sent this message in plain (unencrypted) form because the 5G-AKA authentication procedure had not yet been completed—meaning no security context or encryption keys had been established. According to 3GPP standards, NAS messages exchanged before successful authentication and key agreement (i.e., before 5G-AKA is completed) are allowed to be sent in plain text because the cryptographic context for securing these messages is not yet available. The UE, upon receiving the registration reject, did not respond further, which is the expected and secure behavior as per the standard, since it must not proceed with further NAS procedures without a valid security context. Thus, the UE's actions strictly adhered to the 3GPP security requirements for this phase of registration, and no sensitive information was exposed as the registration request does not contain credentials that require protection prior to authentication. Therefore, the UE's behavior in this test 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, the UE completed initial NAS procedures and sent an Identity Response message to the AMF, which was still in plain (unencrypted) form because the 5G-AKA authentication procedure had not yet been completed. The AMF, under test control, then sent a plain (unencrypted) Service Reject message with cause 99 ("Information element non-existent or not implemented"), after which the UE did not respond further. According to the 3GPP 5G standard (TS 24.501), until 5G-AKA is completed and security contexts are established, NAS messages—including Identity Response—are permitted to be sent in plain text. The UE is expected to process messages received in plain text during this pre-authentication phase. Upon receiving a Service Reject message before security activation, the UE is not required to respond further, as the session is effectively terminated. Given this, the UE's behavior—sending the expected plain Identity Response before authentication and not responding to the Service Reject—aligns with 3GPP security requirements and does not expose additional security risks, as encryption is not possible prior to 5G-AKA completion. Therefore, the UE's actions were in accordance with the 5G standard and did not compromise security in this context. 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 UE sent an Identity Response, the AMF issued an Authentication Request message to the UE. Notably, this Authentication Request was sent in plain (unencrypted) NAS, before the completion of the 5G-AKA procedure, which is required to establish a security context for protecting subsequent NAS messages. Upon receiving the plain Authentication Request, the UE responded with an Authentication Failure message, specifying the cause as "Non-5G authentication unacceptable." According to the 3GPP 5G standard (TS 24.501 and TS 33.501), the Authentication Request must be sent in plain NAS before security is established, but the authentication vectors (RAND, AUTN, etc.) must be generated according to the 5G-AKA procedure, and the UE must be able to recognize if the authentication mechanism is not 5G-AKA or if the context is not appropriate. The UE’s action to reject the authentication attempt as "Non-5G authentication unacceptable" demonstrates that it correctly detected an unacceptable or unsupported authentication method or context and refused to proceed without proper 5G security. This behavior aligns with 3GPP security requirements, as the UE must not accept authentication procedures that do not adhere to 5G security standards, thereby protecting itself from potential downgrade or replay attacks. Therefore, the UE’s response was appropriate and secure according to the 5G standard. 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, after the initial NAS procedures, the UE responded to an identity request by sending an identity response to the AMF, which is expected behavior during the registration process. At this point, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that the NAS security context (encryption and integrity protection) was not established. According to the 3GPP 5G standards, specifically TS 24.501, the identity response message from the UE is permitted to be sent in plain (unencrypted) form before the completion of 5G-AKA, as the cryptographic keys for securing NAS messages are not yet available. Subsequently, the AMF sent a service reject message with cause 3 ("Illegal UE"), also in plain text, which is again compliant with the standard at this stage of the procedure. The UE did not respond further, which is appropriate since it was rejected service. Throughout this exchange, the UE's actions were consistent with 3GPP security requirements, as it did not attempt to establish secure communications before the necessary authentication and key agreement were completed. Therefore, based on the 5G standard, the UE's behavior in this scenario was secure. Secure
135	135	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00067901611328125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.2038860321044922 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE initiated the registration procedure with the AMF, the AMF responded with a Security Mode Command message that was "protected" but specified the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, with the security header indicating "integrity protected with new security context." Importantly, the 5G-AKA authentication procedure, which is required to establish a security context and enable the use of encryption and integrity protection, had not yet been completed. As a result, the UE received a Security Mode Command instructing it to use no encryption and no integrity protection, which is not compliant with the 3GPP 5G security standards. According to 3GPP TS 33.501, the use of null algorithms (EA0/IA0) is only allowed under specific circumstances (e.g., for emergency services or when explicitly permitted by policy), and devices are expected to reject security mode commands that would result in unprotected NAS signaling in normal operation. The UE responded to this situation by rejecting the Security Mode Command with a "Security mode reject (unspecified)" message, indicating that it did not accept the insecure security configuration. This behavior aligns with the security expectations of the 3GPP standard, as it prevents the establishment of an unprotected or weakly protected signaling channel. Therefore, the UE's action was secure and compliant with the 5G security requirements. 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 and identity verification, the AMF sent a Security Mode Command to the UE, specifying the use of the null cipher algorithm (5G-EA0, meaning no encryption) and the 128-5G-IA3 integrity algorithm, with the security header indicating "integrity protected with new security context." Crucially, the 5G-AKA authentication procedure had not yet been completed, meaning that the keys necessary for establishing a secure context and enabling encryption and integrity protection were not yet derived or shared between the UE and the network. Upon receiving the Security Mode Command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standards, the UE should not accept a security mode command that proposes the null cipher (EA0) unless explicitly allowed by policy, and should also reject any security mode command if the 5G-AKA has not been completed, as this would mean secure keys are not in place to protect subsequent communication. The UE's action to reject the security mode command before AKA completion, especially when null encryption was proposed, aligns with the security requirements of the standard and prevents potential security vulnerabilities such as unprotected message transmission or key misuse. Therefore, the UE's behavior was in accordance with 3GPP security principles and protected the integrity and confidentiality of its communication. 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, after the initial NAS procedures, the UE sent an Authentication Response to the AMF, which is the expected behavior following an Authentication Request as per the 5G-AKA procedure. However, the AMF, under tester control, replied with another Authentication Request instead of proceeding to the Security Mode Command, which would indicate successful authentication and trigger the start of NAS message encryption and integrity protection. The UE, upon receiving this second plain (unencrypted) Authentication Request, responded again with another Authentication Response, still in plain text, as 5G-AKA was not yet completed and security context was not established. According to 3GPP 5G standards (TS 24.501, TS 33.501), the UE should only respond to repeated Authentication Requests if it determines that the previous authentication attempt was unsuccessful or if the AUTN/RAND values are different and valid. However, continuing to process and respond to repeated, potentially replayed, or manipulated Authentication Requests sent in plain text—especially after already providing a valid Authentication Response—can expose the UE to replay and downgrade attacks. Ideally, the UE should detect abnormal behavior (such as repeated authentication requests with the same or invalid parameters) and either ignore or reject further requests to avoid unnecessary exposure before security is activated. In this scenario, by continuing to respond to repeated plain Authentication Requests, the UE is not adhering to best security practices as outlined by 3GPP, making its actions potentially 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, the User Equipment (UE) completed the 5G-AKA authentication procedure, establishing a security context for subsequent NAS message protection. After sending a "Registration Complete" message to the AMF, the UE received a "Deregistration Request (UE terminated)" from the AMF. This downlink message was sent with the security header indicating both integrity protection and ciphering, confirming that the message was protected as per 3GPP requirements following successful authentication. The UE then responded with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to 3GPP standards (TS 24.501), after security context establishment, the UE must only process NAS messages that are integrity protected (and, where required, ciphered). Since the UE only responded to a deregistration request that was properly protected, and did not process or respond to any unprotected or insecure messages, its actions adhered to the expected security behavior. The UE did not accept or act upon any deregistration request that was not integrity protected and ciphered, which is critical to prevent security breaches such as unauthorized deregistration. Therefore, the UE's actions in this test demonstrate compliance with the 5G security requirements for NAS message handling after authentication. Secure

139	139	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 31303030000000007894d5bcdd550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00084686279296875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2040548324584961 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF then responded with an authentication request message, which was sent in plain (unencrypted) form, as the 5G-AKA procedure had not yet been completed and mutual authentication had not been established. The authentication request from the AMF included an ABBA value of 0000, a non-random RAND, and an AUTN of all zeros—values that do not conform to expected cryptographic standards for a legitimate authentication challenge. Upon receiving this invalid authentication request, the UE responded with a 5GMM status message indicating "Invalid mandatory information," rather than proceeding with authentication or sending sensitive information. According to the 3GPP 5G security standards, the UE is expected to validate the integrity and correctness of authentication parameters before responding, and should not proceed if the authentication challenge is malformed or suspicious. By refusing to process the invalid authentication request and instead reporting an error, the UE demonstrated correct and secure behavior as per the standard, preventing potential exploitation due to weak or missing authentication parameters. Secure

140	140	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 300068c66b7f000078b48472b0550000 AUTN: 300068c66b7f0000eeb58472b0550000 ngKSI_TSC: Native security context ngKSI_KSI: 1 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007758140563964844 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20353293418884277 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under your control, responded with an authentication request message sent in plain (unencrypted) format, as is standard before the completion of 5G-AKA authentication and key agreement. At this stage, per the 3GPP 5G standard, messages exchanged before the successful completion of authentication and security mode procedures are not required to be encrypted or integrity protected, because the necessary security context has not yet been established. However, instead of proceeding with the authentication challenge, the UE responded by sending a deregistration request (UE originating), effectively aborting the registration process. This action suggests that the UE either did not accept the authentication challenge or detected something abnormal and chose to discontinue the registration. According to 3GPP standards, it is acceptable for a UE to abort the registration process at any point before security is established, especially if it detects irregularities or for other implementation-specific reasons. The UE did not proceed to send any sensitive information or continue communication without security, and all messages up to this point were in line with expected pre-authentication behavior. Therefore, the UE's action to deregister at this stage does not expose it to security risks and adheres to 5G security requirements. Secure
141	141	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.17494893074035645 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.17513012886047363 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the User Equipment (UE) engaged in a 5G standalone NAS communication with the Access and Mobility Management Function (AMF). After completing the preliminary NAS procedures, the UE sent an authentication response to the AMF as part of the 5G-AKA authentication process. The AMF, under test control, replied with an authentication reject message, which was sent in plain (unencrypted) format. According to the 3GPP 5G standard, messages exchanged during the authentication phase (prior to the successful completion of 5G-AKA and establishment of NAS security) are transmitted without encryption, as the security context has not yet been established. The UE, upon receiving the authentication reject, provided no further response. This behavior aligns with the standard, which specifies that after receiving an authentication reject, the UE should not proceed with further NAS procedures and should not attempt to establish security or continue communication until a new authentication cycle is initiated. Therefore, the UE's actions—transmitting the authentication response in plain text before security activation and ceasing communication after receiving an authentication reject—are consistent with the 3GPP security requirements for this stage of the protocol. The UE did not behave insecurely or expose itself to additional risk within the defined protocol flow. Secure

142	142	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000ee95abdf8e550000 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.15996193885803223 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16019487380981445 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.3615410327911377 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF. Rather than proceeding with the expected 5G-AKA sequence, the AMF sent another authentication request to the UE, but crucially, this message was transmitted in plain (unencrypted) form, and the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards, the authentication and key agreement (AKA) procedure must be successfully completed before any sensitive NAS messages are exchanged in plain text, as this establishes the security context required for encryption and integrity protection. The UE, upon receiving a plain (unencrypted) authentication request after already responding, recognized that the authentication procedure was not being conducted according to 5G security requirements and replied with an "Authentication failure (Non-5G authentication unacceptable)" message. This indicates that the UE correctly identified that the authentication request was not secure, as it was not protected by the established 5G security context, and refused to proceed further. The UE's actions are consistent with the security requirements outlined in the 3GPP 5G standards, as it did not accept potentially insecure authentication procedures and protected itself from possible downgrade or replay attacks. Therefore, the UE's behavior in this scenario was secure. Secure
143	143	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5046439170837402 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 0.5048840045928955 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G User Equipment (UE) first completed the 5G-AKA authentication procedure, which is necessary to establish security keys for protected communication. Following this, the UE sent a "registration complete" message to the AMF, and subsequently, the AMF sent a "deregistration request" message to the UE. Importantly, the deregistration request from the AMF was sent with security protections: the security header indicates that the message was both integrity protected and ciphered, meaning it was encrypted and authenticated as per 3GPP 5G NAS security requirements. According to the packet capture, after receiving the protected deregistration request, the UE did not respond. According to the 3GPP 5G standard, a deregistration request from the network (AMF) must be integrity protected (and, if a security context exists, also ciphered). The UE should only process such a deregistration request if it is securely protected; otherwise, it should ignore or reject it to prevent denial-of-service or malicious deregistration attacks. In this test, since the deregistration request was properly protected and the UE chose not to respond (effectively ignoring the deregistration request), the UE's behavior aligns with a secure implementation—especially if the UE could not verify the authenticity or integrity of the message, or if it was an unexpected request. This cautious behavior helps prevent unauthorized or malicious deregistration. Thus, the UE's actions demonstrate adherence to secure communication principles as outlined by the 3GPP 5G standard. Secure

144	144	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5077369213104248 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080108642578125 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.7157459259033203 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had registered successfully. Following this, the AMF sent a "Configuration Update Command" to the UE, which 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. The packet capture confirms that the NAS security context was established before the exchange of configuration update messages, as the 5G-AKA procedure was already completed. According to the 3GPP 5G standards (TS 24.501 and related specifications), all subsequent NAS messages after the establishment of a security context (i.e., after 5G-AKA) must be both integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions align with this requirement: it only sent and responded to messages that were protected after the security context was established. There is no indication that the UE accepted or responded to any unprotected or insecure messages after 5G-AKA completion. Therefore, the UE's actions in this scenario adhered to the 5G security standards, ensuring secure NAS communication. 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, the 5G-AKA authentication procedure was completed first, establishing the necessary security context for protected NAS signaling. The UE then sent a Security Mode Complete message to the AMF, indicating that it had accepted the security algorithms and parameters provided earlier. However, after this, the AMF (under tester control) sent a new Security Mode Command, which the UE should have rejected or ignored, as per 3GPP TS 24.501 Section 5.4.3.4.1: once the UE has accepted and responded with Security Mode Complete, it should not accept or process a subsequent Security Mode Command with the same or new parameters unless a new security context is established. Despite this, the UE responded again with another Security Mode Complete message, which is not compliant with the 3GPP standard and could potentially allow a downgrade or replay attack, undermining the integrity of the NAS security procedures. This behavior indicates that the UE did not correctly enforce the state machine and security context checks required by the standard, and thus its actions were insecure in this scenario. Insecure

146	146	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.1601390838623047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037797927856445 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was successfully completed, which means that both the User Equipment (UE) and the Access and Mobility Management Function (AMF) had established mutual authentication and security keys for subsequent NAS message protection. After this, the UE sent a "security mode complete" message, indicating it had accepted the security parameters and was ready to communicate securely. The AMF then sent a "deregistration accept" message, which was protected (i.e., encrypted and integrity-protected) as indicated by the packet capture. The UE did not respond further, which is expected behavior after receiving a "deregistration accept" message, as this message indicates the conclusion of the deregistration process and that no further NAS interaction is necessary. According to the 3GPP 5G standard, it is crucial that all NAS messages following the completion of 5G-AKA and security mode command are protected using the established security context. In this scenario, the UE only sent messages after security was established and, upon receiving a protected deregistration accept, did not send any unprotected or unexpected messages. Therefore, the UE's actions adhered to the security requirements outlined by 3GPP and did not expose any vulnerability or deviation from the standard. 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 5G-AKA authentication, the UE sent a "security mode complete" message, indicating that it had accepted the negotiated security algorithms and was ready to use the new security context for NAS message protection. Following this, the AMF sent a "configuration update command" to the UE, which was properly protected (integrity protected with the new security context), as expected after security activation. The UE, upon receiving this message, 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, the UE must verify the protocol state before accepting certain messages. If the AMF sends a message that is not compatible with the current protocol state of the UE (for example, if a configuration update command is not expected in the current registration or connection state), the UE should respond with a status message indicating the incompatibility. This mechanism is a security and robustness feature to prevent protocol state confusion or attacks that could exploit unexpected message types. Therefore, the UE's action—rejecting the message with a status response—demonstrates correct and secure behavior as per the 3GPP standard, since it did not process an out-of-sequence or unexpected message, and all communication was protected with the agreed security context. Secure

148	148	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.11970210075378418 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.11996603012084961 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Congestion) 0.3268871307373047 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it had activated the negotiated security context for NAS signaling protection. The AMF then issued a deregistration request to the UE, which was integrity protected and ciphered, confirming that NAS security was indeed in place for this downlink message. The UE responded appropriately with a deregistration accept message, also under the established security context. According to the 3GPP 5G standards, specifically TS 24.501 and TS 33.501, after 5G-AKA and security mode command/complete, all subsequent NAS messages (including deregistration procedures) must be integrity protected and, if required, ciphered. The UE's actions—activating security upon completion of 5G-AKA, accepting only protected deregistration requests, and sending its own deregistration accept under security—are fully compliant with these requirements. Therefore, the UE's behavior in this scenario was secure, as it adhered to the security expectations of the 5G standard for NAS message protection and did not process any unprotected or suspicious requests. 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.	The interaction between the UE and the AMF during this 5G standalone security test began with the successful completion of the 5G-AKA authentication, which establishes security keys for subsequent NAS message protection. After this, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity protection). However, the AMF then sent a "security mode command" **after** receiving the "security mode complete" from the UE, which is a deviation from the expected 3GPP 5G NAS procedure. According to 3GPP standards, the security mode command should be sent **before** the security mode complete, as it instructs the UE to activate specific security algorithms, and only after receiving this command should the UE respond with a security mode complete. In this test, the UE, after already completing the security mode procedure, accepted and processed another security mode command from the AMF, which could potentially allow for a downgrade or replay attack if exploited by a malicious AMF. The UE should have rejected or ignored any subsequent security mode command once the security context was established and confirmed. This behavior indicates a protocol weakness, as the UE failed to enforce the correct state machine and sequence, potentially exposing itself to security risks. Therefore, based on the 3GPP standard and the observed behavior, the action taken by the UE was not secure. Insecure

150	150	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.16013693809509277 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16036486625671387 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.3618440628051758 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successful completion of the 5G Authentication and Key Agreement (5G-AKA), the User Equipment (UE) sent a "Security Mode Complete" message to the Access and Mobility Management Function (AMF), confirming that NAS security procedures (integrity protection and ciphering) were established. Subsequently, the AMF issued a "Deregistration Request (UE terminated)" message to the UE, which was protected with both integrity and ciphering, as indicated by the security header (value 2). The UE, upon receiving this protected deregistration request, replied with a "Deregistration Accept" message, thus properly following the deregistration procedure as per 3GPP 5G NAS protocol specifications. The key aspect here is that all critical NAS messages after the security mode procedure—including the deregistration request and accept—were exchanged under an established secure context (integrity protected and ciphered), ensuring confidentiality and authenticity. The UE did not process or respond to any unprotected NAS messages after security activation, which aligns with 3GPP requirements for mandatory protection of such messages post-authentication. Therefore, the UE's actions demonstrate adherence to the 5G security standards, and the communication can be considered secure. Secure
151	151	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00026297569274902344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an initial registration request to the AMF, the AMF responded with an identity request message, specifically asking for the GUTI (Globally Unique Temporary Identifier), and this message was sent in plain text since 5G-AKA authentication had not yet been completed. The UE did not respond to this identity request. According to the 3GPP 5G security standards, before the completion of the 5G-AKA authentication and key agreement, NAS messages are not yet encrypted or integrity protected, meaning any sensitive information sent at this stage could be exposed to interception. The 3GPP standards (TS 33.501) specify that the UE should not send permanent identifiers (such as SUPI or IMSI) in plain text, but responding with a GUTI (a temporary identifier) before security activation is generally considered acceptable because it is not a permanent or sensitive identifier. However, the UE in this test chose not to respond at all to the identity request for its GUTI before security activation. This cautious behavior exceeds the minimum requirements for security, as it avoids even sending the temporary identifier in the clear, thus minimizing the risk of tracking or exposure. Therefore, the action taken by the UE can be considered secure, as it did not expose any identifier before security activation, adhering to and even exceeding the 3GPP security recommendations. Secure

152	152	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated the NAS communication by sending an initial registration request to the AMF, which is a standard procedure for connecting to the 5G network. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that NAS security context (encryption and integrity protection) had not been established between the UE and the AMF. Despite this, the AMF sent a Configuration Update Command to the UE, and this message was marked as "Protected" with an "Unknown" security header. According to 3GPP 5G standards, the UE should not process or respond to NAS messages that are sent as protected (i.e., with security applied) before the completion of the authentication and key agreement process, because the necessary keys for encryption and integrity protection have not been established yet. The UE's action—providing no response to the protected Configuration Update Command—demonstrates correct and secure behavior, as it avoids processing messages that could not be properly validated or decrypted without a security context. This aligns with 3GPP security requirements, which are designed to prevent attacks such as replay or spoofing before mutual authentication and key setup. Therefore, the UE's action in this interaction was secure. Secure
153	153	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3200 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007700920104980469 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.20126700401306152 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated the registration process by sending an initial registration request to the AMF. The AMF responded with a Security Mode Command, which was protected using a security header indicating "Integrity protected with new security context" (type 3), and specified the use of ciphering algorithm 128-5G-EA3 and integrity algorithm 5G-IA0 (null integrity). However, at this point, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for encryption and integrity protection was not yet established. According to the 3GPP 5G standard, the UE should only accept a Security Mode Command that is integrity protected with a valid security context after 5G-AKA has been completed. Since the integrity algorithm specified was null (5G-IA0), no actual integrity protection was provided, and the message was sent as "protected" even though the security context was not yet valid. The UE responded with a 5GMM status message indicating "Invalid mandatory information," which is a correct behavior according to the standard when it receives a Security Mode Command that is not properly protected or is sent before the security context is established. This response by the UE prevents the establishment of a potentially insecure connection and demonstrates adherence to the security procedures defined by 3GPP. Therefore, the UE's actions in this scenario were secure and compliant with the 5G standard. 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, after the UE initiated registration by sending an initial registration request to the AMF, the AMF responded with a configuration update command that was protected using integrity protection and ciphering, as indicated by the security header. However, the 5G-AKA authentication and key agreement procedure, which is essential for establishing security context and deriving encryption/integrity keys, had not yet been completed at the time the configuration update command was sent. According to the 3GPP 5G standard, security protection (integrity and ciphering) for NAS messages is only permitted after the successful completion of 5G-AKA, ensuring that both the UE and network share the necessary keys. Since the UE had not yet completed 5G-AKA, it correctly did not respond to the protected configuration update command, as it would not have had the security context required to process or verify the protected message. Responding to such a message before security context establishment would be a violation of the standard and could expose the UE to security vulnerabilities. Therefore, the UE's action of not responding was in full compliance with 3GPP security procedures and protected it from potential attacks that might exploit premature security activation. 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, after the UE sent an initial registration request to the AMF, the AMF responded with a protected Deregistration Accept message before the 5G-AKA authentication and key agreement procedure had been completed. According to 3GPP 5G security standards, specifically TS 33.501, NAS message protection (integrity and encryption) can only be applied after security context establishment, which occurs as a result of successful completion of 5G-AKA. Since the 5G-AKA was not yet completed, the UE should not have accepted or processed any protected NAS messages, as it would not have the necessary keys to verify or decrypt them. In this test, the UE did not respond to the protected Deregistration Accept message sent by the AMF, which is the correct and secure behavior according to the standard. The UE's refusal to respond demonstrates that it does not process protected messages before security activation, thereby preventing potential security vulnerabilities such as message spoofing or replay attacks. 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, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF replied with a Security Mode Command, which was marked as "protected" and indicated the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, with the security header specifying "integrity protected with new security context." However, the critical step of 5G-AKA authentication had not yet been completed, meaning that no valid security context had been established between the UE and the network. Upon receiving the Security Mode Command with null algorithms and in the absence of completed 5G-AKA, the UE rejected the command by sending a Security Mode Reject message, citing an unspecified reason. According to the 3GPP 5G security standards, the UE is required to ensure that a proper security context is in place and to reject any attempt to establish security using null algorithms or without prior authentication, as this could expose the communication to security vulnerabilities. The UE's action to reject the security mode command in this scenario aligns with the expected secure behavior as outlined in the standards, preventing the establishment of an unprotected or weakly protected connection. Therefore, the UE acted securely in this interaction. Secure
157	157	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006291866302490234 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated NAS communication by sending an Initial Registration Request to the AMF, which is a standard procedure to start the registration process in 5G standalone networks. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is necessary for establishing mutual authentication and deriving the security keys for NAS message protection—the AMF responded with a Deregistration Request message that was both integrity protected and ciphered (as indicated by the security header type 2). According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must only be applied after successful completion of the authentication and security procedures (i.e., after 5G-AKA). Since the UE had not yet completed 5G-AKA, it would not have the necessary security context or keys to decrypt or verify the protected Deregistration Request. The UE's lack of response in this situation demonstrates correct and secure behavior, as processing or responding to protected NAS messages without an established security context would be a violation of the 3GPP security requirements and could expose the UE to security risks, such as replay or spoofing attacks. Therefore, the UE's action aligns with the 5G standard and demonstrates secure handling of the situation. 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 completing the initial NAS procedures but before the 5G-AKA authentication was completed, the UE sent an identity response to the AMF, after which the AMF issued another identity request, specifically requesting the IMEISV, in plain (unencrypted) NAS signaling. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), sensitive information such as IMEI or IMEISV should only be transmitted after NAS security (ciphering and integrity protection) is activated, which occurs after successful 5G-AKA authentication. Since the 5G-AKA procedure was not completed, the NAS messages were unprotected, and the UE's refusal to send the IMEISV in plain text is in line with the security requirements of the 5G standard. This behavior prevents potential exposure of sensitive device identifiers in unprotected signaling, thereby protecting user privacy and device security. Therefore, the UE's action—refusing to respond to the IMEISV request in plain NAS before security activation—demonstrates secure and standards-compliant behavior. Secure
159	159	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 13 UE provided: No response The packet capture during the test using wireshark is: 0.03987693786621094 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04032492637634277 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Roaming not allowed in this tracking area) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures up to the point of sending an Identity Response message to the AMF, after which the AMF replied with a GMM Status message indicating "Roaming not allowed in this tracking area" (5GMM Cause 13). Importantly, this downlink GMM Status message was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning no security context was established. According to the 3GPP 5G standard, before the completion of 5G-AKA, NAS messages between the UE and the AMF are permitted to be sent in plain text because encryption and integrity protection are only mandated after mutual authentication and key establishment. Upon receiving the plain GMM Status message, the UE did not respond, which is compliant with the standard: the UE is not required to respond to a GMM Status message, especially one indicating an error such as "Roaming not allowed." There is no indication that the UE accepted or acted upon any unauthorized or out-of-spec messages, nor did it proceed with any sensitive operations without security context. Therefore, the UE's action—sending the required Identity Response and then not responding further in the absence of a security context—aligns with 3GPP requirements for this phase of NAS communication and does not expose the UE to undue risk. Secure

160	160	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.038893938064575195 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039427995681762695 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF were engaged in NAS (Non-Access Stratum) communication as part of a 5G standalone security procedure. The UE sent an Identity Response uplink message to the AMF, after which the AMF sent a Configuration Update Command as a plain (unencrypted) NAS message, since the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed. According to 3GPP 5G standards, security protection for NAS messages (i.e., encryption and integrity protection) must not be applied until after the successful completion of 5G-AKA, when security contexts are established. Before this point, messages are exchanged in plain text. When the AMF sent the Configuration Update Command as a plain message prior to security activation, the UE did not respond. This is the correct and secure behavior, as per 3GPP standards, because the Configuration Update Command is a security-protected NAS procedure and should not be accepted or processed by the UE unless NAS security is active. Accepting such a message before security activation could expose the UE to security risks such as spoofing or manipulation. Therefore, the UE's lack of response demonstrates adherence to the 5G security requirements and proper handling of out-of-sequence or insecure messages. Secure
161	161	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0400080680847168 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04023408889770508 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) had not yet completed the 5G-AKA authentication and key agreement procedure, which is required by 3GPP standards to establish security context for encrypted and integrity-protected NAS communication. The UE sent an Identity Response message to the AMF, which is expected and typically occurs before authentication is completed. However, the AMF, under test control, responded with a Deregistration Accept message that was marked as "Protected" (i.e., it was integrity protected or encrypted), even though the security context had not yet been established because 5G-AKA was not completed. The UE, upon receiving this protected message before keys were in place, did not respond. According to the 3GPP 5G standard (TS 24.501), a UE must ignore or discard NAS messages that are protected (integrity protected or encrypted) before the security context is established through successful authentication (5G-AKA). By not responding to the protected Deregistration Accept message, the UE correctly followed the security procedures outlined in the standard, thereby preventing potential security vulnerabilities such as accepting unauthorized or spoofed protected messages prior to authentication. This action demonstrates that the UE's behavior was secure and compliant with 3GPP requirements. Secure

162	162	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.03969311714172363 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003500938415527 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed initial NAS steps and sent an Identity Response message to the AMF, after which the AMF replied with a Service Accept message that was protected (integrity protected and/or ciphered). However, crucially, the 5G-AKA authentication and key agreement procedure had not yet been completed at this point, which means that the necessary security context for NAS message encryption and integrity protection was not established. According to the 3GPP 5G standard (TS 24.501), the UE should only accept protected NAS messages (such as Service Accept) after the 5G-AKA procedure is completed and a security context is in place. Since the UE did not respond to the protected Service Accept message from the AMF, it indicates that the UE correctly rejected or ignored a protected NAS message before the establishment of security, thus adhering to the expected security behavior defined by the standard. This response from the UE prevents potential security vulnerabilities, such as accepting messages that could be spoofed or manipulated before mutual authentication and key establishment. Therefore, the UE's actions in this scenario were secure. Secure
163	163	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039769887924194336 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399930477142334 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF were engaged in NAS communication where, after the initial steps, the UE sent an Identity Response message to the AMF. Immediately following this, the AMF sent a Deregistration Request to the UE. Notably, the Deregistration Request was sent with integrity protection and ciphering enabled (security header type 2), despite the fact that the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G standard (TS 24.501), NAS message security (integrity protection and ciphering) must only be applied after successful completion of the 5G-AKA procedure and the establishment of NAS security context. Since the 5G-AKA was not completed, the UE would not have any valid NAS security context to decrypt or verify the security of the incoming message. The UE’s lack of response to the protected Deregistration Request indicates that it correctly rejected or ignored the message, as it could not be properly processed without the security context. This behavior aligns with the 3GPP specification, which states that UEs must discard protected messages if no security context has been established. Therefore, the UE’s actions in this scenario were secure and compliant with the 5G standard. Secure

164	164	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.03993701934814453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04126906394958496 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24338102340698242 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE completed the initial NAS steps and sent an identity response, the AMF responded with a Security Mode Command message that was integrity protected and indicated the use of new security context, specifying ciphering and integrity algorithms, and including an ABBA value. However, the 5G-AKA authentication procedure had not yet been completed, which means that the shared keys necessary to derive NAS security keys for encryption and integrity protection had not been established between the UE and the AMF. According to the 3GPP 5G standard, the Security Mode Command must only be sent after successful authentication (i.e., after 5G-AKA is completed), as this ensures that NAS security keys are available to both entities for secure communication. The UE correctly identified that the Security Mode Command was received prematurely—before key establishment—and responded by rejecting the command with a "Security mode rejected, unspecified" message. This behavior is compliant with the 3GPP standards and is considered a secure action, as the UE did not proceed with security procedures without a valid security context, thus preventing potential security vulnerabilities. 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 security test for a 5G standalone User Equipment (UE), the UE sent an authentication response to the AMF as part of the NAS procedures. Immediately after, the AMF sent a configuration update command to the UE, which was integrity protected but not encrypted, as 5G-AKA had not yet been completed. According to 3GPP 5G NAS security procedures, encryption and integrity protection of NAS messages must only be enabled after the successful completion of the 5G-AKA authentication procedure, which establishes security keys. Since the AMF sent a protected (integrity only) message before 5G-AKA was completed, and the UE did not respond to this message, the UE correctly refused to process a protected message before security context establishment. This behavior aligns with the 3GPP standard, as the UE must not accept or process integrity protected or encrypted NAS messages before authentication and key agreement have been completed. Therefore, the UE's action was secure and compliant with the 5G security requirements. Secure

167	167	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.07818889617919922 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.07842707633972168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE completed the initial NAS procedures and sent an authentication response, the AMF sent an identity request asking for the IMEISV. Notably, this identity request was sent in plain (unencrypted) NAS signaling, as the 5G-AKA authentication procedure had not yet been completed; thus, security context and ciphering were not established. According to the 3GPP 5G standard (TS 24.501), the UE must avoid exposing sensitive permanent identifiers such as IMEI or IMEISV over unprotected NAS signaling to prevent privacy risks like device tracking or unauthorized identification. The UE, in this case, did not respond to the AMF's plain (unencrypted) identity request for IMEISV, thereby refusing to disclose its permanent identity in an insecure manner. This action aligns with 3GPP security recommendations to protect user and device privacy before security activation. Therefore, the UE's behavior was secure and in accordance with the 5G standard. Secure
168	168	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.24675607681274414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.24697303771972656 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Service accept 0.4485650062561035 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE first sent an Authentication Response to the AMF, which is a step in the 5G-AKA authentication procedure. However, the 5G-AKA authentication was not completed, as indicated in the summary. Despite this, the AMF responded with a Service Accept message that was marked as "Protected," even though the necessary security context (which is established only after successful 5G-AKA) was not yet in place. The UE then proceeded to send a Deregistration Request. According to the 3GPP 5G security standards, NAS message protection (encryption and integrity) must only be enabled after the 5G-AKA procedure is fully completed and the security context is established. Since the UE acted on a Service Accept message that was "Protected" before authentication was completed and then sent a Deregistration Request, it indicates that the UE accepted a security-protected message before the secure context was valid. This is a security vulnerability because it allows for the possibility of unauthorized or manipulated messages being accepted outside the proper security context. Therefore, the UE's action of accepting and acting upon a protected message before successful authentication and security context establishment is not compliant with 3GPP security requirements 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 authentication process. However, before the authentication was completed, the AMF sent a GMM Status message with a cause value of 26 ("Non-5G authentication unacceptable") to the UE. Importantly, this GMM Status message was sent in plain (unencrypted) format, as the security context had not yet been established because the 5G-AKA process was not completed. According to the 3GPP 5G standard, the UE should not accept or act upon any plain NAS messages that are received after the authentication procedure has started but before security context establishment, except for very specific cases (e.g., certain status messages). The UE, in this case, did not respond to the plain GMM Status message from the AMF, which aligns with the security principle of not accepting or processing unprotected messages once the authentication phase has begun. This behavior prevents potential security risks such as replay or injection attacks by ensuring that only protected messages are processed after the start of authentication. Therefore, the UE's action was in accordance with the 3GPP security requirements. Secure
170	170	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11972379684448242 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999678611755371 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Authentication Response to the AMF, indicating that the 5G-AKA authentication process was still ongoing and not yet completed. Immediately after receiving the Authentication Response, the AMF sent a Deregistration Request to the UE, with the NAS security header indicating that the message was both integrity protected and ciphered. According to the 3GPP 5G security standard, NAS message protection (integrity and ciphering) should only be applied after the successful completion of the 5G-AKA procedure, which establishes the security context and keys required for encryption and integrity protection. Since the 5G-AKA was not completed, the UE had not yet derived the necessary security keys, and thus, it was not in a position to decrypt or verify the integrity of the protected Deregistration Request. The UE's lack of response to this protected message is consistent with the standard, as it should not process or respond to messages that are protected with security algorithms before a security context is established. Therefore, the UE's action—refusing to respond to a prematurely protected NAS message—demonstrates secure and standards-compliant behavior. 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 completion of the 5G-AKA authentication and security procedures, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (integrity and ciphering) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message for the IMEISV in plain (unencrypted) NAS, rather than within the established security context. 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, the UE is required to reject or ignore any subsequent plain NAS messages, as responding to such messages could expose sensitive information (like IMEISV) to interception or replay attacks. By refusing to respond to the unprotected identity request, the UE correctly adhered to the security requirements outlined in the standard, thus protecting its privacy and integrity. This behavior demonstrates that the UE's actions were secure and compliant with 3GPP specifications. Secure
172	172	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15984892845153809 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16009902954101562 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE in plain (unencrypted) format, requesting the UE's GUTI (Globally Unique Temporary Identifier). According to the 3GPP 5G standard (TS 24.501), once NAS security has been established (i.e., after "security mode complete"), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where possible, encrypted. The UE, upon receiving an unprotected (plain) identity request after NAS security activation, is expected not to respond, as replying to such a message would violate security procedures and potentially expose sensitive information. In this test, the UE did not respond to the plain identity request, which is the correct and secure behavior as per the standard, since responding could open the UE to security vulnerabilities such as identity disclosure attacks. Therefore, the UE's actions demonstrate compliance with 3GPP security requirements and maintain the integrity of the communication. Secure

173	173	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.15993309020996094 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16013097763061523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) 0.3612639904022217 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security should be activated and subsequent messages should be integrity protected and ciphered. However, the AMF responded with a Service Reject message that was sent in plain (unencrypted) format, using 5GMM Cause 111 (Protocol error, unspecified). Following this, the UE sent a Deregistration Request (UE originating) to the AMF. According to 3GPP standards, once security mode is complete, the UE expects all subsequent NAS messages from the network to be protected. If the UE receives a plain (unprotected) NAS message from the AMF after security activation, the standard requires the UE to treat this as a protocol error and initiate deregistration to protect itself from potential security threats, such as replay or man-in-the-middle attacks. In this test, the UE correctly responded to the unprotected Service Reject message by deregistering itself, as specified in the 3GPP TS 24.501 standard (section 5.4.3.4.3 and related security procedures). This demonstrates that the UE adhered to the security requirements and did not accept or process unprotected messages after security activation, thus maintaining the security of the communication. Secure
174	174	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: c2ada16de5afa04c9abbf0b2aba327aa AUTN: 3030303030303000ee55922b5d550000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.15995287895202637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016292572021484 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, 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 Security Mode Complete message, which indicates that it accepted the negotiated security algorithms and was ready to begin protected NAS communication. However, following this, the AMF sent an Authentication Request message to the UE, but this message was sent in plain (unencrypted) NAS, despite the fact that a security context should have already been established after the Security Mode Complete. According to the 3GPP 5G standard, once the security mode is established, all subsequent NAS messages (except for a few exceptions) must be integrity protected and, if required, encrypted. The UE, upon receiving an unprotected (plain) Authentication Request after security was established, did not respond. This behavior aligns with 3GPP security requirements, which state that the UE must ignore or discard any subsequent NAS messages that are not properly protected once a security context is active, to prevent downgrade or replay attacks. Therefore, the UE's refusal to respond to an insecure, unprotected message after security activation demonstrates correct and secure behavior according to the standard. Secure

175	175	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.15975189208984375 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15996503829956055 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated NAS security algorithms and that all subsequent NAS messages should be integrity protected and, where applicable, encrypted. However, the AMF then sent a "service accept" message in plain (unencrypted and non-integrity protected) form, and the UE did not respond to this message. According to 3GPP standards (specifically TS 24.501), after the security mode procedure is complete, the UE must expect all subsequent NAS messages from the network to be protected using the agreed security context. If the UE receives a plain NAS message after security activation, it should treat this as a protocol error and discard the message without processing it or responding. In this test, the UE's lack of response to the unprotected "service accept" message is consistent with the 3GPP security requirements, as accepting or responding to a plain message after security activation could expose the UE to security vulnerabilities such as replay or impersonation attacks. Therefore, the UE's actions were in line with the 5G standard and demonstrated secure behavior. Secure
176	176	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.47094106674194336 UE to AMF UplinkNASTransport, Registration complete 0.47116804122924805 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "registration complete" message to the AMF, indicating the end of the initial NAS security setup. Following this, the AMF sent an "identity request" message to the UE, requesting the SUCI (Subscription Concealed Identifier). Notably, this identity request was sent as a plain (unencrypted) NAS message, even though the security context had already been established via 5G-AKA. According to the 3GPP 5G security standards, once the NAS security context is established, all subsequent NAS messages, including identity requests, must be integrity protected and, where applicable, encrypted. The UE, upon receiving an unprotected (plain) identity request after security activation, did not respond. This behavior aligns with 3GPP security requirements, as responding to an unprotected identity request after security context establishment could expose sensitive information and make the UE vulnerable to various attacks, such as identity interception or replay attacks. By refusing to respond to an improperly protected message, the UE is upholding the security principles mandated by the 5G standard and protecting subscriber privacy. 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 the described interaction, after completing the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF. Subsequently, the AMF sent an "Authentication Request" as a plain (unencrypted) NAS message, despite the fact that the security context should have already been established after 5G-AKA. According to 3GPP standards (TS 24.501), once 5G-AKA is completed and a security context is in place, all subsequent NAS messages, including any authentication procedures, must be sent in an encrypted and integrity-protected manner. Upon receiving an unprotected authentication request after security activation, the UE is expected to reject or ignore the message to prevent downgrade or replay attacks. In this test, the UE did not respond to the unprotected authentication request, which indicates that it correctly refused to process a potentially insecure message, thereby adhering to the 3GPP security requirements. Therefore, the UE's action was secure. Secure
178	178	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 6.593172073364258 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.593342065811157 AMF to UE SACK (Ack=24, Arwnd=106401) , DownlinkNASTransport, Identity request 6.797163009643555 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF. Subsequently, the AMF sent an "Identity Request" asking for the SUCI (Subscription Concealed Identifier) from the UE, but crucially, this message was sent in plain (unencrypted) NAS signaling, even though 5G-AKA had already been completed and security context was established. Upon receiving this unprotected identity request, the UE did not respond with the requested identity; instead, it immediately initiated a "Deregistration Request (UE originating)" message. According to 3GPP TS 33.501, once 5G-AKA is completed and security context is established, all subsequent NAS messages, especially those carrying sensitive information such as identity requests, must be integrity protected and, where applicable, encrypted. The 3GPP standard also specifies that the UE should not respond to identity requests or other sensitive requests sent without proper NAS security after security activation; instead, it may choose to deregister or take other protective actions. The UE's behavior here—refusing to send its SUCI in response to an unprotected identity request and instead deregistering—demonstrates strict adherence to 5G security standards and best practices for protecting subscriber identity. This action prevents possible exposure of sensitive information over an insecure channel and mitigates the risk of identity interception or downgrade attacks. Therefore, the UE's actions in this scenario were secure and compliant with 3GPP requirements. Secure

179	179	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.265115976333618 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2653589248657227 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.469132900238037 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) completed the 5G-AKA authentication and sent a "registration complete" message to the AMF, indicating that the security context should be established and subsequent NAS messages should be integrity protected and, if required, encrypted. However, the AMF then sent a "configuration update command" as a plain (unencrypted and non-integrity protected) NAS message, as indicated by the security header value of 0. Upon receiving this unprotected message after security context establishment, the UE responded by sending a "deregistration request (UE originating)" to the AMF. According to the 3GPP 5G NAS security specifications (TS 24.501), after the successful completion of 5G-AKA, the UE is required to reject or ignore any subsequent NAS messages that are not integrity protected (i.e., sent as plain NAS), as this could indicate a security breach or protocol misbehavior. The UE's action of deregistering itself upon receiving a plain NAS message after security activation is a correct and secure response, as it prevents potential exploitation or downgrade attacks. Therefore, based on the 3GPP standard, the UE's behavior in this test was secure. 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 the 5G-AKA authentication procedure (which establishes NAS security context), the UE sent an UplinkNASTransport message to the AMF, after which the AMF responded with a Configuration Update Command. Notably, the Configuration Update Command from the AMF was sent as a plain (unencrypted and unauthenticated) NAS message, indicated by the Security Header value of 0. Following receipt of this plain message, the UE responded by sending a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G standard (TS 24.501), after the NAS security context is established (i.e., after 5G-AKA), all subsequent NAS signaling messages between the UE and AMF must be integrity protected and, if required, encrypted. The UE is expected to reject or ignore plain NAS messages that are received after security activation, as accepting or acting upon such messages would expose the UE to security vulnerabilities (such as replay or tampering attacks). In this test, the UE actively processed the plain Configuration Update Command and responded with a Deregistration Request, indicating that it accepted and acted upon an unauthenticated, unprotected NAS message after security was established. This behavior is non-compliant with 3GPP security requirements and exposes the UE to potential attacks. Therefore, the action taken by the UE was insecure. Insecure

181	181	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3100 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: No response The packet capture during the test using wireshark is: 2.4268798828125 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4271068572998047 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.42726993560791 AMF to UE DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, after the completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF responded with an Authentication Request message that was sent in plain (unencrypted) form, containing sensitive parameters such as ABBA, RAND, and AUTN. According to the 3GPP 5G standard, after successful completion of 5G-AKA, the UE and the network are expected to establish a security context, ensuring that further NAS messages are protected (encrypted and integrity-protected). The UE, upon receiving a plain (unencrypted) Authentication Request after security context establishment, did not respond. This behavior is in line with 3GPP security requirements, as the UE should reject or ignore NAS messages that are not properly protected after a security context is in place, to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to the insecure message demonstrates adherence to security best practices as defined by the 5G 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, 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, the 5G-AKA authentication procedure was completed, which means that both the UE and the AMF should have established security keys for NAS message integrity and confidentiality protection, as required by the 3GPP 5G standard. After the authentication, the UE sent a UL NAS Transport message, and the AMF responded with a Service Reject message. Notably, the Service Reject message from the AMF was sent in plain (unencrypted) text, with a 5GMM cause code 111 (“protocol error, unspecified”). The UE did not respond further to this message. According to 3GPP TS 24.501, once 5G-AKA is completed, the UE is mandated to send and expect NAS messages in a protected (integrity protected and, if required, ciphered) format. If the UE receives a downlink NAS message in plain text after security has been activated, it should ignore the message and not process it or respond, as processing unprotected messages after security activation would be a security vulnerability. In this test, the UE correctly ignored and did not respond to the unprotected (plain) Service Reject message sent by the AMF after security activation. Therefore, the UE's behavior was compliant with the 3GPP security requirements and did not expose itself to protocol downgrade or other security risks. Secure

183	183	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000eeb598a00f560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5556139945983887 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.555833101272583 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5559549331665039 AMF to UE DownlinkNASTransport, Authentication request 0.7596380710601807 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, after completing the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, which was followed by the AMF sending an Authentication Request message in plain (unencrypted) form. According to the 3GPP 5G standards, once 5G-AKA is completed, a security context is established and all subsequent NAS signaling messages between the UE and AMF must be protected with integrity and, where required, confidentiality (encryption). However, in this test, the AMF deliberately sent an unprotected (plain) Authentication Request after 5G-AKA completion. The UE, upon receiving this unexpected plain message, responded by initiating a Deregistration Request (UE originating), effectively terminating its connection rather than proceeding with the authentication or accepting further unprotected messages. This behavior aligns with the 3GPP security requirements, which specify that the UE must reject or terminate communication if it receives unprotected NAS messages after security has been activated, as this could indicate a security breach or downgrade attack. Therefore, the UE’s action demonstrates correct and secure behavior according to the standard, as it refused to process insecure messages after the security context was established. 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 the described test scenario, after the successful completion of 5G-AKA (which establishes security context and keys for encryption and integrity protection of NAS messages), 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 IMEI, and notably, this Identity Request was sent as a plain (unencrypted) message. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where confidentiality is required, also encrypted. When the UE received the plain Identity Request for IMEI, instead of responding with the requested identity, it initiated a Deregistration Request (UE originating). This response indicates that the UE refused to provide the IMEI in response to an improperly protected (plain) NAS message after security context was established, thereby adhering to the security requirements outlined by 3GPP. The UE's action demonstrates a secure behavior, as it did not expose sensitive information (IMEI) in response to an insecure request, and instead terminated the session as a precaution. 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, the 5G-AKA (Authentication and Key Agreement) procedure was completed between the UE and the AMF, establishing the necessary security context for subsequent NAS (Non-Access Stratum) communication. After authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Registration Reject message indicating "No network slices available" (5GMM Cause 62). Notably, the Registration Reject message from the AMF was sent in plain (unencrypted) text, and the UE did not respond further to this message. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA, all subsequent NAS messages, except for a limited set of exceptions (such as certain reject messages), must be integrity protected and, if possible, ciphered. The standard allows Registration Reject messages to be sent in plain text under specific circumstances, particularly if the network cannot derive security keys or if the UE is not authorized. However, in this case, since the 5G-AKA was completed and a security context should exist, the expectation is that the UE should only accept protected messages and ignore or discard unprotected (plain) messages where security is expected. The UE's action—providing no response to the plain Registration Reject message—aligns with the security requirements in the standard, as it helps prevent potential security attacks such as downgrade or spoofing, where an attacker could inject plain reject messages to disconnect the UE. Therefore, the UE's behavior was secure and compliant with the 3GPP standard. 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 successfully completing 5G-AKA authentication, the UE sent an Uplink NAS Transport message (PDU session establishment request) to the AMF. In response, the AMF sent a Security Mode Command message as a plain (unencrypted and unauthenticated) NAS message, even though the 5G-AKA procedure—which establishes the keys for NAS encryption and integrity protection—had already been completed. According to the 3GPP 5G standard (TS 24.501, TS 33.501), after 5G-AKA completion, the Security Mode Command is the first message that should be integrity protected (and optionally ciphered), but it is allowed to be sent as a plain message if security context is not yet activated. However, once the Security Mode Command is sent, the UE is expected to respond with a Security Mode Complete message, protected with the selected algorithms (in this case, 5G-EA6 for ciphering and 128-5G-IA1 for integrity). Instead, the UE did not respond to the Security Mode Command, and shortly after, it initiated a Deregistration Request to the AMF. This behavior indicates that the UE rejected the Security Mode Command, likely because it was received as a plain NAS message after 5G-AKA, which could be interpreted as a potential security risk or protocol violation (since an attacker could inject or replay such plain messages). By refusing to proceed and deregistering, the UE avoided establishing security with potentially compromised parameters and protected itself from a downgrade or injection attack. This aligns with the security principles outlined in 3GPP, where a UE should not accept or respond to unexpected plain NAS messages after authentication. Therefore, the UE's actions were in accordance with the 5G security standard and demonstrated secure behavior in this context. Secure
187	187	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 2.197134017944336 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 2.197467088699341 AMF to UE SACK (Ack=11, Arwnd=106334) , DownlinkNASTransport, Configuration update command 2.1975760459899902 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an uplink NAS transport message to the AMF. Subsequently, the AMF issued an identity request message to the UE, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version). Notably, this identity request message was sent as a plain (unencrypted) NAS message, even though the 5G-AKA procedure had already been completed, meaning NAS security (encryption and integrity protection) should have been activated. According to 3GPP standards (such as TS 33.501 and TS 24.501), after the 5G-AKA procedure, all subsequent NAS messages—especially those involving sensitive information such as the IMEISV—must be protected by NAS security. The UE, in this case, did not respond to the unprotected identity request. This behavior aligns with the 3GPP security requirements, as the UE is expected to ignore or reject requests for sensitive information such as the IMEISV if they are not protected by NAS security after authentication. Therefore, the UE’s action of not responding to an unprotected identity request after 5G-AKA completion is consistent with secure behavior as defined by the 3GPP standard. Secure

188	188	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.8423888683319092 gNB to AMF UEContextReleaseComplete, InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.8428249359130859 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was completed, which should have established security context for NAS message encryption and integrity protection between the UE and the AMF. After this, the UE sent a Service Request message, and the AMF responded with a Deregistration Accept message sent in plain (unencrypted) format. The UE did not respond to this plain message. According to the 3GPP 5G standard (TS 24.501), after successful authentication and security mode command (i.e., after 5G-AKA), all subsequent NAS messages must be integrity protected and, where applicable, encrypted. If the UE receives a NAS message after security is activated but finds it unprotected (e.g., in plain text), the UE must discard the message and not process it further, as processing unprotected NAS messages after security activation poses a security risk (such as spoofing or replay attacks). In this test, the UE correctly did not respond to the unprotected Deregistration Accept message, demonstrating compliance with 3GPP security requirements by refusing to process a plain NAS message after security establishment. Therefore, the action taken by the UE was secure according to the 5G standard. Secure
189	189	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.602246046066284 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.602970123291016 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a service request to the AMF. In response, the AMF issued a Security Mode Command message to the UE, but this message was sent as a plain (unencrypted and unauthenticated) 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 the completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF should be integrity protected and, if possible, ciphered, except for a few specific cases (such as the initial registration or when security is not yet established). The Security Mode Command is used to establish NAS security, but after 5G-AKA, the expectation is that the UE should only accept a Security Mode Command if it is integrity protected, to prevent downgrade or man-in-the-middle attacks. In this test, the UE did not respond to the plain Security Mode Command, which indicates that it correctly rejected an insecure request that did not meet 3GPP security requirements. This demonstrates that the UE adhered to the standard by refusing to proceed with insecure communication after authentication was completed. 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 completing the 5G-AKA procedure, the UE sent a service request to the AMF. In response, the AMF sent an Authentication Request message to the UE, but this message was sent in plain (unencrypted) form. The UE did not respond to this plain Authentication Request. According to the 3GPP 5G standard, after the security context is established via 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. The Authentication Request message being sent in plain text after 5G-AKA completion is a protocol violation by the AMF. The UE, by refusing to respond to an unprotected message after security context establishment, is following the 3GPP security requirements and protecting itself from potential security risks such as replay or interception attacks. Therefore, the UE's action—refusing to respond to a plain, unprotected message post-5G-AKA—is secure and compliant with 3GPP standards. 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 completing the 5G-AKA authentication, the UE initiated a service request to the AMF. The AMF, under test control, responded with an Authentication Request message that was sent in plain (unencrypted) text, despite the fact that a native security context was already established (ngKSI_TSC: Native, ngKSI_KSI: 4). Upon receiving this unexpected plain Authentication Request, the UE replied with an Authentication Failure message, specifically indicating "ngKSI already in use." According to the 3GPP 5G standards, after successful completion of 5G-AKA and establishment of a native security context, all subsequent NAS messages, including authentication requests, must be integrity protected and, where required, encrypted. The UE's detection of the reused ngKSI and its refusal to process the plain, unprotected Authentication Request is a secure behavior as per the standard, as it prevents potential replay or downgrade attacks and enforces the integrity and confidentiality requirements outlined by 3GPP. Therefore, the UE's actions demonstrate correct security compliance in this scenario. Secure
192	192	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 35.06067895889282 UE to AMF SACK (Ack=27, Arwnd=106496) , UplinkNASTransport, Service request 35.06101393699646 AMF to UE SACK (Ack=36, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the User Equipment (UE) sent a service request to the Access and Mobility Management Function (AMF). In response, the AMF issued an identity request for the TMSI (Temporary Mobile Subscriber Identity) in a plain (unencrypted) NAS message. Notably, the UE did not respond to this request. According to 3GPP 5G security standards, once 5G-AKA is completed, the NAS security context should be established, and subsequent NAS messages—especially those involving sensitive information like identity—must be encrypted and integrity protected. The AMF's decision to send an identity request in plain text after security activation is a protocol violation and could expose the UE to identity interception or replay attacks. The UE's refusal to respond to an unprotected identity request after 5G-AKA demonstrates compliance with the 3GPP security guidelines, as it prevents the potential leakage of sensitive information when the communication is not properly secured. Therefore, the UE's action in this scenario was secure and aligned with the 5G security requirements. Secure

193	193	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 9.49011492729187 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.490720987319946 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Service Request message to the AMF. The AMF responded with a Configuration Update Command, which was sent as a protected (secured) downlink NAS message. However, the UE did not respond to this message. According to the 3GPP 5G security standards, once 5G-AKA is completed, NAS signaling messages between the UE and the AMF must be integrity protected, and, where applicable, encrypted using the negotiated security context. The Configuration Update Command should be both integrity protected and, depending on the security policy, possibly encrypted. The UE is expected to process protected NAS messages and respond accordingly. The fact that the UE did not respond to the protected Configuration Update Command suggests that it either failed to process a valid, secured message or did not recognize the security header. This behavior is not compliant with 3GPP standards, as a standards-compliant UE should recognize and respond to protected NAS messages after security activation. Therefore, the action taken by the UE in this scenario is insecure. Insecure
194	194	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 18.81248188018799 UE to AMF UplinkNASTransport, Service request 18.8126699924469 AMF to UE SACK (Ack=18, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, after the successful completion of the 5G-AKA authentication procedure, the User Equipment (UE) initiated a service request to the Access and Mobility Management Function (AMF). In response, the AMF sent an "Authentication Reject" message to the UE in plain (unencrypted) form. According to the 3GPP 5G standards, once 5G-AKA is completed, both the UE and the AMF should have established security context, and all subsequent NAS messages—including service requests and authentication reject messages—should be protected with NAS security (i.e., encrypted and integrity protected). The UE, upon receiving an Authentication Reject message in plain text after security context is established, is expected to treat this as a potential security breach (e.g., a replay or downgrade attack) and should not respond further, as per 3GPP TS 24.501 specifications. In this test, the UE did not respond to the unprotected Authentication Reject message, which is the correct and secure behavior according to the standard, as it prevents possible exploitation or manipulation by unauthorized entities. Therefore, based on the described interaction and the 3GPP security requirements, the UE's action was secure. Secure

195	195_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 9.680989980697632 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.681249141693115 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Identity request 9.884641170501709 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G-AKA authentication procedure—which establishes mutual authentication and sets up NAS security keys—the UE sent a service request to the AMF. The AMF, under the test operator's control, responded with an identity request for the SUCI, but crucially, this message was sent in plain (unencrypted) NAS. The UE then responded with an identity response, also in plain NAS. According to the 3GPP 5G security specifications (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF are required to be integrity protected and, where confidentiality is needed, encrypted using the established NAS security context. The SUCI (Subscription Concealed Identifier) is specifically designed to protect the user's permanent identifier (SUPI) even if sent in plain, but after security context establishment, the expectation is that all NAS messages, including identity responses, should be protected. In this case, the UE accepted and responded to an unprotected identity request after the security context was in place, which is a deviation from the standard. The correct behavior would have been for the UE to reject or ignore the unprotected request, or at minimum, not respond with sensitive information in plain. Therefore, the action taken by the UE was insecure according to 3GPP standards. 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 UE sent a Service Request to the AMF, which is the expected behavior to initiate a new session or resume a suspended one. The AMF then responded with a Configuration Update Command, which was sent as a protected (i.e., integrity protected and/or ciphered) NAS message. However, the UE did not respond to this message. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages, including configuration updates, should be both integrity protected and ciphered. The fact that the AMF sent the Configuration Update Command as a protected message aligns with the standard. The UE's lack of response, however, is problematic. A compliant UE should be able to process protected NAS messages and respond appropriately, such as by sending a Configuration Update Complete message. Failure to respond could indicate that the UE did not recognize the security header or could not process the protected message, which may expose the device to potential security risks or protocol failures. This behavior suggests a deviation from the expected secure handling of NAS messages post-authentication and may indicate a security weakness in the UE's implementation. 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 registration by sending an Initial Registration Request to the AMF. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that a security context (for encryption and integrity protection of NAS messages) had not been established between the UE and the AMF. Despite this, the AMF responded with a Deregistration Request message that was protected with integrity and ciphering, as indicated by the security header (2: Integrity protected and ciphered). According to the 3GPP 5G security standards (TS 33.501), NAS message protection (integrity and ciphering) can only be applied after the successful completion of 5G-AKA and the establishment of a NAS security context. If the UE receives a protected NAS message before security context establishment, the standard dictates that the UE must discard the message and not respond, as it cannot verify the integrity or decrypt the message. In this test, the UE did not respond to the protected Deregistration Request, which aligns with the expected secure behavior as per 3GPP standards. This demonstrates that the UE correctly enforced the security requirements by refusing to process or respond to a protected message before security context was established. Secure
198	198	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15979790687561035 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16023778915405273 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message requesting the UE's GUTI, but this message was sent in plain (unencrypted) form rather than being protected by NAS security. The UE did not respond to this unprotected identity request. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (after security mode complete), the UE is required to only accept and respond to NAS messages that are integrity protected and, where required, encrypted. If the AMF sends a plain NAS message after security mode activation, the UE should ignore it and not respond, as responding could expose sensitive information and violate security procedures. Therefore, the UE's action of not responding to the plain identity request aligns with 3GPP security requirements and demonstrates secure behavior. Secure

199	199	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.1600339412689209 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602790355682373 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF completed the 5G-AKA procedure, which establishes mutual authentication and security keys for NAS message protection. After this, the UE sent a "security mode complete" message, indicating that it has agreed to the negotiated security algorithms and is ready to use NAS encryption and integrity protection for subsequent messages. However, the AMF then sent an "identity request" for the IMEISV as a plain (unencrypted and non-integrity-protected) message, even though the security context was already established. According to 3GPP standards (TS 24.501), after the security mode is complete, all subsequent NAS messages—including identity requests—must be protected using the agreed security algorithms. The UE, upon receiving a plain identity request after security activation, did not respond. This behavior aligns with the 3GPP security requirements, which dictate that a compliant UE must ignore or silently discard unprotected NAS messages after security activation to prevent potential identity disclosure or downgrade attacks. Therefore, the UE acted securely by refusing to respond to an improperly protected request, as per the 5G standard. 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 the described 5G standalone test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier). The UE did not respond to this plain identity request. According to the 3GPP 5G security standard (TS 33.501), after successful 5G-AKA and the establishment of NAS security, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if possible, encrypted. The SUCI is a privacy-sensitive identifier, and the 5G standard explicitly requires that such identifiers must not be sent in the clear after NAS security is established. By refusing to respond to an unprotected identity request after security activation, the UE is correctly adhering to the security requirements of the standard, thereby protecting the subscriber's identity and maintaining the integrity of the secure channel. Therefore, the UE's action in this scenario is secure. Secure

201	201	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.15867114067077637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15893101692199707 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure—which establishes a security context for NAS message encryption and integrity—the UE sent a "security mode complete" message, confirming that it had activated the negotiated security algorithms. Subsequently, the AMF sent an "identity request" message requesting the UE's IMEI; however, this message was sent in plain (unencrypted) NAS format, despite the security context having been established. According to the 3GPP 5G standards (TS 24.501), once the security context is set up (i.e., after 5G-AKA and security mode complete), all subsequent NAS messages—including identity requests—must be integrity protected and, where applicable, ciphered. The UE, upon receiving a plain (unencrypted) identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which mandates that the UE should ignore any NAS messages that are not integrity protected after security activation, as responding to such messages could expose sensitive information (such as IMEI) to potential interception or replay attacks. Therefore, the UE's action of not responding to the plain identity request was secure and in full compliance with the 5G security procedures. Secure
202	202	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.15091204643249512 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15117597579956055 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security (integrity and encryption) should now be activated for subsequent NAS messages. However, the AMF, under tester control, sent an Identity Request message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after Security Mode Complete), all subsequent NAS messages between the UE and AMF must be integrity protected and, where applicable, encrypted. The UE, recognizing that the Identity Request was sent in plain text after security activation, did not respond, thereby refusing to expose its identity in an insecure manner. This action is compliant with the 3GPP security requirements and protects the UE from potential identity exposure or downgrade attacks. Therefore, the UE's behavior in this scenario was secure and in line with the 5G standard. Secure

203	203	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15087509155273438 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15108299255371094 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message, indicating that NAS security had been established and future NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent an Identity Request message to the UE in plain (unencrypted) format, requesting the UE's GUTI. The UE did not respond to this message. According to the 3GPP 5G standard (TS 24.501), after NAS security is activated, the UE must only accept and respond to NAS messages that are properly protected; it should ignore or discard any subsequent plain (unencrypted) NAS messages to prevent potential security risks such as interception or spoofing. The UE's lack of response to the unprotected Identity Request demonstrates correct and secure behavior in compliance with the 5G standards, as it avoids exposing sensitive information over an unprotected channel after security activation. Therefore, the UE's action was secure. Secure
204	204	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15074801445007324 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15094995498657227 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described test scenario, after the successful completion of 5G-AKA authentication (which establishes the security context for NAS message encryption and integrity protection), the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure NAS communication. Subsequently, the AMF sent an "identity request" message to the UE, specifically requesting the IMEISV. Notably, this identity request was sent in plain (unencrypted) format, even though a security context was already established. According to the 3GPP 5G standard (TS 24.501, section 5.4.4.4), after the NAS security mode is established, all subsequent NAS messages (including identity requests) must be integrity protected and, if possible, encrypted. The UE, upon receiving an identity request in plain text after the security mode was established, correctly did not respond, as responding to such a request would expose sensitive information (IMEISV) over an unprotected channel and violate 3GPP security guidelines. This behavior demonstrates that the UE adhered to the security requirements by refusing to transmit sensitive information unless the request was properly protected. Therefore, the UE's action in this scenario was in line with the 5G security standards and can be considered secure. Secure

205	205	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4575481414794922 UE to AMF UplinkNASTransport, Registration complete 0.4577751159667969 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the NAS security context had been established and further NAS messages should be protected (i.e., integrity protected and encrypted). However, the AMF subsequently sent an "Identity Request" message requesting the SUCI from the UE, but this message was sent in plain (unencrypted and unprotected) form. The UE did not respond to this identity request. According to the 3GPP 5G standards (TS 24.501), after the NAS security context is established—signaled by the completion of 5G-AKA and the sending of "Registration Complete"—the UE must only accept further NAS messages that are integrity protected and, if required, encrypted. The UE is expected to ignore or silently discard any subsequent unprotected NAS messages, including identity requests, to prevent security vulnerabilities such as replay or impersonation attacks. Therefore, the UE's action of not responding to the unprotected identity request aligns with the security requirements of the 5G standard, demonstrating correct and secure behavior. Secure
206	206	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4691789150238037 UE to AMF UplinkNASTransport, Registration complete 0.46941208839416504 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and security procedures, the UE sent a "registration complete" message to the AMF. Subsequently, the AMF issued an "identity request" for the SUCI (Subscription Concealed Identifier) in a plain (unencrypted) NAS message. The UE, upon receiving this request, did not respond. According to the 3GPP 5G standard, after the security context is established (i.e., after 5G-AKA is completed), all subsequent NAS messages containing sensitive information—such as identity requests or responses—must be protected by NAS security (i.e., encrypted and integrity protected). The AMF's request for the SUCI in plain text after security activation is a protocol violation, as the SUCI is a privacy-sensitive identifier. The UE's refusal to respond to an unprotected identity request after security has been established demonstrates correct and secure behavior, as it avoids exposing sensitive information over an unprotected channel. Therefore, the UE's actions are in line with 3GPP security requirements and protect subscriber privacy against potential interception or replay attacks. 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 security test, after completing the 5G-AKA authentication procedure, the UE sent a "registration complete" message to the AMF, indicating that the initial NAS security context had been established. Following this, the AMF sent an "identity request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). Notably, the AMF sent this identity request as a plain (unencrypted) NAS message, even though 5G-AKA had already been completed, and thus NAS security (integrity and encryption) should have been activated for all subsequent NAS messages. The UE did not respond to this plain identity request. According to the 3GPP 5G standard (TS 24.501), once the security context is established after 5G-AKA, the UE is required to reject or ignore any unprotected (plain) NAS messages that require security, such as identity requests, to prevent potential security breaches like identity interception or replay attacks. By not responding to the plain identity request after security activation, the UE correctly adhered to the 3GPP security requirements, thereby protecting the subscriber's identity and maintaining the integrity of the communication. Therefore, the UE's action in this situation was secure. Secure
208	208	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4989509582519531 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.49918699264526367 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and security procedures, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context should be established and subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent an "Identity Request" message in plain (unencrypted) NAS format, requesting the SUCI (Subscription Concealed Identifier) from the UE. According to the 3GPP 5G security specifications (TS 33.501 and TS 24.501), once the 5G-AKA is completed and security is activated, the UE must expect all subsequent NAS messages to be integrity protected and ciphered. If the UE receives a plain (unencrypted) NAS message after security activation, it should treat it as a protocol error and must not respond with sensitive information such as the SUCI. In this test, the UE did not respond to the plain "Identity Request" message from the AMF, which aligns with 3GPP security requirements and prevents a potential security vulnerability where an attacker could trick the UE into revealing sensitive identifiers in plain text. Therefore, the UE's action was secure and compliant with the 5G standard. Secure

209	209	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48286890983581543 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48304104804992676 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G Authentication and Key Agreement (5G-AKA), the UE sent a "Registration Complete" message to the AMF, indicating that initial NAS security procedures—including mutual authentication and establishment of NAS security context—were 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 format. According to the 3GPP 5G standards (TS 24.501), after 5G-AKA and the establishment of the NAS security context, all subsequent NAS messages—especially those involving sensitive information like subscriber identity—must be protected (i.e., integrity protected and, where applicable, ciphered). The UE, upon receiving an unprotected (plain) Identity Request after NAS security was established, did not respond. This behavior is correct and secure as per the standard, since responding to a plain identity request after security context establishment could expose the subscriber's identity to interception or replay attacks. The UE's refusal to respond to an insecure request demonstrates adherence to 3GPP security requirements and proper protection of subscriber identity information. Secure
210	210	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48984408378601074 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4900491237640381 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the security context establishment process was finished and subsequent NAS messages should be protected. However, after this, the AMF sent an "Identity Request" message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501), once the 5G-AKA procedure is completed and security context is established, all subsequent NAS messages, especially those involving sensitive identifiers like SUCI, must be integrity protected and, where applicable, encrypted. The UE is required to ignore or silently discard any NAS messages received in plain format after security activation, as responding to unprotected requests could expose sensitive information or make the UE vulnerable to certain attacks (such as replay or man-in-the-middle attacks). The UE's action of not responding to the unprotected identity request aligns with these security requirements, as it prevents the disclosure of the SUCI over an unprotected channel. Therefore, the UE behaved securely in accordance with the 3GPP 5G standard. Secure

211	211	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 4.666033029556274 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 4.666288137435913 AMF to UE SACK (Ack=20, Arwnd=106429) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure—which establishes a security context and enables encryption for NAS messages—the UE sent a "Registration Complete" message to the AMF, signaling the end of the registration process. Subsequently, the AMF (under your control) sent an "Identity Request" message to the UE, specifically requesting the TMSI, but crucially, this message was sent in plain (unencrypted) text. According to the 3GPP 5G standard (TS 24.501), once a security context has been established (i.e., after 5G-AKA is completed), all subsequent NAS messages between the UE and the AMF should be integrity protected and, where applicable, encrypted. If the AMF sends a NAS message in plain text after security activation, the UE is expected to treat this as a protocol violation and should not respond to such messages, as responding could expose sensitive information and undermine the security guarantees of the 5G system. In this test, the UE did not respond to the unprotected "Identity Request" message, which is the correct and secure behavior as per 3GPP specifications, ensuring that sensitive information is not disclosed over an unprotected channel. Therefore, the UE's action in this scenario aligns with 5G security 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 5G-AKA (which establishes a security context for NAS message encryption and integrity protection), the UE sent a UL NAS Transport message to the AMF, followed by an AMF-initiated Identity Request for the IMEISV. Notably, the AMF sent this Identity Request as a plain (unencrypted) NAS message, even though the security context had already been established. According to the 3GPP 5G standard (TS 24.501), once the 5G-AKA procedure is completed, all subsequent NAS messages—especially those requesting sensitive information like IMEISV—must be sent with integrity protection and encryption enabled. The UE, recognizing that the Identity Request was sent in plain text after security was established, correctly did not respond to the request, as responding would risk exposing sensitive device information (IMEISV) in cleartext, which is a violation of the standard's security requirements. This behavior demonstrates that the UE adhered to the security guidelines set by 3GPP, refusing to transmit sensitive information unless the signaling is properly protected. Therefore, the UE's actions were secure and compliant with the 5G standard. Secure

213	213	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.7595288753509521 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.7598080635070801 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, following the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically a PDU session establishment request) to the AMF. In response, the AMF issued an Identity Request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. Notably, this Identity Request was sent as a plain (unencrypted) NAS message, despite the fact that 5G-AKA had already been completed, which means NAS security (encryption and integrity protection) should have been activated according to 3GPP standards. The UE, upon receiving this unprotected Identity Request post-authentication, did not respond. According to 3GPP TS 33.501 and TS 24.501, after the completion of 5G-AKA and establishment of NAS security context, the UE is required to ignore any NAS messages sent in plain (unencrypted) form, as accepting or responding to such messages could expose sensitive information or make the UE vulnerable to certain attacks (such as identity interception or replay attacks). Therefore, the UE's action of not responding to the plain Identity Request after NAS security was established aligns with the security requirements of the 5G standard and demonstrates correct, secure behavior in this context. Secure
214	214	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.7997701168060303 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.8000459671020508 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication 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 UL NAS Transport message, likely as part of a PDU session establishment request. Following this, the AMF sent an Identity Request message to the UE, specifically requesting the TMSI, and this message was sent in plain (unencrypted) NAS format. The UE, however, did not respond to this Identity Request. According to the 3GPP 5G standards, once 5G-AKA is complete and a security context is established, all subsequent NAS messages, especially those that could reveal subscriber identity (such as Identity Requests/Responses), must be protected by NAS security (i.e., encrypted and integrity protected). The AMF's decision to send an unprotected (plain) Identity Request after security setup is against the standard, and the UE's refusal to respond to such an insecure request is the correct and secure behavior as outlined by 3GPP. This prevents possible exposure of sensitive identity information over the air. Thus, the UE's action in this scenario was secure and compliant with the 5G standard. Secure

215	215	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.5246391296386719 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5248539447784424 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5249319076538086 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, indicating that security context establishment should have been completed and subsequent NAS messages should be protected (i.e., encrypted and integrity-protected). However, the AMF then sent an Identity Request message in plain (unencrypted) format, requesting the IMEISV from the UE. The UE did not respond to this request. According to the 3GPP 5G security standard (TS 33.501), once 5G-AKA is completed and the security context is established, the UE must only accept and respond to NAS messages that are integrity protected and, if required, encrypted. Plain (unencrypted and non-integrity protected) identity requests after security activation are considered a security risk, as they could be used for device tracking or information disclosure by a rogue AMF. By not responding to the plain Identity Request after security context was established, the UE acted in accordance with 3GPP security requirements and protected its sensitive information from potential exposure. Therefore, the UE's behavior in this scenario was secure. 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 completing the 5G-AKA authentication and key agreement, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message to the UE, requesting the SUCI (Subscription Concealed Identifier). Notably, this Identity Request was sent in plain (unencrypted) NAS, despite the 5G-AKA having been completed. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed and NAS security has been activated, all subsequent NAS messages, especially those carrying sensitive information such as identity requests and responses, must be protected (integrity protected and, where possible, encrypted). The UE, upon receiving an unprotected Identity Request after security activation, correctly did not respond, as responding in the clear would risk exposing sensitive identity information and violate 3GPP security requirements. The UE's refusal to reply to an unprotected identity request after security activation demonstrates adherence to the 5G security standard and a secure implementation. Secure

217	217	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.531268835067749 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5314879417419434 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5316059589385986 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, after the successful completion of the 5G-AKA authentication procedure (which establishes mutual authentication and security keys between the UE and the network), the UE sent a UL NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message to the UE, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version). Notably, the Identity Request was sent as a plain (unencrypted) NAS message, even though the 5G-AKA had already been completed and security keys were available. According to the 3GPP 5G security standard (TS 24.501, section 5.4.4.2), after the completion of 5G-AKA, all subsequent NAS messages, including identity requests and responses, must be integrity protected and, if possible, encrypted. The UE, in this test, did not respond to the plain (unencrypted) Identity Request message from the AMF. This behavior aligns with the 3GPP standard, which states that the UE should ignore identity requests sent in plain NAS after security context activation, to prevent potential security risks such as IMEISV disclosure to an attacker. Therefore, the UE's refusal to respond to an unprotected identity request after 5G-AKA demonstrates secure behavior in accordance with 3GPP requirements. Secure
218	218	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 13.027754783630371 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 13.028036832809448 AMF to UE SACK (Ack=11, Arwnd=106361) , DownlinkNASTransport, Configuration update command 13.02815294265747 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA procedure—which establishes mutual authentication and derives keys for NAS message encryption and integrity protection—the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message to the UE, specifically requesting the TMSI, and this message was sent in plain (unencrypted) text. Notably, the UE did not respond to this plain Identity Request. According to the 3GPP 5G security specifications, once 5G-AKA is complete, all subsequent NAS messages between the UE and the AMF must be integrity protected and, except for a few exceptions (such as Service Request in some cases), encrypted to protect user privacy and prevent sensitive information from being exposed over the air interface. The TMSI, while not as sensitive as the SUPI (IMSI), is still considered privacy-relevant information. The UE's refusal to respond to an unprotected (plain) Identity Request after security context establishment aligns with 3GPP security requirements, as responding would risk exposing the TMSI in clear text. Therefore, the UE's action in withholding its response to an unprotected identity request after AKA completion demonstrates correct and secure behavior according to the 5G standard. Secure

219	219	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.5992319583892822 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5994939804077148 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent an Identity Request message, specifically requesting the TMSI (Temporary Mobile Subscriber Identity), and this message was sent in plain (unencrypted) NAS. The UE did not respond to this request. According to the 3GPP 5G standard, after the successful completion of 5G-AKA, NAS security (encryption and integrity protection) should be activated for all subsequent NAS messages, except for a few specific scenarios (such as the initial registration before authentication). Identity Request messages sent in plain after security activation are considered a security risk, as they could expose sensitive identifiers to eavesdropping. The UE, by refusing to respond to an unprotected (plain) Identity Request after security activation, is acting in accordance with 3GPP security recommendations, which state that the UE should not send identifying information over unprotected NAS after security context establishment. Therefore, the UE's action was secure and compliant with the standard. Secure
220	220	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.6309528350830078 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.63124680519104 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (Authentication and Key Agreement), the UE sent a UL NAS Transport message to the AMF, which then responded with an Identity Request message requesting the TMSI (Temporary Mobile Subscriber Identity). Notably, this Identity Request was sent as a plain (unencrypted) message, despite the fact that the security context should have been established following the completion of 5G-AKA. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages—especially those requesting or containing sensitive subscriber identities—must be protected with NAS security (encryption and integrity protection). The UE, upon receiving a plain Identity Request after security activation, is expected to ignore or not respond to such messages, as responding could expose sensitive information and compromise user privacy. In this test, the UE did not respond to the unprotected Identity Request for TMSI, which aligns with the security requirements outlined by 3GPP. By refusing to respond to a plain (unencrypted) identity request after security activation, the UE demonstrated secure behavior in accordance with the 5G standard. 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 successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a service request message to the AMF, which is expected behavior as the next step in establishing a service. The AMF then responded with a service accept message, but crucially, this downlink message was sent in plain (unencrypted) form. According to the 3GPP 5G standard, specifically TS 33.501, after the completion of 5G-AKA, both the UE and the network must establish NAS security (encryption and integrity protection) before any further NAS messages are exchanged, except for a few explicitly allowed exceptions (such as initial registration or authentication messages). A service accept message is not among these exceptions and should be protected. The UE, upon receiving an unprotected (plain) service accept message after security context establishment, is required by the standard to discard the message and not respond, as a security measure to prevent downgrade or replay attacks. In this test, the UE did not respond to the unprotected service accept message, indicating that it correctly enforced the required security policy by refusing to process an insecure message. Therefore, the UE's action was compliant with the 3GPP standard and demonstrated secure behavior in this context. Secure
222	222	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 8.977952003479004 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.978222846984863 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA procedure (which establishes mutual authentication and derives security keys), the UE sent a service request to the AMF. The AMF responded with a service accept message, but crucially, this downlink message was sent in plain (unencrypted) text. According to 3GPP 5G standards, specifically TS 24.501, once the 5G-AKA procedure is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, ciphered (encrypted) to ensure confidentiality and integrity of the signaling. Upon receiving a plain (unencrypted) service accept message after authentication, a compliant UE should reject the message, ignore it, or otherwise not proceed with the session, as accepting such a message could expose the UE to security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected service accept message, which indicates that it did not accept or process the insecure message. This behavior is in line with the 3GPP security requirements, as the UE correctly refused to interact further when security was not properly applied. Secure

223	223	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 1.0053770542144775 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0059680938720703 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement (which establishes the security context for NAS signaling), the UE sent a Service Request message to the AMF. The AMF, controlled by the tester, responded with a Service Reject message, specifically indicating "UE identity cannot be derived by the network" (5GMM Cause: 9). Notably, this Service Reject message was sent in plain (unencrypted) NAS, despite the earlier completion of 5G-AKA, which should have enabled NAS security. According to 3GPP 5G standards (TS 24.501), after security mode is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. The UE, upon receiving a plain (unencrypted) Service Reject message after 5G-AKA, did not respond further. This behavior is compliant with 3GPP specifications, which state that the UE should ignore or discard NAS messages that are not integrity protected when a security context is active, as accepting such messages could expose the UE to security risks such as spoofing or denial-of-service attacks. Therefore, the UE’s lack of response to the unprotected Service Reject message demonstrates correct and secure behavior as per the 5G standard. Secure
224	224	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 0.9605340957641602 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.9612541198730469 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request message to the AMF, initiating a request for service. The AMF, under test control, responded with a service reject message indicating "UE identity cannot be derived by the network" (5GMM Cause 9). Importantly, this service reject was sent as a plain (unencrypted and unauthenticated) NAS message, 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 according to the 3GPP 5G standard (TS 24.501). The UE, upon receiving this plain service reject, did not respond, which is a critical point. According to 3GPP specifications, after NAS security is established, the UE must ignore any subsequent NAS messages that are not integrity protected, as accepting plain messages could expose the UE to security risks such as spoofing or denial-of-service attacks. The UE's lack of response to the plain (unsecured) service reject demonstrates proper adherence to the security requirements of the standard, as it did not process or act on an insecure message after security context was established. Therefore, the UE's action in this scenario was in line with 3GPP security guidelines and protected against potential attacks. Secure

225	225	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.7581770420074463 UE to AMF UplinkNASTransport, Service request 0.7587769031524658 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication and key agreement (which establishes security context for NAS message protection), the UE sent a Service Request to the AMF. In response, the AMF sent a Service Reject message with 5GMM Cause 111 (protocol error, unspecified), and crucially, this message was sent in plain (unencrypted and unauthenticated) format. According to the 3GPP 5G security standards (notably TS 24.501), once the 5G-AKA procedure is completed and a security context is established, all subsequent NAS messages, including Service Reject, must be integrity protected and, where required, ciphered. The UE, upon receiving a plain (unprotected) Service Reject message after security context activation, did not respond to this message. This behavior aligns with the 3GPP specification, which mandates that UEs must ignore any NAS messages that are not integrity protected when a security context is active, as this could otherwise expose the UE to various attacks such as spoofing or denial of service. Therefore, the UE's action—refusing to process or respond to an unprotected Service Reject after 5G-AKA—is compliant with the standard and demonstrates secure behavior in this context. Secure
226	226	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 21 UE provided: No response The packet capture during the test using wireshark is: 0.7632501125335693 UE to AMF UplinkNASTransport, Service request 0.7634460926055908 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Service reject (Synch failure) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement 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 service reject with the 5GMM cause value 21 (indicating "synchronization failure"), and notably, this downlink message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed, NAS signaling between the UE and the AMF should be integrity protected and, where possible, ciphered (encrypted). The UE, upon receiving a plain (unencrypted) NAS message after security context establishment, is expected to discard the message and not respond, as a security measure to prevent potential attacks such as replay or man-in-the-middle. In this test, the UE did not respond to the unprotected service reject message, which demonstrates compliance with the 3GPP security requirements and appropriate handling of potentially insecure messages. This behavior ensures that the UE does not act upon or acknowledge NAS messages that are not properly protected after security activation, thereby maintaining the integrity and confidentiality of its communications. Secure

227	227	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03d2 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.5453281402587891 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5457210540771484 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5461199283599854 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent a Security Mode Command to the UE, which was protected (i.e., integrity protected and/or encrypted) using the selected cipher (5G-EA6) and integrity (128-5G-IA2) algorithms, as per 3GPP standards. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G NAS protocol, after 5G-AKA, the AMF initiates NAS security procedures by sending a Security Mode Command, to which the UE must respond (typically with a Security Mode Complete message) to establish a secure NAS signalling context. The fact that the UE did not respond to the Security Mode Command indicates a failure to complete the NAS security setup. This is a deviation from the expected behavior defined by 3GPP, as the UE should always respond to the Security Mode Command to ensure secure communication. Not responding could leave the session in an insecure or undefined state, potentially exposing the UE or the network to security risks. Therefore, based on the 3GPP standard and the observed behavior, the action taken by the UE was insecure. Insecure

228	228	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00f2 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 2.722198963165283 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.7225029468536377 AMF to UE SACK (Ack=8, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.722743034362793 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure between the UE and the AMF, the UE sent an Uplink NAS Transport message, which is expected as part of normal NAS signaling. The AMF then responded with a Security Mode Command message, which is used to establish NAS security by selecting ciphering and integrity algorithms for protecting subsequent NAS messages. However, the Security Mode Command from the AMF was sent as "Protected" but specified both the ciphering algorithm (5G-EA0) and integrity algorithm (5G-IA0) as "null" (i.e., no encryption or integrity protection). The UE, upon receiving this message, did not respond. According to 3GPP standards, after 5G-AKA, the Security Mode Command should select strong ciphering and integrity algorithms (not null) to ensure the confidentiality and integrity of NAS signaling. The use of null algorithms is only permitted in specific, limited scenarios (such as emergency services or low capability devices), and even then, the UE should be able to recognize and handle such cases appropriately. In this test, the UE's lack of response to the Security Mode Command with null algorithms indicates that it did not proceed with an insecure configuration, thus protecting itself from operating without NAS security. This behavior aligns with secure 5G implementation practices, as the UE refused to engage in unprotected communication after authentication. 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 successfully completing the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is expected behavior for initiating further 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 security header value of 0 ("Plain NAS message"). According to the 3GPP 5G security specifications (such as TS 33.501), after 5G-AKA authentication and establishment of NAS security context, all subsequent NAS messages between the UE and the AMF must be integrity-protected and, when required, encrypted. The UE's action in this test was to provide no response to the plain (insecure) Configuration Update Command. This behavior is in line with the 3GPP standard, which mandates that the UE must discard any NAS messages received without integrity protection after security has been activated. By refusing to process or respond to an unauthenticated and unencrypted message post-authentication, the UE demonstrated secure behavior in accordance with the standard. Secure

230	230	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.6443009376525879 UE to AMF UplinkNASTransport, Registration complete 0.644589900970459 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command, Unknown code (0x31) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication, the UE sent a "registration complete" message to the AMF. Subsequently, the AMF responded with a "security mode command" message, which was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the "Plain NAS message (0)" security header. The UE did not respond to this security mode command. According to the 3GPP 5G standard, after successful authentication (5G-AKA), subsequent security-sensitive NAS messages, such as the security mode command, must be integrity protected and, if possible, encrypted. Sending the security mode command in plain text is a security risk because it could be intercepted or tampered with by an attacker. The UE, by refusing to respond to a plain (unprotected) security mode command after authentication, is adhering to the 3GPP security requirements and protecting itself from potential attacks, such as replay or man-in-the-middle attacks. Therefore, the UE's action of not responding to an insecure message is in accordance with the 5G security specification and demonstrates secure behavior. Secure

231	231	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3100 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.4284870624542236 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4289300441741943 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4293291568756104 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the User Equipment (UE) sent an Uplink NAS Transport message to the Access and Mobility Management Function (AMF). Subsequently, the AMF sent a Security Mode Command to the UE, but crucially, this command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), after the 5G-AKA procedure is completed, all subsequent NAS messages that are security-relevant—especially the Security Mode Command—should be integrity protected and, if possible, encrypted using the negotiated algorithms (in this case, 5G-EA6 for ciphering and 5G-IA5 for integrity protection). The fact that the AMF sent the Security Mode Command in plain text represents a deviation from the expected secure behavior. The UE, upon receiving this plain Security Mode Command after 5G-AKA, did not respond, which aligns with the 3GPP security requirements: the UE should ignore or reject such messages that are not properly protected, as responding to them could expose the UE to security risks such as replay or man-in-the-middle attacks. Therefore, by refusing to respond to an insecurely transmitted Security Mode Command, the UE demonstrated secure behavior in compliance with the 3GPP standard. Secure
232	232	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.7425761222839355 UE to AMF UplinkNASTransport, Service request 0.7428131103515625 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G-AKA authentication procedure, the User Equipment (UE) sent a Service Request message to the Access and Mobility Management Function (AMF). In response, the AMF sent an Authentication Reject message to the UE, and this message was transmitted in plain (unencrypted) form. According to the 3GPP 5G security standard, once 5G-AKA is completed, NAS security should be activated, and all subsequent NAS messages exchanged between the UE and AMF must be integrity protected and ciphered, except for a few specified cases (such as initial registration or messages prior to security activation). The Authentication Reject message sent after 5G-AKA completion should be protected, as the security context has already been established. The UE, upon receiving an unprotected (plain) Authentication Reject message after security activation, did not respond, effectively ignoring the message. This behavior aligns with the 3GPP standard, which requires the UE to discard any unprotected NAS messages received when a security context is active, in order to prevent security breaches such as downgrading or spoofing attacks. Therefore, the UE's action of not responding to the unprotected Authentication Reject message demonstrates adherence to the security requirements and is considered secure. Secure

233	233	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.7530779838562012 UE to AMF UplinkNASTransport, Service request 0.7533168792724609 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing 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 Authentication Reject message to the UE, and this downlink message was sent in plain (unencrypted) form. According to the 3GPP 5G standards, specifically TS 24.501, after successful completion of 5G-AKA, the UE and AMF should establish NAS security, and all subsequent NAS messages (except for a small set of exceptions such as some reject messages) must be integrity protected and, in most cases, also encrypted. However, the standard (see TS 24.501, section 8.2.6) explicitly allows certain messages, including Authentication Reject, to be sent without NAS security if the security context is not available or cannot be established. In this test, the UE, upon receiving an unprotected Authentication Reject message after 5G-AKA completion, did not respond further. This behavior is compliant with the 3GPP standard, as the UE is expected to cease NAS communication upon receiving an Authentication Reject, regardless of the security protection of the message. Therefore, the UE's action—providing no further response—aligns with the expected secure behavior as per 3GPP specifications. 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 security test of a 5G standalone User Equipment (UE), the UE completed the initial NAS procedures and sent an authentication response to the AMF. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet activated. The AMF then sent an identity request to the UE, requesting the TMSI, and this message was sent in plain (unencrypted) text, as expected before security activation. The UE did not respond to this identity request. According to the 3GPP 5G standards, before the completion of 5G-AKA, all NAS messages are sent in plain text, and the UE should be cautious when responding to identity requests in the clear, especially for sensitive identifiers. The UE's refusal to respond to a plain (unencrypted) identity request before the establishment of a secure NAS context aligns with security best practices to prevent exposure of sensitive information to potential attackers. This demonstrates that the UE is following the expected secure behavior as outlined in the standard, as it avoids revealing identifiers before security is in place. 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 completed the initial NAS steps and sent an authentication response to the AMF, the AMF sent an identity request for the IMEISV in plain (unencrypted) NAS message format because the 5G-AKA procedure had not yet been completed; this meant that security (integrity protection and ciphering) for NAS messages was not yet activated. The UE, upon receiving this plain identity request for the IMEISV, did not respond. According to the 3GPP 5G standards, particularly TS 24.501, a UE is expected to withhold sensitive information such as the IMEI or IMEISV if the request arrives before NAS security is established, specifically to prevent exposure of permanent or device-specific identifiers over an unprotected channel. The UE's lack of response to the unprotected identity request demonstrates correct and secure behavior, as it avoids potential privacy and security risks that could arise from sending the IMEISV in plain text. Therefore, the UE's action aligns with 3GPP security requirements and best practices for protecting device identity information during the NAS procedure. 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 security test, 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 to the UE, which is intended to establish NAS security (encryption and integrity protection) by activating the negotiated ciphering and integrity algorithms. However, the Security Mode Command message from the AMF was sent as a plain (unencrypted and unauthenticated) NAS message (indicated by security header type 0), which is permissible according to 3GPP standards since NAS security is not yet activated at this stage. Critically, after receiving the plain Security Mode Command, the UE responded with a Deregistration Request, but this message was also sent as a plain NAS message, without activating NAS security. According to 3GPP TS 24.501, after receiving and accepting the Security Mode Command, the UE is required to activate NAS security and send all subsequent NAS messages (including Deregistration Request) as integrity protected (and, if required, ciphered) messages. The fact that the UE sent the Deregistration Request in plain text, without NAS security, exposes the message to potential interception or tampering, which is a violation of the 5G security standard. Therefore, the UE's action of sending a plain Deregistration Request after security mode setup is considered insecure according to 3GPP specifications. 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 successfully completing the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then responded with a Security Mode Command. The Security Mode Command was protected, with the cipher algorithm set to 5G-EA5, but the integrity algorithm was set to 5G-IA0 (null), meaning no integrity protection was applied. The security header was reported as unknown, and critically, the UE did not respond to this Security Mode Command. According to 3GPP standards, after 5G-AKA, the Security Mode Command should establish both ciphering and integrity protection, and the use of 5G-IA0 (null integrity) is generally not allowed for NAS signaling due to the risk of replay or tampering attacks. The UE's lack of response to a Security Mode Command that does not provide integrity protection aligns with the standard's intent to prevent insecure security configurations from being accepted. Therefore, the UE acted securely by refusing to proceed with a configuration that could compromise security by allowing null integrity protection. 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 message to the AMF, and the AMF subsequently sent another Identity Request message, specifically requesting the TMSI, in plain (unencrypted) NAS. At this stage, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet activated. According to 3GPP standards (TS 24.501), before NAS security activation, the UE is permitted to respond to identity requests in plain NAS, but it must take care not to reveal sensitive permanent identifiers such as the SUPI (IMSI) in plain text. However, in this test, the AMF requested a less sensitive temporary identifier (TMSI), and the UE chose not to respond at all to the plain identity request. This behavior is in line with security best practices: by withholding any response until NAS security is activated, the UE avoids exposing even temporary identifiers over an unprotected channel, thus minimizing the risk of interception or tracking. This cautious approach aligns with the intent of 3GPP standards to protect user privacy and security before mutual authentication and key establishment. Therefore, the UE's action in not responding to the plain identity request is 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 UE and AMF engaged in NAS communication, where the UE initially sent an identity response, after which the AMF issued another identity request for the IMEISV (International Mobile Equipment Identity Software Version). Notably, this identity request was sent in plain (unencrypted) form because the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that NAS security context was not yet established. According to 3GPP 5G security standards, sensitive information such as the IMEISV should only be transmitted after NAS security is activated to prevent exposure of device identifiers over the air. The UE, upon receiving an unprotected identity request for the IMEISV prior to the completion of 5G-AKA, chose not to respond. This behavior aligns with 3GPP security recommendations, which state that the UE should not transmit permanent or sensitive identifiers in plain text before NAS security is established. By withholding its IMEISV in this context, the UE demonstrated secure and standards-compliant behavior, effectively protecting its identity from potential interception. 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 security test for a 5G standalone User Equipment (UE), the authentication phase (5G-AKA) was completed successfully, and the UE sent an authentication response to the Access and Mobility Management Function (AMF). Subsequently, the AMF sent a Security Mode Command to the UE, specifying ciphering and integrity algorithms (128-5G-EA3 and 128-5G-IA1), but crucially, the Security Mode Command was sent as a plain (unencrypted) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard, the Security Mode Command is always sent as a plain NAS message because it is used to establish the security context for subsequent encrypted communication. The UE, upon receiving the Security Mode Command in plain text, is expected to process it and respond with a Security Mode Complete message, which would be the first message sent with the negotiated security algorithms applied. However, in this test, the UE did not respond at all to the plain Security Mode Command. Since the Security Mode Command is required by the standard to be sent in the clear, the UE should have accepted and responded to it. By not responding, the UE failed to proceed with the security context establishment, which could indicate a non-compliance or a misconfiguration. However, from a security perspective, the UE did not expose any sensitive information or respond to a potentially insecure or unexpected message format; rather, it simply did not proceed. Therefore, the UE's action in this context did not compromise security, but it also did not fulfill the expected protocol behavior. Based strictly on the security aspect and not protocol completeness, the UE's action was secure, as it did not accept or process a message in an insecure manner. 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-AKA authentication procedure was completed successfully, establishing the necessary security context for subsequent NAS message protection. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms (ciphering: 5G-EA7, integrity: 128-5G-IA2). However, the AMF then sent another "security mode command" message to the UE, this time as a protected message, which is not the expected behavior per 3GPP standards. According to 3GPP TS 24.501, after the security mode procedure is completed and acknowledged by the "security mode complete" from the UE, the AMF should not send another "security mode command" unless a new security context needs to be established. The UE, in this case, did not respond to the unexpected protected "security mode command" message from the AMF. This behavior aligns with the 3GPP standard, which expects the UE to ignore unexpected or out-of-sequence security procedure messages, especially when they are protected and the security context has already been established. By not responding, the UE avoided potential security risks that could arise from replay or downgrade attacks. Therefore, the UE's action was secure and compliant with the 5G standard. 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 security test of a 5G standalone User Equipment (UE), the interaction began with the UE completing the 5G-AKA authentication procedure and sending an Authentication Response uplink message to the AMF. The AMF, under test control, then sent a Security Mode Command downlink message that was protected using the specified cipher (128-5G-EA1) and integrity (128-5G-IA2) algorithms, with the ABBA parameter set to 03f3. The test notes that the security header of the message was "Unknown," and crucially, the UE did not provide any response to the Security Mode Command. According to the 3GPP 5G standard, after the 5G-AKA procedure, the UE is expected to process the Security Mode Command, verify its integrity, and respond with a Security Mode Complete message if the command is valid and properly protected. The absence of any response from the UE, despite the command being sent with protection and after successful authentication, indicates that the UE either did not recognize the security header, could not process the protected message, or failed to handle the procedure correctly. This behavior is not compliant with the 3GPP standard, which expects the UE to respond appropriately to a valid Security Mode Command following authentication. The lack of response could expose the connection to potential security risks, such as denial of service or improper session establishment, and may indicate a flaw in the UE's implementation of the NAS security procedures. Therefore, based on the observed actions, the UE's behavior 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, the 5G-AKA authentication procedure between the UE and the AMF was successfully completed, as indicated by the UE sending an authentication response to the AMF. Following this, the AMF sent a Security Mode Command to the UE. However, the Security Mode Command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header being set to "Plain NAS message (0)." According to the 3GPP 5G standards (TS 24.501), after successful completion of 5G-AKA, the UE should expect that any subsequent Security Mode Command from the AMF be integrity protected (i.e., not sent as a plain message) to prevent potential security risks such as man-in-the-middle attacks. The UE, upon receiving a plain Security Mode Command after authentication, did not respond, which aligns with the security requirements of the standard: the UE should reject or ignore such insecure messages to prevent compromise of its security context. Therefore, the UE's lack of response indicates it acted securely and in compliance with 3GPP security guidelines. 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, the 5G-AKA authentication procedure was completed successfully, after which the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms and the start of NAS security (ciphering and integrity protection). However, the AMF then sent another "security mode command" message to the UE, but this message was sent as a plain (unencrypted and unauthenticated) NAS message, with the ciphering algorithm set to 5G-EA0 (null encryption) and the integrity algorithm set to 128-5G-IA2. According to the 3GPP 5G standard (TS 24.501), after the security mode command/complete exchange, all subsequent NAS messages must be protected according to the negotiated security context. The UE, upon receiving an unexpected and unprotected security mode command after security context establishment, did not respond. This behavior aligns with the 3GPP security requirements, as the UE must not accept or respond to unprotected NAS messages that could indicate a security downgrade or replay attack after security activation. By refusing to respond, the UE demonstrated secure behavior, protecting itself from potential security threats such as replay or downgrade attacks. 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.	During the test, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV (International Mobile Equipment Identity and Software Version). Notably, this identity request was sent as a plain (unencrypted) NAS message because the 5G-AKA authentication procedure had not yet been completed; thus, NAS security (encryption and integrity protection) was not active. The UE did not respond to this plain identity request. According to the 3GPP 5G standard, the UE should not disclose sensitive device identities such as the IMEI or IMEISV over unprotected (unencrypted) NAS messages to prevent potential interception and misuse by attackers. By refusing to respond to an unprotected identity request before the completion of 5G-AKA, the UE correctly protected its device identity information as per the security requirements of the standard. Therefore, the UE's action was secure. 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 security test, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the TMSI, but this request was sent in plain (unencrypted) form because the 5G-AKA authentication procedure had not yet been completed. According to 3GPP 5G security standards, sensitive information such as permanent or temporary identities should not be transmitted in plain text after the initial registration and before security context activation, as this exposes the UE to potential identity interception or replay attacks. The UE, upon receiving an unprotected (plain) identity request before the completion of 5G-AKA and the establishment of a secure NAS security context, chose not to respond. This behavior aligns with 3GPP security guidelines, which specify that the UE should not disclose its identity in cleartext when a secure context has not been established. Therefore, the UE's refusal to respond to the plain identity request demonstrates a secure and standards-compliant reaction to a potentially insecure situation. 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 initial NAS procedures, the UE sent an authentication response to the AMF, which then replied with an identity request for the IMEISV. Importantly, this identity request was sent as a plain (unencrypted) message because the 5G-AKA procedure had not yet been completed, and thus NAS security context had not been established. The UE did not respond to this plain identity request. According to the 3GPP 5G security standards (such as TS 33.501), the IMEISV is considered a sensitive identifier and should only be transmitted after NAS security has been activated (i.e., after 5G-AKA is completed and encryption is in place). By refusing to respond to a plain, unencrypted identity request for the IMEISV, the UE adhered to the security requirements of the 5G standard, protecting against exposure of sensitive information over an unprotected channel. Therefore, the UE's action in this scenario was secure and compliant with 3GPP guidelines. Secure

248	248	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA3 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.11875295639038086 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11905193328857422 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test of a 5G standalone User Equipment (UE), the NAS communication proceeded as follows: after completing the 5G-AKA authentication procedure, the UE sent an uplink authentication response to the AMF. Subsequently, the AMF sent a downlink Security Mode Command, which was indicated as "Protected" and used the cipher algorithm 128-5G-EA2 and integrity algorithm 128-5G-IA3. The ABBA value was 1111, and the security header was marked as "Unknown." Crucially, after receiving the Security Mode Command, the UE did not respond. According to the 3GPP 5G standard (TS 24.501), after successful authentication and upon receipt of a Security Mode Command, the UE is expected to verify the integrity and protection of the message, and only proceed if the message is valid and protected with the agreed algorithms. If the Security Mode Command is not properly protected or if the security header is unknown or invalid, the UE should not respond, as responding could expose it to security risks such as downgrade or replay attacks. In this test, since the Security Mode Command was marked as "Protected" but the security header was "Unknown," the UE's lack of response suggests that it detected an anomaly or invalid protection in the message and chose not to proceed, which is the correct and secure behavior according to the standard. Thus, the UE's action was in line with 3GPP security requirements, prioritizing the integrity and confidentiality of the communication. Secure
249	249	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.7274200916290283 UE to AMF UplinkNASTransport, Service request 0.7277319431304932 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the User Equipment (UE) and Access and Mobility Management Function (AMF) completed the 5G-AKA authentication process, which establishes security keys for subsequent NAS (Non-Access Stratum) message encryption and integrity protection. After authentication, the UE sent a Service Request to the AMF, which is the expected behavior. The AMF then responded with a Configuration Update Command; however, this message was sent as a plain (unencrypted and non-integrity-protected) NAS message, as indicated by the "Plain NAS message (0)" security header. According to the 3GPP 5G standard (TS 24.501), after completion of the 5G-AKA procedure and the establishment of NAS security, all subsequent NAS messages (except a very limited set of exceptions) must be sent with security protection (i.e., encrypted and/or integrity protected). The UE did not respond to this unprotected configuration update command. This behavior aligns with 3GPP requirements, as the UE is expected to discard or ignore any NAS messages received without security protection once NAS security is activated. Therefore, the UE's action of not responding to the plain (insecure) message demonstrates secure and standards-compliant behavior in this context. 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.	During the test, after the initial NAS procedures, the UE sent an identity response to the AMF. Subsequently, the AMF issued another identity request, specifically requesting the IMEISV, and this request was sent in plain (unencrypted) NAS signaling, as the 5G-AKA authentication procedure had not yet been completed. According to 3GPP 5G standards, sensitive information such as the IMEISV should only be transmitted after the NAS security context is established, which occurs after the successful completion of 5G-AKA. Since the UE did not respond to the AMF's plain (unencrypted) identity request for the IMEISV, the UE correctly refused to expose sensitive information before the establishment of a secure channel. This behavior aligns with 3GPP security recommendations, as sending the IMEISV in plain text prior to authentication and encryption would expose the UE to privacy risks, such as device tracking or interception of device identifiers. Therefore, the UE's action in withholding its IMEISV in response to an unprotected request demonstrates adherence to proper security procedures as outlined by the 5G 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 and the AMF engaged in NAS communication prior to the completion of the 5G-AKA authentication procedure, meaning that NAS security (encryption and integrity protection) had not yet been established. Following standard procedures, the UE sent an identity response to a previous request. However, after this, the AMF (under your control) sent another identity request message in plain (unencrypted) form, requesting the TMSI. The UE did not respond to this second, unprotected identity request. According to the 3GPP 5G standard, the UE must only respond to identity requests that are valid and expected within the protocol flow, especially before NAS security is established, as responding to unexpected or repeated plain identity requests could expose sensitive information (such as the TMSI or SUPI) to interception or replay attacks. By refusing to respond to the second, unsolicited, and unprotected identity request, the UE adhered to best security practices outlined by 3GPP, protecting itself from potential security vulnerabilities. Therefore, the UE's action in this scenario was secure. Secure

252	252	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03987598419189453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040084123611450195 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, presumably in reply to an earlier Identity Request. Following this, the AMF sent another Identity Request, this time specifically requesting the IMEISV, and crucially, this message was sent in plain (unencrypted) text because the 5G-AKA authentication and key agreement procedure had not yet been completed. The UE did not respond to this request. According to the 3GPP 5G specifications, sensitive information such as the IMEISV should not be transmitted in the clear before security (i.e., encryption and integrity protection) is activated, which only happens after successful completion of 5G-AKA. The UE's refusal to respond to a plain (unencrypted) Identity Request for the IMEISV before security was established aligns with the 3GPP security requirements and is considered a secure behavior. This prevents exposure of the IMEISV to potential eavesdroppers and demonstrates that the UE is properly enforcing security policies. 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 5G-AKA authentication, the UE initiated a Service Request to the AMF, which responded with an Identity Request for the GUTI (Globally Unique Temporary Identifier). Notably, the AMF sent this Identity Request message in plain (unencrypted) NAS, despite the fact that 5G-AKA had already been completed and security context should have been established. According to 3GPP standards (TS 24.501), after successful authentication and establishment of NAS security, all subsequent NAS messages—including identity requests—should be integrity protected and, if possible, encrypted. The UE, upon receiving an unprotected (plain) Identity Request after security context has been set up, is expected to treat this as a potential security threat (e.g., a replay or downgrade attack) and should not respond to such messages in plain. In this test, the UE did not respond to the unprotected Identity Request, which aligns with the security requirements and best practices defined by 3GPP for post-authentication NAS communication. By refusing to respond to a plain Identity Request after security setup, the UE effectively mitigates the risk of exposing sensitive information and prevents possible exploitation by unauthorized entities. Therefore, the UE's action in this scenario is compliant with 3GPP security standards 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 completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the security context should now be established. However, the AMF responded with a Service Accept message sent in plain (unencrypted and unauthenticated) NAS, rather than a protected message as required by the 3GPP 5G security specifications (TS 24.501, TS 33.501). According to the standard, after 5G-AKA is completed and security mode is activated, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, ciphered. The UE, upon receiving a plain (unprotected) NAS message after security activation, should ignore the message and not process it further, as processing such messages could expose the UE to various security threats such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected Service Accept message, indicating that it correctly identified the security violation and refused to process the message. This behavior aligns with the 3GPP security requirements and demonstrates that the UE maintained a secure posture by not accepting or responding to NAS messages that were not properly protected after security activation. Secure
255	255	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 12.160748958587646 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 12.161019086837769 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test scenario, after successfully completing the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which then responded with a plain (unencrypted) Identity Request asking for the UE's IMEI. According to the 3GPP 5G security standards, once the 5G-AKA procedure is completed, all subsequent NAS signaling messages, including identity requests, must be integrity protected and, where possible, encrypted to prevent sensitive information such as the IMEI from being exposed over the air. The UE, upon receiving an unprotected (plain) identity request for its IMEI after security context establishment, chose not to respond. This behavior aligns with 3GPP recommendations, which state that the UE should not transmit sensitive permanent identifiers, such as the IMEI, in plain text after security has been activated. By refusing to respond, the UE protected its sensitive identity information from potential interception or misuse. Therefore, the UE's action is consistent with 3GPP security requirements and demonstrates secure behavior in this context. 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.	During this 5G standalone security test, after a successful completion of the 5G-AKA authentication procedure, the User Equipment (UE) sent a "Registration Complete" NAS message to the AMF. The AMF then responded with a "5GMM Status" message, specifically indicating a cause value of 97 ("Message type non-existent or not implemented"), and crucially, this status message was sent in plain (unencrypted) format. According to 3GPP specifications (TS 24.501, section 5.4.5), once 5G-AKA is completed, all subsequent NAS messages—except for a very limited set of exceptions (such as certain security mode command failures or specific status messages in exceptional cases)—must be integrity protected and, where required, ciphered. The "Registration Complete" message from the UE was appropriately sent after security activation, but when the AMF sent an unprotected (plain) "5GMM Status" message, the UE did not respond. This behavior aligns with the 3GPP standard, which states that UEs must ignore unprotected messages that are received after security has been activated, except in narrowly defined circumstances. By not responding to the unprotected status message, the UE demonstrated correct and secure behavior as per the 5G security requirements, ensuring that it does not process or act upon potentially malicious or tampered messages. Secure
257	257	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4328169822692871 UE to AMF UplinkNASTransport, Registration complete 0.4330179691314697 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier). Notably, this downlink message from the AMF was sent in plain (unencrypted) form, even though the 5G-AKA had already been completed, which means that NAS security (encryption and integrity protection) should have been activated at this stage according to the 3GPP 5G standard (TS 24.501). The UE, upon receiving this unprotected identity request post-authentication, did not respond. This action aligns with 3GPP security guidelines, which state that after the security context is established (i.e., after 5G-AKA and NAS security mode command), the UE must ignore any unprotected NAS messages that require security, such as identity requests. Responding to an unprotected identity request in this context would risk exposing sensitive information. Therefore, by refusing to respond to the unprotected request, the UE demonstrated secure behavior in accordance with 3GPP standards. 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 the security test scenario, after the successful completion of 5G-AKA authentication and security setup, the UE sent a "Registration Complete" message to the AMF, followed by the AMF sending a deregistration request as a downlink NAS message. According to the packet capture, this deregistration request from the AMF was sent as a plain (unencrypted) message, but with a security header indicating "integrity protected and ciphered (2)", which suggests that the message should have been both integrity protected and encrypted. The UE subsequently responded with a deregistration request (UE originating). According to 3GPP 5G NAS security requirements (TS 24.501), after the establishment of the NAS security context (post-5G-AKA), all subsequent NAS messages, including deregistration requests, must be integrity protected and ciphered except for a few exceptions (such as initial registration and authentication messages). Since the AMF sent a deregistration request in plain text after security activation, the UE should have rejected or ignored this message, as accepting plain NAS messages after security activation could expose the UE to security risks such as replay or downgrade attacks. However, in this test, the UE accepted the plain deregistration request and responded accordingly, which is a deviation from the 3GPP standard and represents insecure behavior, as the UE should not process plain NAS messages after security has been established. Insecure
259	259	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 99 UE provided: No response The packet capture during the test using wireshark is: 0.5207638740539551 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.521324872970581 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Information element non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described security test, after the completion of 5G-AKA—which establishes mutual authentication and the keys necessary for NAS message encryption—the UE sent an Uplink NAS Transport message to the AMF. The AMF then responded with a GMM Status message, indicating a 5GMM Cause code 99 ("Information element non-existent or not implemented"), and crucially, this message was sent as plain (unencrypted) NAS. According to 3GPP standards (TS 24.501), after successful completion of 5G-AKA, all subsequent NAS messages between the UE and AMF must be integrity protected and encrypted, except for certain explicitly allowed exceptions (such as some security mode commands or status messages under specific conditions). However, when the AMF sends a plain (unencrypted) GMM Status message after security has been activated, the standard expects the UE to silently discard such messages and not respond, as processing unprotected messages post-authentication would be a security risk (to prevent downgrade or replay attacks). In this test, the UE did not respond to the unprotected GMM Status message, which aligns with the security requirements specified by 3GPP. Therefore, the UE's action of ignoring the unprotected message demonstrates secure behavior in accordance with the standard. 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 completion of 5G-AKA (authentication and key agreement), the UE sent a "registration complete" uplink NAS message to the AMF, which should have marked the transition into a secure NAS communication state, where messages between the UE and AMF are expected to be integrity protected and ciphered according to 3GPP standards. However, the AMF responded with a "gmm status" message (5GMM Cause: 101, indicating "Message not compatible with the protocol state") that was sent in plain (unencrypted and without integrity protection). Upon receiving this plain, out-of-spec message, the UE responded with a "deregistration request (UE originating)" message. According to 3GPP TS 24.501, after 5G-AKA is completed and security is activated, the UE must expect all subsequent NAS messages to be secured; reception of an unsecured NAS message in this state is considered a protocol violation and a potential security risk. The correct and secure behavior for the UE, as per 3GPP standards, is to abort the connection or deregister itself upon receiving such a message, as this may indicate a security attack (such as a downgrade or replay attack). In this test, the UE correctly detected the out-of-spec plain message and initiated deregistration, thereby protecting itself from potential security threats and following the standard-mandated procedure. Therefore, the UE's action was secure. Secure
261	261	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0101 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.7511579990386963 UE to AMF UplinkNASTransport, Service request 0.7514059543609619 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test of a 5G standalone User Equipment (UE), after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the Access and Mobility Management Function (AMF). In response, the AMF issued a Security Mode Command, which was observed to be sent as a protected (encrypted and integrity-protected) NAS message, utilizing the negotiated ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, with an ABBA value of 0101. The security header of the message was reported as "Unknown" in the test, and notably, the UE did not provide any response to this Security Mode Command. According to the 3GPP 5G standard, after the 5G-AKA is completed, the Service Request from the UE is expected, and the AMF should respond with a Security Mode Command to initiate NAS security context activation. The UE is required to process this command 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 that it failed to proceed with the security context establishment, which is a deviation from the 3GPP standard and leaves the session in an incomplete and potentially insecure state, as further communication cannot be securely protected without the UE's confirmation. Therefore, based on the interaction, the UE's action was insecure because it did not complete the necessary security procedure as required by the 3GPP 5G standard. 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 the described 5G standalone security test, the UE completed the 5G-AKA authentication procedure and then sent a service request to the AMF. In response, the AMF issued a Security Mode Command as a plain (unencrypted) NAS message, specifying the use of a null ciphering algorithm (5G-EA0) and an integrity algorithm (128-5G-IA2). The UE did not respond to this Security Mode Command. According to the 3GPP 5G security standards, after successful authentication, the NAS security context should be established, and subsequent critical NAS messages (such as the Security Mode Command) should be integrity protected and, where required, ciphered. Sending a Security Mode Command in plain text with a null ciphering algorithm is not secure and exposes the communication to possible interception and manipulation. The UE, by refusing to respond to such an insecure request, is following the security expectations set forth in the standard, as it should reject or ignore requests that do not meet the required security protections. Therefore, the UE's action of not responding is consistent with secure behavior as specified by 3GPP. 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 security test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent a Registration Reject message with 5GMM Cause 74 ("Temporarily not authorized for this SNPN"), and this message was sent in plain (unencrypted) form. The UE provided no response to this registration reject. According to the 3GPP 5G standard, after the completion of 5G-AKA, subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted. However, the Registration Reject message is one of the few exceptions allowed by the standard (see 3GPP TS 24.501, section 9.11.3.3), which states that certain messages, including Registration Reject, may be sent in plain NAS if the network cannot establish security context or chooses not to for specific causes. The UE, upon receiving a plain Registration Reject, is expected to accept it and not respond further, as per the standard. Therefore, the UE's action—sending an uplink NAS transport after 5G-AKA, receiving a plain Registration Reject, and then not responding—aligns with 3GPP security requirements. The UE did not exhibit any insecure behavior in this exchange. Secure

264	264	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 6 UE provided: No response The packet capture during the test using wireshark is: 2.427165985107422 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4275641441345215 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4278719425201416 AMF to UE DownlinkNASTransport, Registration reject (Illegal ME) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as NAS security (ciphering and integrity protection) should be activated following authentication. Subsequently, the AMF issued a Registration Reject message with cause "6" (Illegal ME), and this message was sent in plain (unencrypted and non-integrity protected) form. According to the 3GPP 5G standard (TS 24.501), after security mode command and successful 5G-AKA, the UE should only accept critical NAS messages (such as Registration Reject) if they are received with the appropriate security protections enabled (integrity protected and, if possible, ciphered). The UE, in this case, did not respond to the Registration Reject message sent in plain text, which is the correct and secure behavior per the standard; it should ignore such messages that are not integrity protected after security context is established. This prevents downgrade or spoofing attacks where an attacker might attempt to disrupt service by sending unauthenticated rejection messages. Therefore, the UE's action—refusing to process or respond to an unprotected Registration Reject after 5G-AKA—is secure and compliant with 3GPP security requirements. Secure

265	265_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1111 RAND: 0e38a634245d3e4aea72a7f7a7148161 AUTN: 3d9033e57f3e8000d3eb278394dd7c46 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 1.0084679126739502 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0087080001831055 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Authentication request 1.216444969177246 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the User Equipment (UE) completed the 5G-AKA authentication procedure, after which it sent a Service Request to the Access and Mobility Management Function (AMF). The AMF, under the tester's control, responded with an Authentication Request message that was sent in plain (unencrypted) form, even though a native security context had already been established and the ngKSI (Key Set Identifier) value was already in use. According to 3GPP 5G security standards, once 5G-AKA is successfully completed and a security context is established, all subsequent NAS messages are required to be integrity protected and, where possible, encrypted. The UE, upon receiving an unprotected Authentication Request with an ngKSI value that it had already used, correctly responded with an Authentication Failure message, indicating "ngKSI already in use." This behavior aligns with 3GPP standards, as the UE is expected to reject unauthenticated or replayed requests that violate the expected security context, thus preventing downgrade or replay attacks. Therefore, the UE's action was secure, as it did not accept or process the insecure message and instead reported the anomaly as specified by the standard. Secure
266	266	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.5199589729309082 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.520190954208374 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent an Authentication Reject message in plain (unencrypted) form. Importantly, the UE did not respond to this message. According to the 3GPP 5G standards, once 5G-AKA is completed, NAS security (encryption and integrity protection) should be activated for subsequent NAS messages. The Authentication Reject message is a security-critical message and, per 3GPP TS 24.501, it should only be accepted by the UE if it is integrity protected and, when required, encrypted. If an Authentication Reject is received in plain text after security activation, the UE is expected to ignore it and not react, to prevent security attacks such as downgrades or false rejections. In this test, the UE correctly did not respond to the unauthenticated, unencrypted Authentication Reject message received after security activation. This behavior aligns with the 3GPP security requirements and demonstrates that the UE is resistant to this class of attacks. Secure

267	267	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.5199449062347412 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201799869537354 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent an Authentication Reject message back to the UE, and this message was transmitted in plain (unencrypted) form. According to 3GPP standards, after the completion of 5G-AKA, NAS security (integrity protection and ciphering) should be activated for all subsequent NAS messages, including error and reject messages such as Authentication Reject. The UE's expected secure behavior, as per 3GPP TS 24.501 and TS 33.501, is to ignore any plain (unencrypted) NAS messages received after the security context has been established, since accepting such messages could expose the UE to security vulnerabilities (e.g., replay or downgrade attacks). In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the 3GPP security requirements, as it indicates the UE did not process or act upon an insecure message after security activation. Therefore, the action taken by the UE was secure 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 5G standalone security test, the User Equipment (UE) successfully completed the 5G-AKA authentication procedure, which is a prerequisite for establishing NAS security (encryption and integrity protection of NAS messages). After this, the UE sent a "Registration Complete" uplink NAS message to the AMF, followed by the AMF sending a "Configuration Update Command" downlink NAS message. The test notes that the AMF's downlink message was marked as "Protected," but the security header was "Unknown," and the UE did not respond to this message. According to 3GPP 5G standards, after 5G-AKA completion, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. If the security header is not recognized or the message cannot be verified as protected, the UE is expected to discard the message and not respond, as a security measure to prevent potential attacks or tampering. Given that the UE did not respond to the configuration update command with an unknown security header, it acted in accordance with the 3GPP security specifications by refusing to process an improperly protected message. Therefore, the UE's behavior in this scenario was secure. Secure

269	269	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.46799302101135254 UE to AMF UplinkNASTransport, Registration complete 0.4681861400604248 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test, after the successful completion of the 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior indicating that the NAS security context has been established and all subsequent NAS messages should be protected (i.e., encrypted and integrity protected) according to 3GPP TS 24.501. Following this, the AMF sent a "Deregistration Accept" message to the UE, but crucially, this message was sent in plain (unencrypted) text. According to the 5G security specifications, once the NAS security context is established (after 5G-AKA), the UE must reject or ignore any subsequent NAS messages from the network that are not integrity protected and encrypted, except for a very limited set of exceptions (e.g., Service Reject, Deregistration Request from the network during some specific cases). In this test, the UE did not respond to the plain "Deregistration Accept" message, which aligns with the security expectations of the standard to avoid potential security risks such as downgrade or spoofing attacks. By refusing to process or respond to a plain message after security activation, the UE demonstrated correct and secure behavior according to 3GPP requirements. Secure
270	270	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999805450439453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024100303649902 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS steps, the UE sent an identity response to the AMF, and the AMF subsequently sent another identity request for the IMEISV. Notably, the AMF's identity request was sent in plain (unencrypted) NAS, as the 5G-AKA authentication procedure had not yet been completed; therefore, the NAS security context was not established. According to 3GPP 5G standards (TS 24.501), the IMEISV is considered sensitive information and should only be transmitted after NAS security activation, i.e., after 5G-AKA is completed and NAS messages are encrypted. In this case, the UE did not respond to the AMF's plain (unencrypted) request for the IMEISV, thereby protecting its sensitive information from potential interception or exposure. This behavior aligns with the 3GPP security requirements, which state that the UE must not send the IMEISV in cleartext before NAS security is established. Thus, the UE's action was secure, as it adhered to the standard by refusing to disclose sensitive information over an unprotected channel. Secure

271	271	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.03961491584777832 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.03991198539733887 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the initial NAS procedures but before the 5G-AKA authentication was completed, the UE sent an Identity Response to the AMF. Subsequently, the AMF issued another Identity Request, specifically asking for the IMEI, and this message was sent in plain (unencrypted) form since the 5G-AKA had not yet established security. The UE, upon receiving this plain Identity Request for the IMEI, did not respond. According to the 3GPP 5G standard, the UE must protect sensitive information such as the IMEI and should not send it in response to plain (unencrypted) NAS messages when security context has not been established. By withholding its IMEI in this situation, the UE correctly adhered to the security requirements outlined by 3GPP, preventing exposure of device identity information before encryption was in place. This demonstrates that the UE acted securely by refusing to transmit potentially sensitive information over an unprotected channel. Secure
272	272	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007159709930419922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2011561393737793 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G registration process by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under tester control, responded with a Service Accept message that was marked as "Protected" (i.e., appearing as if it were integrity protected and/or encrypted). However, the critical 5G-AKA authentication and key agreement procedure had not yet been completed; this step is necessary for establishing the security context that enables both integrity protection and encryption of NAS messages between the UE and the AMF. Despite this, the UE accepted the Service Accept message and then sent a Deregistration Request. According to 3GPP 5G security standards, the UE must not accept or process protected NAS messages (such as Service Accept) before the completion of 5G-AKA, since no security context exists to validate or decrypt such messages. The UE should have rejected or ignored the Service Accept message, as it could not have verified its authenticity or integrity. Therefore, the UE’s action of accepting a protected message before security context establishment is a security flaw, as it exposes the UE to potential attacks (e.g., replay or spoofing) and violates the 3GPP security requirements. Insecure

273	273	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11984086036682129 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12007284164428711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Authentication Response to the AMF as part of the 5G-AKA process. However, before the 5G-AKA procedure was successfully completed (i.e., before mutual authentication and the establishment of NAS security context), the AMF sent a Deregistration Request to the UE. Notably, this Deregistration Request was sent as a "protected" NAS message, meaning it was integrity protected and ciphered, as indicated by the security header (2). According to the 3GPP 5G security standards, NAS message protection (integrity protection and ciphering) must only be applied after the successful completion of the 5G-AKA authentication and the associated security context establishment. Prior to this, the UE should not process or respond to any protected NAS messages, as it does not yet share the necessary keys with the network to validate or decrypt such messages. In this test, the UE did not respond to the protected Deregistration Request, which is the correct and secure behavior as per 3GPP standards, since accepting or processing protected messages before security context establishment could expose the UE to security risks such as replay or impersonation attacks. Therefore, the UE's refusal to respond demonstrates adherence to the 3GPP security requirements. 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 the described test scenario, the UE completed the initial NAS steps and sent an authentication response to the AMF, but the 5G-AKA procedure was not yet completed, meaning that mutual authentication and the establishment of NAS security keys (for encryption and integrity protection) had not been finalized. Immediately after receiving the authentication response, the AMF sent a deregistration request to the UE, which was transmitted with integrity protection (as indicated by the security header) but before the security context was properly established. The UE did not respond to this deregistration request. According to the 3GPP 5G standard, NAS security (including integrity protection and encryption) should only be applied after the successful completion of the 5G-AKA procedure—specifically, after the Security Mode Command/Complete exchange and the activation of security context. Since the deregistration request was sent with integrity protection before the NAS security context was established, the UE, by not responding to this message, correctly adhered to the standard by refusing to process a protected message before security activation. This behavior prevents potential security vulnerabilities such as replay or spoofing attacks before mutual authentication and key establishment. Therefore, the UE's action in not responding to the prematurely protected message is in line with 3GPP security requirements and demonstrates secure behavior. Secure

275	275	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007669925689697266 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal ME) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated communication with the AMF by sending an initial registration request, as expected in the 5G standalone registration procedure. However, before the 5G-AKA authentication and key agreement procedure was completed (meaning security context had not yet been established), the AMF responded with a deregistration request that was integrity protected and ciphered—a level of protection that should only be possible after successful 5G-AKA completion. According to the 3GPP 5G standard, the UE should only process protected NAS messages after security has been activated, which is triggered by the successful completion of the authentication procedure. Since the UE did not respond to the protected deregistration request from the AMF (which was sent before security activation), this behavior aligns with 3GPP security requirements and demonstrates that the UE did not process or accept messages that it could not verify as secure. Therefore, the UE's action was secure, as it appropriately ignored a message that was protected before the establishment of a security context. Secure
276	276	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3232 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 1.6001770496368408 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Identity response 1.6007089614868164 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE responded to an identity request with an identity response, following which the AMF issued a Security Mode Command (SMC) to the UE. The 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed at this point, meaning that mutual authentication and key establishment between the UE and the network had not occurred. Critically, the Security Mode Command from the AMF was sent as a plain (unencrypted and unauthenticated) NAS message, and the UE did not respond to this message. According to the 3GPP 5G standard (TS 24.501), the Security Mode Command must only be accepted and processed by the UE after successful completion of authentication (i.e., after 5G-AKA), and the UE must ignore or reject any SMC sent in the clear prior to authentication and key establishment, as this could be an attack vector for downgrades or impersonation. The UE's lack of response to the plain, pre-authentication SMC demonstrates correct security behavior, as it did not accept or process security commands before the establishment of a secure context. Therefore, the UE's action was in line with the 3GPP security requirements and protected against possible security threats in this scenario. Secure

277	277	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.04006814956665039 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040535926818847656 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF were engaged in NAS communication during the initial registration procedure. The UE sent an Identity Response message to the AMF, which is expected to be unprotected since the 5G-AKA authentication and key agreement had not yet been completed; therefore, security context was not yet established. Subsequently, the AMF sent a Configuration Update Command to the UE, but this message was sent with integrity protection (as indicated by the security header) even though the 5G-AKA procedure was not completed, and thus the necessary NAS security context was not available. The UE, upon receiving this protected message without having established security keys, did not respond. According to the 3GPP 5G standard, the UE must only process protected NAS messages after security context is established through successful completion of 5G-AKA. If a protected message is received before this, the UE should ignore or reject it to prevent potential security breaches or protocol errors. Therefore, the UE's lack of response to the prematurely protected message was correct and in line with 3GPP security requirements, as it avoided processing a message that could not be properly authenticated. 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 UE completed the initial NAS procedures up to the identity response, which is expected to be sent in plain (unencrypted) NAS messaging since the 5G-AKA security procedure had not yet been completed. After receiving the identity response, the AMF sent a configuration update command as a plain NAS message (no security header protection), which is not permitted by the 3GPP 5G standard (TS 24.501) except in very specific circumstances, typically before security activation only for a limited set of messages (such as authentication requests or identity requests). Upon receiving this configuration update command in plain NAS, the UE did not process or respond to it; instead, it immediately sent a deregistration request to the AMF. This action by the UE aligns with the 3GPP security requirements: the UE must not accept or process NAS messages that require integrity protection (such as configuration update commands) unless NAS security has been activated via the completion of the 5G-AKA procedure. By refusing to process the insecure message and deregistering, the UE demonstrated correct and secure behavior according to the 5G standard. Thus, the UE's action in this scenario was secure. 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, after the UE initiated the registration process by sending an InitialUEMessage containing a Registration Request, the AMF responded with a Deregistration Accept message, which was sent as a protected (i.e., integrity-protected or encrypted) NAS message. However, the 5G-AKA authentication procedure had not been completed at this point, meaning that the UE and the network had not yet established the necessary security context for NAS message protection (encryption and integrity protection). According to the 3GPP 5G standard, NAS message protection (encryption/integrity) must only be activated after successful completion of the authentication and key agreement (5G-AKA) procedure. Therefore, the UE should not accept or process protected NAS messages before security context establishment, and it is expected behavior for the UE to not respond to a protected message sent prematurely. By not responding to the protected Deregistration Accept message before 5G-AKA was completed, the UE correctly adhered to the 3GPP security requirements, preventing potential security vulnerabilities such as replay or downgrade attacks. Thus, the action taken by the UE was secure and compliant with the 5G standard. Secure
280	280	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007870197296142578 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test scenario, the User Equipment (UE) initiated a 5G standalone registration by sending an initial registration request to the Access and Mobility Management Function (AMF). At this point, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is essential for establishing security context and enabling encryption and integrity protection of subsequent messages, had not yet been completed. Despite this, the AMF responded with a deregistration accept message, which was sent as a "protected" (i.e., integrity-protected or encrypted) downlink NAS message. According to the 3GPP 5G standard, the UE is not expected to process or respond to protected NAS messages before the security context has been established via 5G-AKA, as it would not possess the necessary keys to validate or decrypt such messages. The UE, in this test, did not respond to the protected deregistration accept message, which aligns with the expected secure behavior defined by the 3GPP standard. This is because processing or accepting protected messages without an established security context could expose the UE to security vulnerabilities such as replay or spoofing attacks. Therefore, the UE's action in not responding is considered secure based on the standard. 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 the described test scenario, the UE initiated the registration process by sending an initial registration request to the AMF. At this stage, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that a valid security context had not been established between the UE and the network. Following the registration request, the AMF sent a Configuration Update Command to the UE, and this message was protected with integrity protection and ciphering, using a "new security context" as indicated by the security header type 4. However, since the 5G-AKA had not been completed, the UE had not yet established the necessary keys for NAS security. According to 3GPP 5G standards (TS 33.501), the UE must not process NAS messages that are protected with a security context if the authentication procedure has not been completed, as the keys required for integrity and ciphering are not yet available. Correctly, the UE did not respond to the AMF's protected message, indicating that it refused to process a security-protected NAS message before security establishment. This behavior aligns with 3GPP security requirements and protects the UE from potential security vulnerabilities, such as replay or spoofing attacks before mutual authentication. Therefore, the UE's action was secure and compliant with the 5G standard. Secure
282	282	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006248950958251953 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) initiated a registration process by sending an initial registration request to the Access and Mobility Management Function (AMF). At this stage, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is responsible for establishing mutual authentication and deriving security keys, had not yet been completed. Despite this, the AMF responded with a configuration update command that was integrity protected and ciphered, as indicated by the security header (2). According to the 3GPP 5G standard, user and signaling messages should only be protected (i.e., encrypted and integrity protected) after the security context is established via successful completion of 5G-AKA. Since the UE had not yet completed 5G-AKA, it would not have the necessary keys to decrypt or verify the protected message from the AMF. The UE, therefore, did not respond to the configuration update command, which aligns with the expected secure behavior, as responding to or processing protected messages prior to security context establishment could expose the UE to security vulnerabilities or protocol exploits. By refusing to process or respond to the prematurely protected downlink message, the UE adhered to the security requirements defined by 3GPP. 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 the described test scenario, the UE initiated registration by sending an unprotected initial registration request to the AMF, as expected before security context establishment. The AMF, under tester control, responded with a "service accept" message that was marked as protected, even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security architecture, NAS message protection (encryption and integrity protection) can only be applied after successful completion of 5G-AKA, when both the UE and AMF share a security context. Since the AMF sent a protected message before 5G-AKA, the UE, following the standard, should not process or respond to protected messages when no security context exists. In this test, the UE did not respond to the protected "service accept" message, indicating that it correctly refused to process a protected NAS message before security activation. This behavior aligns with 3GPP security requirements and prevents premature acceptance of potentially spoofed or invalid messages. Therefore, the UE's action in this scenario was secure. Secure
284	284	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006928443908691406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2013227939605713 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF responded with a Service Accept message, which was sent as a protected (NAS security protected) message. However, the 5G-AKA authentication procedure had not yet been completed at this point, meaning that the necessary NAS security context (i.e., encryption and integrity protection keys) was not established. Despite this, the UE proceeded to send a Deregistration Request message following receipt of the Service Accept. According to the 3GPP 5G security specifications, specifically TS 33.501, NAS message protection (integrity and encryption) must only be applied after successful completion of the 5G-AKA procedure and the establishment of NAS security context. Any NAS security protected messages sent by the network before authentication and key agreement are to be ignored by the UE, and the UE should not send further NAS messages except to restart the authentication process. By responding to a downlink NAS-protected message from the AMF before 5G-AKA was completed, the UE violated the expected security behavior and exposed itself to potential security risks, such as replay or spoofing attacks. Therefore, the UE's action in this scenario was **insecure** according to the 3GPP 5G security standard. Insecure

285	285	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039772987365722656 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (PLMN not allowed) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is a normal step in the authentication and registration process. However, before 5G-AKA security procedures were completed (i.e., before mutual authentication and the establishment of NAS security), the AMF sent a Deregistration Request message to the UE. Notably, this Deregistration Request was sent using NAS security protection (integrity protected and ciphered), even though the 5G-AKA procedure, which establishes the necessary keys for such protection, had not yet been completed. According to the 3GPP 5G standards, the UE should ignore and not process NAS messages that are protected (integrity/ciphered) prior to the establishment of NAS security context through the completion of 5G-AKA. In this case, the UE correctly provided no response to the protected Deregistration Request, indicating that it did not process a message that was inappropriately protected before security establishment. This behavior aligns with the security requirements of the standard, as responding to such a message could expose the UE to potential attacks or protocol errors. Therefore, the UE's action was secure and compliant with 3GPP 5G security procedures. 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 User Equipment (UE) initiated the 5G NAS registration by sending an Initial Registration Request to the Access and Mobility Management Function (AMF). 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) had not been established between the UE and the AMF. The AMF then responded with a protected (i.e., integrity-protected and/or ciphered) GMM Status message, indicating a 5GMM cause code of 98 (Message type not compatible with the protocol state). According to the 3GPP 5G standard (TS 24.501), before 5G-AKA is completed, the UE is not required—and in fact, is not able—to process protected NAS messages, as the necessary security context and keys have not been established. The correct and secure behavior for the UE in this situation is to ignore or silently discard any NAS messages that are received with security protection before the NAS security context is set up. The UE did not respond to the protected GMM Status message from the AMF, which aligns with the expected secure behavior per the standard, as responding could lead to vulnerabilities or protocol confusion. Therefore, the UE's actions in this scenario were secure and compliant with 3GPP requirements. 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 NAS session by sending an initial registration request to the AMF, which is standard behavior for a device attempting to connect to a 5G standalone network. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that a secure NAS security context (including encryption and integrity protection) had not been established between the UE and the AMF. Subsequently, the AMF, under test control, sent a protected (i.e., integrity protected and/or encrypted) GMM status message with a 5GMM cause value of 3 ("Illegal UE") back to the UE. According to 3GPP standards, specifically TS 24.501, the UE should not process or respond to protected NAS messages before the NAS security context is established via 5G-AKA, as it cannot verify their authenticity or integrity. The UE's action of providing no response to the protected GMM status message prior to the completion of 5G-AKA is therefore correct and secure, as responding could expose it to security risks such as replay or spoofing attacks. The UE adhered to the 3GPP security requirements by ignoring a message it could not yet securely process. 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. In response, the AMF sent a Security Mode Command with the security header set to "Integrity protected with new security context (3)", using the null cipher algorithm (5G-EA0) and integrity protection algorithm 128-5G-IA2. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that no secure key material was established between the UE and the network. Upon receiving the Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, security-protected NAS messages (integrity and/or ciphered) should only be exchanged after successful completion of the 5G-AKA authentication and key agreement, which establishes the necessary security context. The AMF’s premature use of integrity protection (with a new security context) before authentication is non-standard, and the UE correctly identified this as an error, responding with a status message indicating invalid information. This behavior demonstrates that the UE did not accept or process security-protected messages before the security context was properly established, which aligns with the security requirements of the 3GPP standard. Therefore, the UE's actions were secure in this context. Secure

289	289	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 6.12048602104187 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Identity response 6.120656967163086 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE responded to an AMF identity request by sending an identity response. Subsequently, the AMF issued another identity request, specifically requesting the GUTI (Globally Unique Temporary Identifier), but this second request was sent in plain (unencrypted) NAS message format, as the 5G-AKA authentication procedure had not yet been completed. The UE did not respond to this subsequent plain identity request. According to the 3GPP 5G security standards, particularly TS 33.501, once the UE has provided its identity in response to an initial request, any further requests for sensitive information (like GUTI) sent in plain (unencrypted) NAS messages before the completion of 5G-AKA should be treated with caution, as responding could expose the UE to privacy and security risks such as identity theft or tracking. By not responding to the second plain identity request, the UE demonstrated adherence to the security principle of not disclosing sensitive information over an unprotected channel, as prescribed by the standard. Therefore, the UE’s action in this interaction was secure. Secure
290	290	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.039791107177734375 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040058135986328125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS (Non-Access Stratum) communication with the AMF (Access and Mobility Management Function). After completing previous NAS procedures, the UE sent an Identity Response, after which the AMF issued a subsequent Identity Request, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version) from the UE. Notably, this Identity Request was sent in plain (unencrypted) form because the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, and therefore, NAS security context was not established. According to 3GPP 5G security standards, prior to the completion of 5G-AKA and the establishment of NAS security, sensitive information such as the IMEISV should not be transmitted over the air in plain text. The UE, in this case, did not respond to the plain (unencrypted) request for the IMEISV, thereby refraining from exposing sensitive device identity information before a secure context was established. This behavior aligns with 3GPP security recommendations, as the UE protected its own security and privacy by not transmitting sensitive information in the clear. Therefore, based on the 5G standard, the UE’s action was secure. 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.	During the security test, the UE and the AMF engaged in NAS communication before the completion of the 5G-AKA authentication procedure. After the UE sent an identity response, the AMF issued another identity request, specifically requesting the TMSI, and crucially, this request was sent in plain (unencrypted) NAS messaging because 5G-AKA had not yet been completed. The UE did not respond to this subsequent identity request. According to the 3GPP 5G standard, user identity information such as the TMSI should only be transmitted in plain text before authentication and security activation if necessary for registration or authentication procedures. However, the standard also emphasizes minimizing exposure of subscriber identities in unprotected messages. Since the 5G-AKA was not yet completed and the request was sent in plain text, the UE's refusal to respond with its TMSI in this context demonstrates a secure behavior, as it avoids exposing sensitive identity information before a secure channel is established. This behavior aligns with best practices for protecting subscriber privacy and resisting potential identity exposure attacks. Therefore, the UE's action in this scenario was secure. Secure
292	292	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.11100292205810547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11120295524597168 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Not ciphered) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on 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 Authentication and Key Agreement (5G-AKA) procedure was completed, the AMF sent a deregistration request to the UE. Notably, this deregistration request was sent as a protected message with integrity protection, even though the security context from a completed 5G-AKA procedure had not yet been established. According to the 3GPP 5G standard, NAS message protection (integrity and encryption) should only be applied after the successful completion of the authentication and security setup (i.e., after 5G-AKA is complete and NAS security mode command/complete exchange has occurred). Since the UE had not yet established a security context, it correctly did not respond to a deregistration request that was integrity protected, as it would not have the necessary keys to validate or process the protected message. This behavior prevents potential security vulnerabilities such as accepting or acting on messages that appear protected but for which the UE cannot verify authenticity, which could be exploited in certain attacks. Therefore, the UE's action—refusing to respond to a protected message before security context establishment—aligns with the security requirements of the 3GPP 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 completion of the 5G-AKA procedure, the UE sent a "registration complete" message to the AMF, indicating that mutual authentication and key agreement had been successfully established. Following this, the AMF sent a "configuration update command" to the UE, but crucially, this downlink NAS message was sent as a plain (unencrypted and unauthenticated) message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), once the 5G-AKA procedure is completed and security context is established, all subsequent NAS messages, including configuration update commands, must be integrity protected and, where required, ciphered. The UE, upon receiving a plain NAS message when security context is already active, is expected to discard the message and not respond, in order to prevent security vulnerabilities such as replay or modification attacks. In this test, the UE did not respond to the plain configuration update command from the AMF, which is compliant with 3GPP security requirements and demonstrates correct and secure behavior by the UE. 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, the UE and AMF completed the 5G-AKA authentication, after which the UE sent a Security Mode Complete message to the AMF. According to the 3GPP 5G security standard, once 5G-AKA is completed and the security mode is established (Security Mode Complete), all subsequent NAS messages between the UE and AMF should be integrity protected and, where required, ciphered using the negotiated security context. However, in this test, after the Security Mode Complete message from the UE, the AMF sent an Authentication Request message in plain (unencrypted and unprotected) form, which is not compliant with the 3GPP standard. The UE, upon receiving this unexpected plain NAS message after security activation, did not respond. According to the 3GPP specification (TS 24.501), the UE is required to ignore and not process any unprotected NAS messages after security has been activated, to prevent downgrade or replay attacks. By not responding to the plain Authentication Request, the UE demonstrated correct and secure behavior as per the standard, refusing to process messages that could compromise the established security context. Therefore, the UE's action in this scenario was secure. 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 procedure (which establishes mutual authentication and key agreement between the UE and the network), the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security parameters and was ready to enter a secure NAS communication state. Subsequently, the AMF sent a "service reject" message with 5GMM Cause 111 (protocol error, unspecified), and crucially, this message was sent in plain (unencrypted) NAS format rather than being integrity protected and encrypted as required after security mode is established. According to the 3GPP 5G standard (TS 24.501, section 5.4.3.4 and related security procedures), once the NAS security context is established (i.e., after the security mode complete), all subsequent NAS messages exchanged between the UE and the network must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain, unprotected NAS message after security mode is active, is required by the standard to discard the message and not process or respond to it, as processing such messages would be a security vulnerability (e.g., exposing the UE to spoofing or replay attacks). In this test, the UE did not respond to the unprotected "service reject" message, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by refusing to accept or act on messages that violate the expected security context. This shows that the UE's actions were secure according to 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 the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, indicating that it had agreed to the security parameters and was ready to begin protected NAS communication. However, the AMF, under test control, subsequently sent an Authentication Request message to the UE in plain (unencrypted) form, which deviates from the expected 5G protocol sequence—authentication should occur before security mode setup, and after security mode is complete, all subsequent NAS messages must be integrity protected and, if required, encrypted. The UE, upon receiving this unexpected and insecure plain Authentication Request after security mode completion, did not respond. According to the 3GPP 5G security standard, the UE is required to reject or ignore any NAS messages that are not properly integrity protected after the security context is established. The UE's lack of response demonstrates compliance with the standard and protects against potential security risks such as replay or downgrade attacks. Therefore, the UE's action was secure and aligned with 3GPP requirements. Secure

297	297	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.16003108024597168 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16027402877807617 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the 5G-AKA authentication procedure was successfully completed, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated NAS security algorithms and was ready to send and receive encrypted NAS messages. However, the subsequent message from the AMF—a "deregistration accept"—was sent in plain (unencrypted) form. According to the 3GPP 5G standards (TS 24.501), once the security mode is complete, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. The UE, upon receiving a plain (unencrypted) NAS message after security activation, should discard the message and not process it, as this could be a sign of a security attack or protocol misconfiguration. In this test, the UE provided no response to the plain "deregistration accept" message, which aligns with the expected secure behavior as per 3GPP standards, since it did not accept or process a message that was not properly protected after security was established. Therefore, the UE acted securely in this scenario. Secure
298	298	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.1601550579071045 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16047000885009766 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure between the User Equipment (UE) and the Access and Mobility Management Function (AMF), the UE sent a "Security Mode Complete" message to the AMF, indicating that it was ready to proceed with NAS security-protected communication. However, the AMF then sent an "Authentication Reject" message to the UE, and critically, this message was sent as a plain (unencrypted and unauthenticated) NAS message. According to the 3GPP 5G standard (TS 24.501), after the security context is established (i.e., after 5G-AKA and Security Mode Complete), all subsequent NAS messages—especially those with security implications such as "Authentication Reject"—must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain "Authentication Reject" message after security context establishment, did not respond further, which aligns with the 3GPP security requirements. This behavior prevents the UE from accepting potentially spoofed or tampered messages that could compromise its security context or allow for denial-of-service attacks. Therefore, the UE's action of ignoring the unauthenticated message is compliant with the 5G standard and demonstrates secure behavior in this context. Secure

299	299	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.15986394882202148 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16010284423828125 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, which indicates that the NAS security context should now be established and all subsequent NAS messages should be protected (i.e., integrity protected and, if required, ciphered). However, the AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted and unprotected) format. According to the 3GPP 5G standards (notably TS 24.501), once the security context is activated, the UE is required to ignore any subsequent plain NAS messages that should be protected, except for a very limited set of messages (such as Service Reject and Deregistration Accept under specific conditions). Authentication Reject is not among the exceptions and, after security activation, should only be accepted if integrity protected. In this test, the UE did not respond to the plain Authentication Reject, which demonstrates compliance with the 3GPP security requirements by not accepting or reacting to an unprotected message that could be a security threat (e.g., a replay or spoofing attempt). Therefore, the UE's action was secure. Secure
300	300	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.15969204902648926 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15989899635314941 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA procedure—which establishes mutual authentication and the security context between the UE and the network—the UE sent a "security mode complete" message to the AMF, indicating it was ready to begin secure NAS communication. Immediately after, the AMF sent an "identity request" message requesting the UE's TMSI; importantly, this message was sent in plain (unencrypted) NAS, despite the security context having already been established. According to 3GPP 5G security standards (TS 33.501), once the security mode command is completed, all subsequent NAS messages—including identity requests—must be integrity protected and ciphered (encrypted). The UE, upon receiving an unprotected identity request after security activation, did not respond. This behavior is correct and secure: the UE is required by the standard to ignore or silently discard any unprotected NAS messages received after the security context is active, as responding to such messages could expose sensitive information to potential attackers. Therefore, the UE's refusal to respond to an unprotected identity request after completing security setup demonstrates compliance with 3GPP security requirements and is the secure action. Secure